Türkiye İç Denetim Enstitüsü

The IIA Research Foundation

# Uluslararası İç Denetim Standartları

## *Meslekî Uygulama Çerçevesi*

*(2007'deki Değişikliklerle)*

Deloitte.

# Uluslararası İç Denetim Standartları

## *Meslekî Uygulama Çerçevesi*

***(2007'deki Değişikliklerle)***

**TÜRKİYE**
**İÇ DENETİM ENSTİTÜSÜ**
**www.tide.org.tr**

**THE INSTITUTE OF**
**INTERNAL AUDITORS**
**www.theiia.org**

**Açıklama**

IIA bu kitabı bilgilendirme ve eğitim amaçlarıyla basmıştır. Bu kitap, bilgi sağlamak amacında olup herhangi bir hukukî veya muhasebeyle ilgili tavsiyeyi ikame etmez. IIA bu tür bir tavsiye vermediği gibi bu yayının basımı yoluyla herhangi bir hukukî veya muhasebeyle ilgili sonuca dair garanti de vermez. Hukuk veya muhasebe sorunlarının ortaya çıkması durumunda profesyonel yardım aranmalı ve alınmalıdır.

İç Denetim Meslekî Uygulama Çerçevesi, IIA Yönetim Kurulu'nun Kılavuzluk Görev Gücü tarafından mesleğin mevcut ve geliştirilmekte olan uygulama kılavuzunun hemen hemen tüm yönlerini düzenleyecek şekilde tasarlanmıştır. Etik Kuralları, İç Denetim Standartları ve Uygulama Önerilerinden oluşan İç Denetim Meslekî Uygulama Çerçevesi, iç denetimin yeni tarifini esas alarak, iç denetime uzanan yolun dünya standartlarında taşlarını döşemektedir.



Basım Yılı: 2008

Basım Yeri: Print Center
Sanayi Mah. Manolya Sok. No.3 Seyrantepe / İSTANBUL
Tel: (0212) 371 03 00

# SUNUŞ

Bir mesleğin evrensel kabul görmüş standartlarının olması, mesleğin icrasından umulan her seviyedeki faydaların da bir nevi teminatıdır. İç denetim de dünyadaki meslekdaşlarımızın ortak mücadeleleriyle standartlarını oluşturma aşamasını yakalamış, geçmiş ve iş dünyasındaki yeni şartlar karşısında kendisini yenileyerek varlığını devam ettirme çabasını sürdüren bir meslek konumuna gelmiştir.

IIA'nın Uluslararası İç Denetim Standartları, 2004 yılından beri bütün IIA üyeleri ve Uluslararası İç Denetçiler (CIA) için zorunlu kılavuz hâline gelmiştir. *Standartlar*, zorunlu olmayan Uygulama Önerileri ile birlikte, mesleğin etkin ve verimli icrasına sağlam zemin hazırlayan bir meslekî uygulama çerçevesi sunmaktadır.

Elinizdeki bu baskı, TİDE tarafından meslekdaşlarımızın istifadesine 1996 ve 2004 yıllarında sunulan ve 'Kırmızı Kitap' olarak da bilinen eserin 2007'de yapılan değişiklikleri de ihtiva eden güncel versiyonudur. Geçen zaman diliminde, özel ve kamu sektöründeki şirket ve kurumların iç denetim mesleğini uluslararası standartlarda uygulamak için gittikçe artan bir çaba sergilemeleri ve bu çaba içinde Kırmızı Kitabı rehber olarak değerlendirmeleri, 1995'ten beri artarak süren faaliyetlerimizin meyvelerini verdiği anlamına geliyor ve bizi mutlu ediyor.

Bu çalışmanın yapılmasında emeği geçen, *İstanbul Menkul Kıymetler Borsası Teftiş Kurulu başmüfettişleri* Ali Şîr Yardım (CIA, CFE), Serhan Göktürk (CIA, CFE), Asım Erdener Ayhan (CIA, CFE, CISA) ve UBS Menkul Değerler A.Ş. İç Denetim Müdürü Uzay Şener (CIA, SMMM) başta olmak üzere TİDE Standartlar Komitesi üyelerimize ve önceki baskıda olduğu gibi projenin maddî açıdan desteklenmesinde büyük pay sahibi olan *Deloitte & Touche Türkiye* yetkililerine gönülden teşekkürlerimizi sunarız.

**Türkiye İç Denetim Enstitüsü**
**Yönetim Kurulu**

# İÇİNDEKİLER

**SUNUŞ** ..... iii
**İÇİNDEKİLER** ..... vii
**ULUSLARARASI İÇ DENETİM STANDARTLARI** ..... 1
**ÖNSÖZ** ..... 3
**İÇ DENETİMİN TANIMI** ..... 7
**ETİK KURALLARI** ..... 9
**GİRİŞ** ..... 15
**Nitelik Standartları** ..... 19
1000 Amaç, Yetki ve Sorumluluklar ..... 19
1100 Bağımsızlık ve Objektiflik ..... 19
1110 Kurum İçi Bağımsızlık ..... 19
1120 Bireysel Objektiflik ..... 19
1130 Bağımsızlık ve Objektifliği Bozan Etkenler ..... 19
1200 Yeterlilik ve Azamî Meslekî Özen ve Dikkat ..... 20
1210 Yeterlilik ..... 21
1220 Azamî Meslekî Özen ve Dikkat ..... 21
1230 Sürekli Meslekî Gelişim ..... 22
1300 Kalite Güvence ve Geliştirme Programı ..... 22
1310 Kalite Programı Değerlendirmeler ..... 23
1311 İç Değerlendirmeler ..... 23
1312 Dış Değerlendirmeler ..... 23
1320 Kalite Programı Hakkında Raporlama ..... 23
1330 "Standartlara Uygun Yapılmıştır" İbaresinin Kullanılması ..... 23
1340 Aykırılıkların Açıklanması ..... 24
**Performans Standartları** ..... 25
2000 İç Denetim Faaliyetinin Yönetimi ..... 25
2010 Planlama ..... 25
2020 Bildirim ve Onay ..... 25
2030 Kaynak Yönetimi ..... 25

2040 Politika ve Prosedürler ..... 25
2050 Eşgüdüm ..... 26
2060 Yönetim Kurulu, Denetim Kurulu ve Üst Yönetime Raporlamalar ..... 26
2100 İşin Niteliği ..... 26
2110 Risk Yönetimi ..... 26
2120 Kontrol ..... 27
2130 Yönetişim ..... 28
2200 Görev Planlaması ..... 29
2201 Planlamada Dikkate Alınması Gerekenler ..... 29
2210 Görev Amaçları ..... 30
2220 Görev Kapsamı ..... 30
2230 Görev Kaynaklarının Tahsisi ..... 31
2240 Görev İş Programı ..... 31
2300 Görevin Yapılması ..... 31
2310 Bilgilerin Tespiti ve Tanımlanması ..... 31
2320 Analiz ve Değerlendirme ..... 31
2330 Bilgilerin Kaydedilmesi ..... 31
2340 Görevin Gözetim ve Kontrolü ..... 32
2400 Sonuçların Raporlanması ..... 32
2410 Raporlama Kıstasları ..... 32
2420 Raporlamaların Kalitesi ..... 33
2421 Hatâ ve Eksiklikler ..... 33
2430 Görevlendirmelerde Standartlara Aykırılıkların Açıklanması ..... 33
2440 Sonuçların Raporlanması ..... 33
2500 İlerlemenin Gözlenmesi ..... 34
2600 Yönetimin Artık (Bakiye) Riskleri Üstlenmesi ..... 34

**TERİMLER SÖZLÜĞÜ** ..... 35
**UYGULAMA ÖNERİLERİ** ..... 41
**NİTELİK STANDARTLARI İLE İLGİLİ OLANLAR**
1000-1 : İç Denetim Yönetmeliği ..... 43
1000.C1-1 : İç Denetçilerin Danışmanlık Faaliyetlerinin ... Yürütülmesine İlişkin İlkeler ..... 45
1000.C1-2 : Resmî Danışmanlık Görevlerine İlişkin Ek Hususlar ..... 49
1000.C1-3 : İdarî Kurumsal Düzenlemelerdeki Danışmanlık Görevlerine İlişkin Ek Hususlar ..... 59
1100-1 : Bağımsızlık ve Objektiflik ..... 69
1110-1 : Kurum İçi Bağımsızlık ..... 71
1110.A1-1 : Bilgi Talebinin Sebebinin Açıklanması ..... 73
1110-2 : İç Denetim Yöneticisi-Hiyerarşik İlişkiler ..... 75
1120-1 : Bireysel Objektiflik ..... 83
1130-1 : Bağımsızlık veya Objektifliği Bozan Etkenler ..... 85
1130.A1-1 : İç Denetçilerin Daha Önceden Sorumlu Olduğu Faaliyetlere İlişkin Değerlendirmeleri ..... 87
1130.A1-2 : Diğer (Denetim Dışı) İşlevler Karşısında İç Denetçinin Sorumluluğu ..... 89
1200-1 : Yeterlilik ve Azamî Özen ve Dikkat ..... 93
1210-1 : Yeterlilik ..... 95
1210.A1-1 : İç Denetim Faaliyetini Tamamlamak veya Desteklemek Amacıyla Hizmetlerin Dışarıdan Temini ..... 97
1210.A2-1 : Suiistimal Riskinin Değerlendirilmesi, Önlenmesi ve Tesbitinde Denetçinin Sorumlulukları ..... 103
1210.A2-2 : Suiistimalin Soruşturulması, Raporlanması, Çözüme Kavuşturulması ve İletişim İle İlgili Denetçinin Sorumlulukları ..... 115
1220-1 : Azamî Meslekî Özen ve Dikkat ..... 125
1220-2 : Bilgisayar Destekli Denetim Teknikleri (BDDT'ler) ..... 125

1230-1 : Sürekli Meslekî Gelişim..... 137
1300-1 : Kalite Güvence ve Geliştirme Programı ..... 139
1310-1 : Kalite Programı Değerlendirmeleri..... 143
1311-1 : İç Değerlendirmeler ..... 147
1311-2 : İç Denetim Faaliyetinin Gözden Geçirilmesinin Desteklenmesi İçin (Nicel Metrikler ve Nitel Değerlendirmeler) Ölçülerin Tesis Edilmesi ... 151
1312-1 : Dış Değerlendirmeler..... 162
1312-2 : Dış Değerlendirmeler: Bağımsız Onaylı Özdeğerlendirme..... 169
1320-1 : Kalite Programı Hakkında Raporlama..... 175
1330-1 : "Standartlara Uygun Yapılmıştır" İbaresinin Kullanılması..... 177

**PERFORMANS STANDARTLARI İLE İLGİLİ OLANLAR**

2000-1 : İç Denetim Faaliyetinin Yönetimi..... 179
2010-1 : Planlama..... 181
2010-2 : Denetim Planıyla Risk ve Risk Maruziyeti Arasında Bağlantı Kurulması..... 183
2020-1 : Bildirim ve Onay..... 187
2030-1 : Kaynak Yönetimi ..... 189
2040-1 : Politika ve Prosedürler ..... 193
2050-1 : Eşgüdüm..... 195
2050-2 : Dış Denetim Hizmetlerinin Satın Alınması ..... 201
2060-1 : Denetim Komitesi, Yönetim Kurulu ve Üst Yönetime Raporlama ..... 207
2060-2 : Denetim Komitesiyle İlişkiler..... 209
2100-1 : İşin Niteliği ..... 217
2100-2 : Bilgi Güvenliği..... 221
2100-3 : İç Denetimin Risk Yönetim Sürecindeki Rolü .. 223
2100-4 : Risk Yönetim Süreci Bulunmayan Kurumlarda İç Denetimin Rolü..... 227

| | | |
|---|---|---|
| 2100-5 | : Mevzuata Uyum Programlarının Değerlendirilmesinde Hukukî Mülâhazalar | 231 |
| 2100-6 | : E-Ticaret Faaliyetlerinin Kontrol ve Denetimi | 241 |
| 2100-7 | : Çevresel Risklerin Tanımlanması ve Rapor Edilmesinde İç Denetçinin Rolü | 251 |
| 2100-8 | : Bir Kurumun Gizlilik Politikasının Değerlendirilmesinde İç Denetçinin Rolü | 257 |
| 2100-9 | : Uygulama Sistemlerinin İncelenmesi | 261 |
| 2100-10 | : Denetim Örnekleme Çalışması | 267 |
| 2100-11 | : Yaygın Etkili Bilişim Sistemleri (BS) Kontrollerinin Etkisi | 275 |
| 2100-12 | : Bilişim Sistemleri (BS) Faaliyetlerinin Başka Kurumlarda Yaptırılması | 285 |
| 2100-13 | : Üçüncü Tarafların Bir Kurumun BT Kontrolleri Üzerindeki Etkisi | 291 |
| 2100-14 | : Denetim Delili Koşulu | 303 |
| 2110-1 | : Risk Yönetim Sürecinin Yeterliliğinin Değerlendirilmesi | 309 |
| 2110-2 | : İş Devamlılığı Sürecinde İç Denetçinin Rolü | 315 |
| 2120.A1-1 | : Kontrol Süreçlerinin Değerlendirilmesi ve Rapor Edilmesi | 321 |
| 2120.A1-2 | : Kontrol Süreçlerinin Yeterliliğini Değerlendirmede Kontrol Özdeğerlendirme önteminin Kullanılması | 327 |
| 2120.A1-3 | : Üç Aylık Finansal Raporlama, Özel Durum Açıklamaları ve Yönetim Onayları onusunda İç Denetçinin Rolü | 335 |
| 2120.A1-4 | : Finansal Raporlama Sürecinin Denetlenmesi | 343 |
| 2120.A4-1 | : Kontrol Kıstasları | 353 |
| 2130-1 | : İç Denetim Faaliyeti ve İç Denetçinin Bir Kurumun Etik Kültüründe Oynadığı Rol | 355 |
| 2200-1 | : Görev Planlaması | 361 |

2210-1 : Görev Amaçları ..... 365
2210.A1-1 : Görev Planlamasında Risk Değerlendirmesi ... 367
2230-1 : Görev Kaynaklarının Tahsisi ..... 371
2240-1 : Görev Programı ..... 373
2240.A1-1 : İş Programlarının Onaylanması ..... 375
2300-1 : İç Denetçinin Denetiminde Kişisel Bilgiler Kullanması ..... 377
2310-1 : Bilgilerin Tespiti ve Tanımlanması ..... 379
2320-1 : Analiz ve Değerlendirme ..... 381
2330-1 : Bilgilerin Kaydedilmesi ..... 385
2330.A1-1 : Görev Kayıtlarının Kontrolü ..... 389
2330.A1-2 : Görev Kayıtlarına Erişim Hakkı Verilmesine Dair Hukukî Mülâhazalar ..... 391
2330.A2-1 : Kayıtların Saklanması ..... 397
2340-1 : Görevin Gözetim ve Kontrolü ..... 399
2400-1 : Sonuçların Raporlanmasına Dair Hukukî Mülâhazalar ..... 403
2410-1 : Raporlama Kıstasları ..... 407
2420-1 : Raporlamaların Kalitesi ..... 413
2440-1 : Görev Sonuçlarının Raporlanacağı Taraflar .... 415
2440-2 : Kurum Dışına Raporlamalar ..... 417
2440-3 : Hassas Bilgilerin Hiyerarşi İçinde ve Dışında Raporlanması ..... 421
2500-1 : İlerlemenin Gözlenmesi ..... 429
2500.A1-1 : Takip Süreci ..... 431
2600-1 : Yönetimin Artık (Bakiye) Riskleri Üstlenmesi ... 433

# ULUSLARARASI İÇ DENETİM STANDARTLARI

# ÖNSÖZ

Haziran 1999'da, Uluslararası İç Denetçiler Enstitüsü (IIA) yönetim kurulunda yapılan oylama ile yeni bir *iç denetim tanımı* ve yeni bir *Meslekî Uygulama Çerçevesi* kabul edildi. Genel anlamda Çerçeve, bilgi ile rehberliğin birbirine nasıl uyacağına dair yapısal bir plan sunmaktadır. Çerçeve, uyumlu bir sistem olarak, mesleğe yararlı teknik, yöntem ve kavramların geliştirilmesi, yorumlanması ve uygulanmasına imkân sağlamaktadır. Özellikle belirtmek gerekir ki Meslekî Uygulama Çerçevesi'nin amacı, zaman darlığı olan durumlarda da arzu edilen bilgilere kolay ulaşılabilmeyi sağlayan bir düzen oluşturmaktır. Mevcut iç denetim uygulamasını da içine alarak, Meslekî Uygulama Çerçevesi tüm dünyadaki iç denetçilere, yüksek kalitede iç denetim hizmetleri gerektiren ve giderek büyüyen piyasanın ihtiyaçlarına cevap vermede yardımı hedeflemektedir.

Meslekî Uygulama Çerçevesi, 'İç Denetimin Tanımı', 'Etik Kurallar', 'Uluslararası İç Denetim Meslekî Uygulama Standartları (kısaca Uluslararası İç Denetim Standartları veya *Standartlar*)' ve 'Uygulama Önerileri'ni kapsamaktadır. İlk üç madde (İç Denetimin Tanımı, Etik Kurallar, Uluslararası İç Denetim Standartları), zorunlu rehberlik olarak kabul edilmektedir. Tüm *zorunlu* rehberlik maddeleri, yine zorunlu bir süreç vasıtasıyla, meslekî açıdan gözden geçirilmesi için kamuoyuna sunulmuştur ve iç denetim uygulamalarında *gerekli* oldukları düşünülmektedir. Meslekî Uygulama Çerçevesi'nin diğer unsurları *Standartlar* ile bağlantılıdır.

Tanım itibariyle iç denetim, bir kuruluşun faaliyetlerine değer katmak ve bunları geliştirmek için tasarlanan bağımsız bir nesnel güvence ve danışmanlık faaliyetidir. Risk yönetimi, kontrol ve yönetişim süreçlerini değerlendirmek ve geliştirmek için sistematik ve kurallı yaklaşımlar getirerek kuruluşun hedeflerine ulaşmasında yardımcı olur.

Tüm dünyada iç denetim, değişik ortamlarda ve farklı büyüklük, amaç ve yapıya sahip kuruluşlarda yapılır. Ayrıca, farklı ülkelerdeki kanunlar ve gelenekler birbirinden farklıdır. Bu farklılıklar, her bir ortamdaki iç denetim uygulamasını etkileyebilir. Bu yüzden, Meslekî Uygulama Çerçevesinin hayata geçirilmesi üzerinde, iç denetim faaliyetlerinin yerine getirildiği *ortamın* da etkisi olacaktır. Meslekî Uygulama Çerçevesi'nde bulunmayan bilgiler, yürürlükteki mevzuat dikkate alınarak yorumlanmalıdır. Meslekî Uygulama Çerçevesi'nde olan bir bilgi hakkında ortaya çıkan bir durum, mevzuat ile çelişki arz ederse, iç denetçilerin, IIA'ye veya hukuk müşavirlerine başvurmaları tavsiye edilir.

IIA Etik Kuralları'nın amacı, iç denetim mesleğinde *etik bir kültür* oluşturmaktır. Etik Kuralları, iç denetim mesleği için gerekli ve uygundur; ki bu meslek risk yönetimi, kontrol ve yönetişimle ilgili objektif güvence çalışmasında güven üzerine kuruludur.

Meslekî Uygulama Çerçevesi'nde belirtildiği gibi, *Standartlar*, iç denetim biriminin faaliyetlerinin değerlendirilmesi ve ölçülmesinde kullanılan *kıstaslar*dır. *Standartlar*, iç denetim uygulamasının nasıl olması gerektiğini gösterir. *Standartlar*, iç denetçilerin bulunduğu her türlü kurum ve şirkette, iç denetim mesleğinin tamamına hizmet etmek için oluşturulmuştur.

Meslekî Uygulama Çerçevesi'nde, üç takım standart vardır: Nitelik, performans ve uygulama standartları. *Nitelik Standartları*, iç denetim faaliyetlerini yürüten kurum ve fertlerin özelliklerine yöneliktir. *Performans Standartları*, iç denetim faaliyetlerinin tabiatını açıklar ve bu hizmetlerin performansını değerlendirmekte kullanılan kalite ksıtaslarını sağlar. Nitelik ve Performans Standartları, tüm iç denetim hizmetlerine uygulanırken, *Uygulama Standartları,* belirli görev türlerine tatbik edilir.

Zorunlu rehberlikte telâffuz edilen kavramlarla uyum, iç denetçilerin sorumluluklarının yerine getirilmesi açısından gereklidir. Etik Kuralları'nda belirtildiği gibi, iç denetçiler, iç denetim hizmetlerini *Standartlar*'a uygun şekilde yerine getirmelidirler. IIA'nın tüm üyeleri ve tüm uluslararası denetçiler, Etik Kuralları'na ve *Standartlar*'a tâbidir ve bu rehberlik, IIA üyesi olsun ya da olmasın, tüm iç denetim mesleği mensuplarını bağlar.

Daha uygulanabilir olması amacıyla, zorunlu rehberliğin, bir nevi, işin tabiatının bir parçası olması gerekir. Uygulama Önerileri, IIA tarafından ısrarla tavsiye edilmektedir. Zorunlu olmasa da, Uygulama Önerileri, *Standartlar*'ın uygulanması açısından IIA'nın kabul ettiği uygulamaları ortaya koymaktadır. Uygulama Önerileri kısmen, *Standartlar*'ın yorumlanmasına veya özel iç denetim ortamlarında uygulanmasına yardımcı olur. Uygulama Önerileri'nin bir çoğu, tüm iç denetçiler tarafından uygulanabilirken, diğerleri, bazı sektörlerde özel denetim yapan veya farklı coğrafî alanlarda hizmet veren iç denetçilerin ihtiyaçlarını gidermek için geliştirilmiş olabilir. Uygulama Önerilerinin hepsi, IIA Meslekî Yayın Komitesi tarafından resmî bir gözden geçirme sürecine tâbi tutulur.

"Kırmızı Kitap" adıyla da bilinen Meslekî Uygulama Çerçevesi'nin bu baskısında, İç Denetimin Tanımı, Etik Kuralları, Standartlar ve Uygulama Önerileri bulunmaktadır. Güncel gelişmeler ve değişiklikler için *http://www.theiia.org/guidance* adresine başvurabilirsiniz.

Önümüzdeki yıllarda, iç denetçiler, rehberlik geliştirme konusundaki faal katılımları sayesinde Meslekî Uygulama Çerçevesi'nin daha da gelişeceğinden emin olabilirler. Konuyla ilgili tüm çevreleri, Meslekî Uygulama Çerçevesi hakkında yorum ve öneri yapmaya davet ediyoruz. Meslekî rehberlik, yorum ve önerilerinizi *guidance@theiia.org* adresine e-posta ile gönderebilirsiniz.

# İÇ DENETİMİN TANIMI

İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir *güvence ve danışmanlık* faaliyetidir. İç denetim, kurumun *risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini* değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.

# ETİK KURALLARI

# ETİK KURALLARI

## Giriş

IIA'nın Etik Kurallarının amacı, iç denetim mesleğinin etik kültürünü geliştirmektir.

> *İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.*

Bir etik kuralları manzumesi geliştirilmesi, iç denetim mesleği için gerekli ve uygundur; ki bu meslek risk yönetimi, kontrol ve yönetişimle ilgili objektif güvence çalışmasında güven üzerine kuruludur. IIA'nın *Etik Kuralları* iki önemli hususu içine almak için yukarıdaki iç denetim tanımının ötesine uzanır:

1. İç denetim mesleği ve uygulamasıyla ilgili '*İlkeler*',

2. İç denetçilerden beklenen davranış tarzını tanımlayan *Davranış Kuralları*. Bu kuralların amacı, İlkelerin uygulamaya dökülmesi amacıyla yorumlanmasına yardımcı olmak ve iç denetçilerin etik davranışları konusunda rehberlik etmektir.

Etik Kuralları, IIA'nın Meslekî Uygulama Çerçevesi ve ilgili diğer IIA duyurularıyla birlikte, başkalarına hizmet veren iç denetçilere bir kılavuzluk sağlar. "*İç denetçiler*", IIA üyelerini, IIA'nın meslekî sertifikalarına sahip olanları (veya adayları) ve yukarıdaki iç denetim tanımı çerçevesinde iç denetim hizmeti verenleri ifade etmektedir.

## Uygulanabilirlik ve Yürütme

Etik Kuralları, iç denetim hizmeti veren kurum ve kişileri bağlar. IIA üyeleri ve IIA'nın sertifikalarına sahip olanlar (ve adaylar) için bu

kuralların ihlâli, IIA'nın yönetmelikleri ve idarî düzenlemelerine göre değerlendirilir ve ele alınır. Belirli bir davranışa *Davranış Kuralları*nda atıfta bulunulmaması, o davranışın kabul edilemez veya yanlış olarak değerlendirilmesini engellemez ve bu sebeple de söz konusu kişiler disiplin cezası açısından sorumludur.

## İlkeler

İç denetçilerin aşağıdaki ilkeleri uygulamaları ve desteklemeleri beklenir:

1. **Dürüstlük**
   İç denetçilerin dürüstlüğü, *güven* oluşturur ve böylece verdikleri hükümlere itimat edilmesine yönelik bir zemin sağlar.

2. **Objektiflik (Nesnellik)**
   İç denetçiler, inceledikleri süreç veya faaliyet ile ilgili bilgiyi toplarken, değerlendirirken ve raporlarken en üst seviyede meslekî objektiflik sergiler. İç denetçiler ilgili tüm şartların değerlendirmesini dengeli bir şekilde yapar ve kendilerinin veya diğerlerinin menfaatlerinden çok etkilenmez.

3. **Gizlilik**
   İç denetçiler, elde ettikleri bilginin sahipliğine ve değerine saygı gösterir; hukukî ve meslekî bir mecburiyet olmadığı sürece de gerekli yetkilendirmeyi almaksızın bilgiyi açıklamaz.

4. **Yetkinlik (Ehil Olma)**
   İç denetçiler, iç denetim hizmetlerinin gerçekleştirilmesinde gereken bilgi, beceri ve tecrübeyi ortaya koyar.

## Davranış Kuralları

1. **Dürüstlük**
   İç denetçiler,

   1.1.Çalışmalarını doğruluk, dikkat ve sorumluluk duygusuyla yaparlar,

1.2. Hukuku gözetir ve hukukun ve mesleğin gerektirdiği özel durum açıklamalarını yaparlar,

1.3. Kanun dışı bir faaliyete bilerek ve isteyerek taraf olmaz veya iç denetim mesleği ve kurum açısından yüz kızartıcı eylemlere girişmezler,

1.4. Kurumun meşru ve etik amaçlarına saygı duyar, katkıda bulunurlar.

**2. Objektiflik (Nesnellik)**

İç denetçiler,

2.1. Değerlendirmelerinin tarafsızlığına zarar verebilecek veya zarar vereceği varsayılabilecek herhangi bir ilişkiye ve faaliyete katılmazlar; bu katılım, kurumun çıkarlarıyla çatışan ilişki ve faaliyetleri de içerir,

2.2. Meslekî muhakemelerini zayıflatabilecek veya zayıflatacağı varsayılabilecek herhangi bir şeyi kabul etmezler,

2.3. Tespit ettikleri ve açıklanmadığı takdirde faaliyetlerinin raporlanmasını bozacak tüm önemli bulguları açıklarlar.

**3. Gizlilik**

İç denetçiler,

3.1. Görevleri sırasında elde ettikleri bilgilerin korunması ve kullanımı konusunda ihtiyatlı olurlar,

3.2. Sahip oldukları bilgileri kişisel menfaatleri için veya hukuka aykırı olarak veya kurumun meşru ve etik amaçlarına zarar verebilecek tarzda kullanmazlar.

**4. Yetkinlik (Ehil Olma)**

4.1. Sadece görevin gerektirdiği bilgi, beceri ve tecrübeye sahip oldukları işleri üstlenmelidirler,

4.2. İç denetim hizmetlerini, *Uluslararası İç Denetim Standartları*na uygun bir şekilde yerine getirirler,

4.3. Kendi yeterliliklerini ve hizmetlerinin etkinlik ve kalitesini devamlı geliştirirler.

# GİRİŞ

İç denetim faaliyetleri, çok çeşitli hukukî ve kültürel ortamlarda; amacı, boyutu, karmaşıklığı ve yapısı çok farklı kurumlarda, kurum içinden ve dışından kişiler tarafından gerçekleştirilmektedir. Söz konusu farklılıkların, her ortamdaki iç denetim uygulamasını etkilemesine rağmen, iç denetçilerin sorumluluklarının yerine getirilmesi söz konusu olduğunda *Uluslararası İç Denetim Meslekî Uygulama Standartları*'na (kısaca '*Standartlar*' veya 'Uluslararası İç Denetim Standartları') uyum, hayatî önem arz eder. İç denetçilerin *Standartlar*a uyumunun hukuken kısmen engellenmesi durumunda, iç denetçiler *Standartlar*ın diğer kısımlarına uymalı ve uyamadıkları kısımla ilgili olarak özel durum açıklaması yapmalıdır.

*Güvence* hizmetleri, iç denetçinin, bir süreç, sistem veya bir başka konu hakkında bağımsız görüş veya kanaat sunabilmek için, eldeki bulguları objektif bir şekilde değerlendirmesini içerir. Güvence görevlerinin nitelik ve kapsamı iç denetçi tarafından belirlenir. Güvence hizmetlerinin, genellikle, üç tarafı vardır: (1) Süreç, sistem veya ele alınan diğer bir konunun doğrudan içinde olan kişi veya grup (süreç sahibi), (2) Değerlendirmeyi yapan kişi veya grup (iç denetçi), (3) Değerlendirmeyi kullanan kişi veya grup (kullanıcı).

*Danışmanlık* hizmetleri, tabiatı gereği tavsiye niteliğinde olup genellikle görevlendirmeyi talep eden müşterinin özel talebi üzerine gerçekleştirilir. Danışmanlık hizmetlerinin nitelik ve kapsamı, değerlendirmeyi talep eden müşteriyle iç denetçi arasındaki sözleşmeye tabidir. Danışmanlık hizmetlerinin genellikle iki tarafı vardır: (1) Tavsiye veren kişi veya grup (iç denetçi), (2) Tavsiye talep eden ve alan kişi veya grup (görevin müşterisi). İç denetçi danışmanlık hizmeti verirken, objektifliğini muhafaza etmeli ve idarî sorumluluk almamalıdır.

*Standartlar*ın amaçları şunlardır:

1. İç denetim uygulamasını olması gerektiği gibi temsil eden temel ilkeleri tanımlamak.
2. Katma değerli iç denetim faaliyetlerini teşvik etmeye ve hayata geçirmeye yönelik bir çerçeve oluşturmak.
3. İç denetim performansının değerlendirilmesine uygun bir zemin oluşturmak.
4. Gelişmiş kurumsal süreç ve faaliyetleri canlandırmak.

*Standartlar*, Nitelik Standartları, Performans Standartları ve Uygulama Standartlarından müteşekkildir. *Nitelik Standartları*, iç denetim faaliyetlerini yürüten taraf ve kurumların özelliklerine yöneliktir. *Performans Standartları* iç denetim faaliyetlerinin tabiatını açıklar ve bu hizmetlerin performansını değerlendirmekte kullanılan kalite kıstaslarını sağlar. Nitelik ve Performans Standartları tüm iç denetim hizmetlerine uygulanırken, Uygulama Standartları belirli görev türlerine tatbik edilir.

Sadece bir küme Nitelik ve Performans Standartı varken, Uygulama Standartları bir çok kümeden oluşur; iç denetim faaliyetinin her ana türü için bir küme Uygulama Standartı söz konusudur. *Uygulama Standartları* güvence ve danışmanlık faaliyetleri için tesis edilmiştir.

Standartlar, *Meslekî Uygulama Çerçevesi*nin bir parçasıdır. Meslekî Uygulama Çerçevesi, iç denetimin 'tanımını', *Etik Kuralları*'nı, *Standartlar*ı ve diğer kılavuzluk bilgilerini içerir. Standartların nasıl uygulanacağına ilişkin kılavuzluk, *IIA Meslekî Konular Komitesi* tarafından yayınlanan Uygulama Önerilerinde ifadesini bulur.

Standartlarda, özel anlamları *Terimler Sözlüğü*nde verilen terimler kullanılmıştır.

*Standartlar*ın geliştirilmesi ve yayınlanması *devamlı* bir süreçtir. IIA *İç Denetim Standartları Kurulu*, *Standartlar*ı yayınlamadan önce çok

geniş katılımlı bir istişare ve tartışma faaliyetine girişmektedir. Bu çalışma, metin taslağı sürecinde, dünya çapında bir yorum talep etme faaliyetini de içermektedir.

Bütün metin taslakları, hem IIA'nın tüm üye kuruluşlarına gönderilmekte hem de IIA'nın internet sitesinde yayınlanmaktadır. *Standartlar*a ilişkin tavsiye ve yorumlar, aşağıdaki adreslere gönderilebilir:

The Institute of Internal Auditors
Global Practices Center,
Professional Practices Group

247 Maitland Avenue
Altamonte Springs, FL 32701-4201, USA
E-posta: standards@theiia.org
İnternet sitesi: http://www.theiia.org

# NİTELİK STANDARTLARI

**1000 Amaç, Yetki ve Sorumluluklar**
İç denetim faaliyetinin amaç, yetki ve sorumlulukları, *Standartlar*la uyumlu olan ve denetim komitesi ve yönetim kurulunca da onaylanan bir yönetmelikte açıkça tanımlanmalıdır.

**1000.A1** Kuruma sağlanan güvence hizmetlerinin niteliği iç denetim yönetmeliğinde tanımlanmalıdır. Eğer kurum dışından taraflara güvence hizmeti temin edilecekse, bunların niteliği de yönetmelikte tanımlanmalıdır.

**1000.C1** Danışmanlık hizmetlerinin niteliği, iç denetim yönetmeliğinde tanımlanmalıdır.

**1100 Bağımsızlık ve Objektiflik**
İç denetim faaliyeti bağımsız olmalı ve iç denetçiler görevlerini yaparken objektif davranmalıdır.

**1110 Kurum İçi Bağımsızlık**
İç Denetim Yöneticisinin, kurum içinde, iç denetim faaliyetinin sorumluluklarını yerine getirmesine imkân sağlayan bir yönetim kademesine bağlı olması gerekir.

**1110.A1** İç denetim faaliyeti, iç denetimin kapsamının tayin edilmesi, iç denetim işlerinin yapılması ve sonuçların raporlanması konularında her türlü müdahaleden uzak ve serbest olmalıdır.

**1120 Bireysel Objektiflik**
İç denetçilerin tarafsız ve önyargısız bir şekilde davranması ve her türlü çıkar çatışmasından kaçınması gerekir.

**1130 Bağımsızlık veya Objektifliği Bozan Etkenler**
Denetçilerin bağımsızlığı veya objektifliği fiilen bozulduğu veya bozulduğu izlenimi doğduğu takdirde, bozulmanın ayrıntıları ilgili taraflara açıklanmalıdır. Bu açıklamanın kapsamı, bozucu etkenin niteliğine bağlıdır.

**1130.A1** İç denetçiler, daha önceden kendilerinin sorumlu olduğu faaliyetlere ilişkin değerlendirme yapmaktan kaçınmalıdır. Bir iç denetçinin son bir yıl içinde kendisinin sorumlu olduğu bir faaliyet hakkında güvence hizmeti vermesinin, objektifliğini bozacağı varsayılır.

**1130.A2** İç Denetim Yöneticisinin sorumluluğundaki işlevlere yönelik güvence görevleri, iç denetim faaliyeti dışından biri tarafından gözetlenmeli ve kontrol edilmelidir.

**1130.C1** İç denetçiler, daha önce sorumlusu oldukları faaliyetlere ilişkin danışmanlık hizmeti verebilir.

**1130.C2** İç denetçiler, önerilen danışmanlık hizmetleriyle ilgili bağımsızlıklarına ve objektifliklerine zarar verecek hususlar söz konusu ise, görevi kabul etmeden önce denetlenene özel durum açıklaması yapmalıdır.

**1200 Yeterlilik ve Azamî Meslekî Özen ve Dikkat**

Görevlendirmeler, yeterlilik ve azamî meslekî özen ve dikkat ile yerine getirilmelidir.

**1210 Yeterlilik**

İç denetçiler, kişisel olarak, sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer vasıflara sahip olmalıdır. İç denetim faaliyeti de, toplu olarak, kendi sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer vasıflara sahip olmalı veya bunları edinmelidir.

**1210.A1** İç denetim personeli, görevin tamamını veya bir kısmını yapmak için gereken bilgi ve becerilerin veya diğer vasıfların hepsine sahip değilse, İç Denetim Yöneticisi kurum dışındaki uzmanlardan nitelikli tavsiye ve yardım temin etmelidir.

**1210.A2** İç denetçi, suiistimal belirtilerini tesbit edebilecek yeterli bilgiye sahip olmalıdır; fakat esas

görevi ve sorumluluğu suiistimalleri tespit etmek ve soruşturmak olan bir kişinin uzmanlığına sahip olması beklenemez.

**1210.A3** İç denetçiler, verilen görevi yerine getirebilmek için bilgi teknolojileri ve kontrolleriyle ilgili kilit bilgilere ve mevcut teknoloji tabanlı denetim tekniklerine sahip olmalıdır. Ancak, bütün iç denetçilerin, asıl sorumluluğu bilgi teknolojileri denetimi olan denetçiler kadar uzmanlığa sahip olması beklenmez.

**1210.C1** İç Denetim Yöneticisi, iç denetim personelinin görevin kısmen veya tamamen gerçekleştirilmesi için gereken bilgiye, beceriye ve diğer vasıflara sahip olmadığı durumlarda, danışmalık görevini reddetmeli veya yeterli tavsiye ve yardımı temin etmelidir.

**1220 Azamî Meslekî Özen ve Dikkat**

İç denetçiler, makul sınırlar içinde tedbirli ve ehil bir iç denetçiden beklenen beceriye sahip olmalı, azamî özen ve dikkati göstermelidir. Azamî meslekî özen ve dikkat, hiç hatâ yapılmayacağı anlamına gelmez.

**1220.A1** İç denetçi, şunları göz önüne alarak azamî meslekî özen ve dikkat göstermelidir:

- Görevin amaçlarına ulaşmak için gereken çalışmanın kapsamı,
- Güvence prosedürlerinin tatbik edildiği konuların nisbî karmaşıklığı, lüzumu veya önemi
- Risk yönetim, kontrol ve yönetişim süreçlerinin etkinliği ve yeterliliği,
- Önemli hatâ, düzensizlik veya aykırılıkların olma ihtimali,
- Güvence görevinin potansiyel faydalarının maliyeti,

**1220.A2** Azamî meslekî özen ve dikkati gösterirken, iç denetçi, bilgisayar destekli denetim tekniklerini ve diğer veri analiz tekniklerini kullanmayı düşünmelidir.

**1220.A3** İç denetçi, amaçları, faaliyetleri veya kaynakları etkileyebilecek önemli risklere karşı uyanık olmalıdır. Ancak, güvence prosedürleri, azamî meslekî özen ve dikkatle uygulansa bile, bütün önemli risklerin teşhis edilebilmesini garantilemez.

**1220.C1** İç denetçi bir danışmanlık görevi sırasında, aşağıdakileri göz önüne alarak azamî meslekî özen ve dikkat göstermelidir:

- Görev sonuçlarının niteliği, zamanlaması ve raporlanması da dahil denetlenenlerin/müşterilerin ihtiyaç ve beklentileri,
- Görev amaçlarına ulaşabilmek için gerekli çalışmanın boyutu ve nisbî karmaşıklığı,
- Danışmanlık görevinin potansiyel faydalarının maliyeti.

**1230 Sürekli Meslekî Gelişim**

İç denetçiler, mevcut bilgi, beceri ve diğer vasıflarını sürekli meslekî gelişimle artırmalı ve güçlendirmelidir.

**1300 Kalite Güvence ve Geliştirme Programı**

İç denetim yöneticisi, iç denetim faaliyetinin tüm yönlerini kapsayan ve etkinliğini sürekli gözleyen bir kalite güvencesi ve geliştirme programı hazırlamalı ve bunu sürdürmelidir. Bu program, dönemsel iç ve dış kalite değerlendirmelerini ve devamlı iç gözlem faaliyetini içermelidir. Programın her parçası, iç denetim faaliyetinin katma değer yaratmasına, kurumun faaliyetlerinin geliştirilmesine yardımcı olmalı ve iç denetim faaliyetinin *Etik Kuralları*na ve *Standartla*ra uyması konusunda güvence sağlamalıdır.

**1310 Kalite Programı Değerlendirmeleri**

İç denetim bölümü, kalite programının genel etkinliğini gözlemek ve değerlendirmek amacına yönelik bir süreç uygulamalıdır. Bu süreç, hem iç hem de dış değerlendirmeleri içermelidir.

**1311 İç Değerlendirmeler**

İç değerlendirmeler:

- iç denetim faaliyetinin performansının devamlı gözden geçirilmesini,
- özdeğerlendirme (kendi kendini değerlendirme) yoluyla veya kurum içinde, iç denetim uygulamaları ve standartlarını bilen kişilerce yapılan dönemsel gözden geçirmeleri kapsamalıdır.

**1312 Dış Değerlendirmeler**

Dış değerlendirmeler, kurum dışından vasıflı ve bağımsız bir gözden geçirme uzmanı veya ekibi tarafından *en azından beş yılda bir* yapılmalıdır. Dış değerlendirme sıklığının arttırılmasına yönelik potansiyel ihtiyaç, dış gözden geçirme uzmanı veya ekibinin sahip olması gereken vasıflar ve bunların bağımsızlığı meseleleri, menfaat çatışması ihtimali de dikkate alınarak, İç Denetim Yöneticisi ile Yönetim Kurulu ve Denetim Kurulu arasında tartışılmalıdır. Bu tartışmalarda, gözden geçirme görevlisi veya ekibinin tecrübesi değerlendirilirken, kurumun büyüklüğü, karmaşıklığı ve sektörü dikkate alınmalıdır.

**1320 Kalite Programı Hakkında Raporlama**

İç Denetim Yöneticisi, dış değerlendirme sonuçlarını denetim komitesi ve yönetim kuruluna raporlamalıdır.

**1330 "Standartlara Uygun Yapılmıştır" İbaresinin Kullanılması**

İç denetçilerin, faaliyetlerinin "*Uluslararası İç Denetim Meslekî Uygulama Standartlarına uygun yapıldığını*" belirtmeleri teşvik edilir. Ancak iç denetçilerin bu ibareyi kullanabilmesi için, kurumun kalite geliştirme programı hakkındaki değerlendirmelerin, iç denetim faaliyetinin *Standartlar*a uyduğunu göstermesi gerekir.

**1340 Aykırılıkların Açıklanması**

İç denetim faaliyetinin *Standartlar*a, iç denetçilerin *Etik Kuralları*na tam uyumu gerçekleştirmesi gerekmekle birlikte, tam uyumun sağlanamadığı durumlar da olabilir. Aykırılıklar, iç denetim faaliyetinin genel kapsamını veya faaliyetlerini etkiler hâle geldiğinde, üst yönetime, denetim komitesine ve yönetim kuruluna özel durum açıklaması yapılmalıdır.

# PERFORMANS STANDARTLARI

**2000 İç Denetim Faaliyetinin Yönetimi**
İç Denetim Yöneticisi, iç denetim faaliyetini, faaliyetin kuruma değer katmasını sağlayacak etkili bir tarzda yönetmelidir.

**2010 Planlama**
İç Denetim Yöneticisi, kurumun hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen risk esaslı planlar yapmalıdır.

**2010.A1** İç denetim faaliyetinin görev planı, en az yılda bir kez yapılan bir risk değerlendirmesine dayanmalıdır. Üst yönetim, denetim komitesi ve yönetim kurulunun fikri, bu sürece dahil edilerek göz önüne alınmalıdır.

**2010.C1** İç denetim yöneticisi, görevin risk yönetimini geliştirme, katma değer yaratma ve faaliyetleri geliştirme potansiyelini değerlendirerek, öne sürülen danışmanlık görevlerini kabul etmeyi düşünmelidir. Kabul edilen bu görevler, plana dahil edilmelidir.

**2020 Bildirim ve Onay**
İç Denetim Yöneticisi, önemli ara değişiklikler de dahil, iç denetim faaliyetinin planlarını ve kaynak ihtiyaçlarını, gözden geçirme ve onay için üst yönetime, denetim komitesine ve yönetim kuruluna bildirmelidir. İç Denetim Yöneticisi, kaynak sınırlamalarının etkilerini de bildirmelidir.

**2030 Kaynak Yönetimi**
İç Denetim Yöneticisi, onaylı planın uygulanabilmesi için, iç denetim kaynaklarının uygun ve yeterli olmasını ve etkin bir şekilde kullanılmasını sağlamalıdır.

**2040 Politika ve Prosedürler**
İç Denetim Yöneticisi, iç denetim faaliyetini yönlendirmek amacına yönelik politika ve prosedürleri belirlemelidir.

**2050 Eşgüdüm**

İç Denetim Yöneticisi; aynı çalışmaların gereksiz yere tekrarlanmasını asgarîye indirmek ve işin kapsamını en uygun şekilde belirlemek amacıyla, ilgili güvence ve danışmanlık hizmetlerini yerine getiren diğer iç ve dış sağlayıcılarla, mevcut bilgileri paylaşmalı ve faaliyetleri bunlarla eşgüdüm içinde sürdürmelidir.

**2060 Yönetim Kurulu, Denetim Kurulu ve Üst Yönetime Raporlamalar**

İç Denetim Yöneticisi, iç denetim faaliyetinin amacı, yetkileri, görev ve sorumlulukları ve plana kıyasla performansı konularında, denetim komitesi ve yönetim kuruluna ve üst yönetime dönemsel raporlar sunmalıdır. Bu raporlar, önemli riskleri, kontrol sorunlarını, kurumsal yönetişim sorunlarını ve denetim komitesinin, yönetim kurulunun ve üst yönetimin ihtiyaç duyabileceği veya talep edebileceği başka konuları da içermelidir.

**2100 İşin Niteliği**

İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**2110 Risk Yönetimi**

İç denetim faaliyeti; önemli risk maruziyetlerini tespit edip değerlendirerek ve risk yönetimi ve kontrol sistemlerinin iyileştirilmesine katkıda bulunarak kuruma yardımcı olmalıdır.

**2110.A1** İç denetim faaliyeti kurumun risk yönetim sisteminin etkinliğini gözlemeli ve değerlendirmelidir.

**2110.A2** İç denetim faaliyeti, aşağıdakileri dikkate alarak, kurumun yönetişim, kontrol, faaliyet ve bilgi sistemlerinin maruz olduğu riskleri değerlendirmelidir:

- Mali ve operasyonel bilgilerin güvenilirliği ve bütünlüğü,
- Faaliyetlerin etkinlik ve verimliliği,
- Varlıkların korunması,
- Kanun, düzenleme ve sözleşmelere uyum.

**2110.C1** İç denetçiler, danışmanlık görevleri sırasında, görevin amaçlarıyla uyumlu şekilde riski ele almalı ve diğer önemli risklere karşı uyanık olmalıdır.

**2110.C2** İç denetçiler, danışmanlık görevlerinden elde ettikleri risk bilgilerini, kurumun maruz kaldığı önemli riskleri belirleme ve değerlendirme sürecinde kullanmalıdır.

**2120 Kontrol**

İç denetim faaliyeti, kontrollerin etkinlik ve verimliliğini değerlendirmek ve sürekli gelişimi teşvik etmek suretiyle, kurumun etkin kontrollere sahip olmasına yardımcı olmalıdır.

**2120.A1** Risk değerlendirmesinin sonuçlarına bağlı olarak, iç denetim faaliyeti, kurumun yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayan kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir. Bu değerlendirme:

- mali ve operasyonel bilgilerin güvenilirliğini,
- faaliyetlerin etkinlik ve verimlililiğini,
- varlıkların korunmasını,
- kanunlara, düzenlemelere ve sözleşmelere uyum konularını kapsamalıdır.

**2120.A2** İç denetçiler, faaliyet ve programların hedef ve amaçlarının kapsamını ve bunların kurumun hedef ve amaçlarına uyumunun derecesini anlayıp değerlendirmelidir.

**2120.A3** İç denetçiler, faaliyet ve programların niyetlenildiği gibi uygulandığını veya gerçekleştirildiğini belirlemek için, faaliyet ve programların tesbit edilen hedef ve amaçlarla

ne kadar uyumlu olduğunu anlayıp değerlendirebilmek için, faaliyet ve programları gözden geçirmelidir.

**2120.A4** Kontrollerin değerlendirilmesi için uygun ve yeterli kıstaslara ihtiyaç vardır. İç denetçiler, yönetimin hedef ve amaçlara ulaşılıp ulaşılmadığını belirlemek için oluşturduğu kıstasların yeterlilik derecesini tespit etmelidir. Bu kıstaslar yeterliyse, iç denetçiler de kendi değerlendirmelerinde bunları kullanabilir. Kıstaslar yeterli değilse, iç denetçiler uygun değerlendirme kıstasları geliştirmek için yönetimle birlikte çalışmalıdır.

**2120.C1** Danışmanlık görevleri sırasında, iç denetçiler, görevin amaçlarıyla uyumlu bir şekilde kontrolleri ele almalı ve herhangi bir kontrol zaafiyetine karşı uyanık olmalıdır.

**2120.C2** İç denetçiler, danışmanlık görevlerinden elde ettikleri kontrol bilgilerini, kurumun maruz kaldığı önemli riskleri belirleme ve değerlendirme sürecinde kullanmalıdır.

**2130 Yönetişim**

İç denetim faaliyeti, aşağıdaki amaçların gerçekleştirilmesi amacıyla yönetişim sürecinin iyileştirilmesi için gerekli tavsiyelerde bulunmalı ve tavsiyeleri değerlendirmelidir:

- Kurum içinde gerekli etik ve diğer değerlerin geliştirilmesi,
- Etkili bir kurumsal performans yönetimi ve hesap verebilirlik,
- Risk ve kontrol bilgilerinin kurumun gerekli alanlarına etkili bir şekilde iletilmesi,
- Yönetim kurulunun, denetim kurulunun, iç ve dış denetçilerin ve üst yönetimin faaliyetleri arasında eşgüdüm sağlamak ve bunlar arasında gerekli bilgilerin etkili bir şekilde iletimini sağlamak.

**2130.A1** İç denetim faaliyeti, kurumun etikle ilgili amaç, program ve faaliyetlerinin tasarımını, uygulanmasını ve etkinliğini değerlendirmelidir.

**2130.C1** Danışmanlık görevinin amaçları, kurumun genel değerleri ve hedefleriyle uyumlu olmalıdır.

**2200 Görev Planlaması**

İç denetçiler, her görev için, kapsam, amaçlar, zamanlama ve kaynak dağılımı hususlarını da dikkate alan ayrı bir plan hazırlamalı ve kaydetmelidir.

**2201 Planlamada Dikkate Alınması Gerekenler**

Bir görevi planlarken, iç denetçiler şu noktaları dikkate almalıdır:

- Denetlenecek olan faaliyetin hedefleri ve faaliyetin kendi performansını kontrol etmesinin araçları,
- Faaliyet ve hedeflerine, kaynaklarına ve operasyonlarına yönelik önemli riskler ve bu potansiyel risklerin etki veya ihtimallerini kabul edilebilir bir seviyede tutmanın yol ve araçları,
- Faaliyetin risk yönetimi ve kontrol sistemlerinde önemli gelişme sağlama imkânları.

**2201.A1** Kurum dışındaki taraflar için bir görevlendirme planlarken, iç denetçiler, görevlendirmenin amaçları, kapsamı, her iki tarafın sorumlulukları ve -görev kayıtlarına erişime ve sonuçların dağıtımına getirilecek kısıtlamalar dahil- diğer karşılıklı beklentiler konusunda söz konusu taraflarla yazılı bir anlaşma yapmalıdır.

**2201.C1** İç denetçiler, görevlendirmenin amaçları, kapsamı, yerine getirilecek sorumluluklar ve diğer müşteri beklentileri hakkında, danışmanlık hizmeti verecekleri müşterileriyle anlaşmalıdır. Çok önemli görevlendirmelerde bu anlaşma yazılı hâle getirilmelidir.

**2210 Görev Amaçları**

Görev amaçları, denetlenen faaliyetle ilgili riskleri, kontrolleri ve yönetişim süreçlerini kapsamalıdır.

**2210.A1** İç denetçi, denetlenen faaliyetle ilgili risklerin ön değerlendirmesini yapmalıdır. Görevin amaçları, bu risk değerlendirmesinin sonuçlarını yansıtmalıdır.

**2210.A2** İç denetçiler, görevin amaçlarını belirlerken, önemli hatâların, düzensizliklerin, aykırılıkların ve diğer risklerin meydana gelme ihtimalini göz önüne almalıdır.

**2210.C1** Danışmanlık görevlerinin amaçlarında, müşteriyle mutabık kalındığı ölçüde, risk, kontrol ve yönetişim süreçlerine de temas edilmelidir.

**2220 Görev Kapsamı**

Görevin kapsamı, görevin amaçlarına ulaşılmasına yetecek seviyede olmalıdır.

**2220.A1** Görevin kapsamı, üçüncü tarafların sahip oldukları dahil, ilgili sistemlerin, kayıtların, personel ve maddî varlıkların değerlendirilmesini de içermelidir.

**2220.A2** Bir güvence görevi sırasında önemli danışmanlık fırsatları çıkarsa, görevin amaçları, kapsamı, karşılıklı sorumluluklar ve diğer beklentilerle ilgili yazılı bir anlaşma hazırlanmalı ve danışmanlık görevinin sonuçları, danışmanlık standartlarına uygun olarak raporlanmalıdır.

**2220.C1** İç denetçiler, danışmanlık görevlerini yaparken, görevin kapsamının, üzerinde mutabık kalınan amaçlara yeterince temas ettiğinden emin olmalıdır. Eğer görev sırasında kapsamla ilgili ihtirazî kayıtları olursa, göreve devam edip etmeyeceğini belirlemek üzere, bunları müşteri ile tartışmalıdır.

**2230 Görev Kaynaklarının Tahsisi**
İç denetçiler, görevin amaçlarına ulaşmak için gereken kaynakları tespit etmelidir. Görev kadrosu, görevin niteliği, karmaşıklığı, zaman kısıtlamaları ve mevcut kaynaklar dikkate alınarak teşkil edilmelidir.

**2240 Görev İş Programı**
İç denetçiler, görev amaçlarına yönelik iş programları hazırlamalıdır. Bu iş programları, kayıtlı hâle getirilmelidir.

**2240.A1** İş programları, görev sırasında uygulanacak bilgi toplama, analiz, değerlendirme ve kayıt prosedürlerini içermeli ve göstermelidir. İş programı, *işe başlanmadan önce* onaylanmalıdır; programda yapılan değişiklikler için de derhal onay alınmalıdır.

**2240.C1** Danışmanlık görevleri için hazırlanan iş programlarının şekli ve içeriği, görevin niteliğine bağlı olarak değişir.

**2300 Görevin Yapılması**
İç denetçiler, üstlendikleri görevin hedeflerine ulaşmak için yeterli bilgileri belirlemeli, analiz etmeli, değerlendirmeli ve kaydetmelidir.

**2310 Bilgilerin Tespiti ve Tanımlanması**
İç denetçiler, görev amaçlarına ulaşmak için yeterli, güvenilir, ilgili ve faydalı olan bilgileri tespit etmeli ve tanımlamalıdır.

**2320 Analiz ve Değerlendirme**
İç denetçiler, vardıkları sonuçları ve görev sonuçlarını uygun analiz ve değerlendirmelere dayandırmalıdır.

**2330 Bilgilerin Kaydedilmesi**
İç denetçiler, vardıkları kanaatlere ve görev sonuçlarına dayanak teşkil eden bütün bilgileri kaydetmelidir.

**2330.A1** İç Denetim Yöneticisi, görev kayıtlarına erişimi kontrol etmelidir. İç Denetim Yöneticisi, gerektiğinde,

bu kayıtları kurum dışı taraflara vermeden önce, üst yönetimin ve/veya hukuk danışmanının onayını almalıdır.

**2330.A2** İç Denetim Yöneticisi, görev kayıtlarının saklanmasına ilişkin esasları belirlemelidir. Bu esaslar, kurumun temel ilkelerine ve ilgili mevzuata uygun olmalıdır.

**2330.C1** İç denetim yöneticileri, görev kayıtlarının tutulması, saklanması ve kurum içi ve dışı taraflara sunulmasını düzenleyen politikalar belirlemelidir. Bu politikalar, kurumun düzenlemelerine, ilgili mevzuata ve diğer gereklere uygun olmalıdır.

**2340 Görevin Gözetim ve Kontrolü**

Görevler; görev amaçlarına ulaşılmasını, kalitenin güvence altına alınmasını ve personelin geliştirilmesini sağlayacak bir tarzda gözetlenmeli ve kontrol edilmelidir.

## 2400 Sonuçların Raporlanması

İç denetçilerin, görev sonuçlarını raporlaması gerekir.

**2410 Raporlama Kıstasları**

Raporlamalar, varılan sonuçlar, yapılan tavsiyeler ve önerilen eylem planlarının yanında görevin hedeflerini ve kapsamını da içermelidir.

**2410.A1** Sonuçları gösteren nihaî rapor, gerektiğinde, iç denetçinin görüş ve kanaatlerini de içermelidir.

**2410.A2** İç denetçiler, görev raporlamalarında tatminkâr bir performans göstermeye teşvik edilmelidir.

**2410.A3** Görev sonuçları kurum dışındaki taraflara bildirilirken, söz konusu bildirim, sonuçların dağıtımı ve kullanımı konusundaki sınırlamaları da içermelidir.

**2410.C1** İlerlemenin raporlanmasının ve danışmanlık görevlerinin sonuçları, görevlendirmenin niteliğine ve

müşterinin ihtiyaçlarına bağlı olarak, şekil ve içerik değiştirir.

**2420 Raporlamaların Kalitesi**
Raporlamalar, doğru, objektif, açık, özlü, yapıcı, tam olmalı ve zamanında sunulmalıdır.

**2421 Hatâ ve Eksiklikler**
Eğer nihaî raporlama önemli bir hatâ veya eksiklik içeriyorsa, İç Denetim Yöneticisi, hatâlı ve eksik raporu alan bütün taraflara düzeltilmiş bilgileri iletmelidir.

**2430 Görevlendirmelerde Standartlara Aykırılıkların Açıklanması**
*Standartlar*a aykırılıklar belli bir görevi etkilediğinde, sonuçlar raporlanırken şu hususlar özel durum olarak açıklanmalıdır:

- Tam olarak uyulamayan *Standart(lar)*
- Aykırılık sebepleri
- Aykırılığın göreve etkisi

**2440 Sonuçların Raporlanması**
İç Denetim Yöneticisi, görev sonuçlarını *uygun taraflara* raporlamalıdır.

**2440.A1** Görev sonuçlarının öngördüğü tedbirlerin alınmasını sağlayabilecek *taraflara*, nihaî görev sonuçlarının raporlanmasından İç Denetim Yöneticisi sorumludur.

**2440.A2** İç Denetim Yöneticisi, aksi kanunî, hukukî düzenlemelerle emredilmediği takdirde, görev sonuçlarını kurum dışındaki taraflara iletmeden önce, kuruma doğabilecek muhtemel riskleri değerlendirmeli, üst yönetim ve/veya hukuk danışmanı ile istişare etmeli ve sonuçların raporlanmasını, kullanımını kısıtlayarak, kontrol etmelidir.

**2440.C1** İç Denetim Yöneticisi, danışmanlık görevlerinin nihaî sonuçlarının müşterilere raporlanmasından sorumludur.

**2440.C2** Danışmanlık görevleri sırasında, risk yönetimi, kontrol ve yönetişim sorunları tesbit edilebilir. Bu sorunlar, kurum için önemli hâle gelir gelmez üst yönetime, denetim komitesine ve yönetim kuruluna bildirilmelidir.

**2500 İlerlemenin Gözlenmesi**

İç Denetim Yöneticisi, yönetime rapor edilen sonuçların akıbetinin gözlenmesi için bir sistem kurmalı ve uygulamalıdır.

**2500.A1** İç Denetim Yöneticisi, yönetimin aldığı tedbirlerin etkili bir şekilde uygulanmasını veya üst yönetimin, gerekli tedbiri almamasının riskini üstlenmeyi kabul etmesini sağlamak ve gelişmeleri gözlemek amacına yönelik bir takip süreci kurmalıdır.

**2500.C1** İç denetim faaliyeti, müşterileriyle mutabık kalındığı ölçüde, danışmanlık görevlerinin sonuçlarının akıbetini gözlemelidir.

**2600 Yönetimin Artık (Bakiye) Riskleri Üstlenmesi**

İç Denetim Yöneticisi, üst yönetimin kurum için kabul edilemeyebilecek bir artık (bakiye) risk düzeyini üstlenmeyi kabul ettiğine inandığı takdirde, konuyu üst yönetimle tartışmalıdır. Artık riskle ilgili bir karara varılamazsa, İç Denetim Yöneticisi ve üst yönetim, konuyu çözümlenmesi için denetim komitesi ve yönetim kuruluna rapor etmelidir.

# TERİMLER SÖZLÜĞÜ

Standartlar ve Uygulama Önerilerinde yer alan bazı terimler aşağıda açıklandığı anlamlarıyla kullanılmıştır.

**Artık/Bakiye Riskler (Residual Risks)**
Yönetimin, olumsuz bir olayın etki ve ihtimalini azaltmak amacıyla, riski karşılamaya yönelik kontrol faaliyetleri de dahil, aldığı tedbirlerden sonra kalan risktir.

**Bağımsızlık (Independence)**
Objektifliği veya objektiflik görüntüsünü bozabilecek şartların dışında olmaktır. Objektifliğe yönelik bu tür tehditlerle, kişisel olarak denetçi, görev, işlev ve kurum seviyesinde mücadele edilmelidir.

**Danışmanlık Hizmetleri (Consulting Services)**
Her hangi bir idarî sorumluluk üstlenmeden, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı müşteri/denetlenen ile birlikte kararlaştırılan istişarî faaliyetler ve bunlarla bağlantılı diğer hizmetlerdir. Usul ve yol göstermek, tavsiyede bulunmak, işleri kolaylaştırmak ve eğitim vermek, bu kapsamdaki faaliyet örnekleridir.

**Değer Katmak (Add Value)**
Değer, güvence ve danışmanlık hizmetleri yoluyla, kurumun amaçlarını gerçekleştirme fırsatlarını geliştirerek, faaliyetleri geliştirme imkânlarını belirleyerek ve/veya riske maruz kalmasını azaltarak sağlanır.

**Denetim Komitesi (Audit Committee)**
Denetim Komitesi, Türk Ticaret Kanunu'ndaki 'Denetim Kurulu'ndan farklı olup yönetim kurulunun komitelerinden biridir. Aslî işlevi, muhasebe, denetim, iç kontrol sistemi ve mali raporlama uygulamaları ile ilgili olarak yönetim kuruluna gözetim görevinde yardımcı olmaktır.

Yönetim kurulunun onayına bağlı olarak, denetim komitesi denetim kurulunun mali konularda bilgili bağımsız üyelerinden oluşur. (Ç.N.)

**Dış Hizmet Sağlayıcısı/Taşeron (External Service Provider)**
Belli bir alanda uzmanlık seviyesinde bilgi, beceri ve tecrübe sahibi olan kurum dışından kişi veya şirketlerdir.

**Etik Kuralları (Code of Ethics)**
Uluslararası İç Denetçiler Enstitüsü (IIA)'nün Etik Kuralları, iç denetim mesleği ve uygulamasıyla ilgili *İlkeler* ve iç denetçilerden beklenen davranış tarzını tanımlayan *Davranış Kuralları*dır. Etik Kuralları iç denetim hizmeti veren tüm kurum ve kişileri bağlar. Bu kuralların amacı, evrensel anlamda iç denetim mesleğinin etik kültürünü geliştirmektir.

**Görev (Engagement)**
İç denetim, kontrol özdeğerlendirme incelemesi, suiistimal incelemesi veya danışmanlık gibi belirli iç denetim işi, vazifesi veya gözden geçirme faaliyetidir. Bir görev, çok sayıda işten veya belirli amaçlara ulaşmayı amaçlayan faaliyetlerden oluşabilir.

**Görev Amaçları (Engagement Objectives)**
İç denetçi tarafından geliştirilen, niyetlenilen görev amaçlarını tanımlayan geniş ifadelerdir.

**Görev İş Programı (Engagement Work Program)**
Görev planını gerçekleştirmeye yönelik hazırlanan ve bir görev sırasında takip edilmesi gereken prosedürleri sıralayan bir belgedir.

**Güvence Hizmetleri (Assurance Services)**
Kurumun risk yönetimi, kontrol ve yönetişim süreçlerine dair bağımsız bir değerlendirme sağlamak amacıyla bulguların objektif bir şekilde incelenmesidir. Mali yapıya, performansa, mevzuat ve düzenlemelere uyuma, bilgi sistemleri güvenliğine ve ihtimam denetimine (due diligence; ayrıntılı durum tespit çalışması) yönelik görevler bu

kapsamdaki örneklerdir.

**İç Denetim Faaliyeti/Birimi (Internal Audit Activity)**
Kurumun faaliyetlerini geliştirmek ve bunlara değer katmak için tasarlanan bağımsız, objektif güvence ve danışmanlık hizmeti sağlayan birim, bölüm, danışman ekibi veya diğer uygulamacılardır. İç denetim faaliyeti, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.

**İç Denetim Yöneticisi (Chief Audit Executive)**
İç denetim faaliyetlerinden en üst seviyede sorumlu olan kişidir. Normal şartlar altında, bu iç denetim müdürüdür. İç denetim faaliyetlerinin kurum dışındaki hizmet sağlayıcılardan temin edildiği durumda, hizmet sözleşmesini ve söz konusu faaliyetlerin tüm kalite güvence çalışmalarını gözeten, iç denetim faaliyetleriyle ilgili üst yönetime, denetim komitesine ve yönetim kuruluna raporlama yapan ve görev sonuçlarının takibini yürüten kişidir. Terim, ayrıca, genel denetçi, baş iç denetçi ve genel müfettiş gibi unvanları da içine alır.

**İhlâller/Sakatlamalar (Impairments)**
Bireysel objektifliği ve kurum içi bağımsızlığı bozabilecek ihlâller, şahsî menfaat çatışmalarını, kapsam sınırlamalarını, kayıtlara, personele ve eşyalara erişim kısıtlamalarını ve kaynak (fonlama) kısıtlamalarını içerir.

**Kontrol (Control)**
*Kontrol*, yönetimin, denetim kurulunun, yönetim kurulunun ve diğer uygun birimlerin riski yönetmek ve belirlenen amaç ve hedeflere ulaşma ihtimalini artırmak amacıyla aldığı tedbirlerdir. Yönetim, hedef ve amaçların gerçekleştirilmesine yönelik makul bir güvence sağlamak için yeterli tedbirin alınmasını planlar, tertipler ve yönlendirir.

**Kontrol Ortamı (Control Environment)**
Yönetim, yönetim kurulu ve denetim kurulunun, kurum içi kontrolün önemine ilişkin tutum ve davranışlarıdır. Kontrol ortamı, iç kontrol sisteminin ana amaçlarının gerçekleştirilmesi için gerekli olan yapı ve disiplini sağlar. Kontrol ortamı aşağıdaki unsurları içerir:

- Dürüstlük ve etik değerler
- Yönetimin felsefesi ve çalışma tarzı
- Teşkilât yapısı
- Yetki ve sorumluluk dağıtımı
- İnsan kaynakları politikası ve uygulaması
- Çalışanların yetkinliği

**Kontrol Süreçleri (Control Processes)**
Riskin, risk yönetim süreçleriyle belirlenen risk toleransları içinde kalmasını temin gayesiyle tasarlanan kontrol çerçevesinin bir parçası olan faaliyet, politika ve prosedürlerdir.

**Kurul (Board)**
Kurul; yönetim kurulu, denetim kurulu, hukuk bölümünün başı, kâr amaçlı olmayan kurumların mütevelli heyeti veya İç Denetim Yöneticisinin işlevsel olarak bağlı bulunduğu denetim komitesi de dahil kurumun atanan diğer birimleri gibi kurumun yönetim mercilerini ifade eder.

**Menfaat/Çıkar Çatışması (Conflict of Interest)**
Kurumun çıkarına olmayan veya menfaatine görünmeyen herhangi bir ilişkidir. Menfaat çatışması, kişinin sorumluluklarını ve görevlerini objektif bir şekilde yerine getirmesini olumsuz etkiler.

**Objektiflik/Nesnellik (Objectivity)**
Objektiflik, iç denetçilerin görevlerini, iş sonucunda çıkan ürüne

gerçekten ve dürüst bir şekilde inanacakları ve bu ürünün kalitesinden önemli bir taviz vermeyecekleri şekilde yapmalarını sağlayan tarafsız bir zihinsel tutumdur. Objektiflik, iç denetçilerin, denetim konularına ilişkin karar ve yargılarını, başkalarınınkilere bağlamamalarını gerektirir.

**Risk (Risk)**
Amaçlara ulaşılması üzerinde etkisi olacak bir olayın meydana gelme ihtimalidir. Risk, etki ve olasılık cinsinden hesaplanır.

**Risk Yönetimi (Risk Management)**
Kurumun amaçlarını gerçekleştirmek üzere makul bir güvence sağlamak amacıyla potansiyel olay ve durumları belirlemek, değerlendirmek, yönetmek ve kontrol etme sürecidir.

**Standart (Standard)**
Geniş bir iç denetim faaliyet sahasının gerçekleştirilmesiyle ve iç denetim performansının değerlendirilmesiyle ilgili gerekleri tanımlayan ve *IIA İç Denetim Standartları Kurulu* tarafından yayınlanan meslekî bir beyandır.

**Suiistimal (Fraud)**
Hile, sahtekârlık, emniyeti kötüye kullanma ile nitelendirilebilecek hukuk dışı fiillerdir. Bu fiiller, sadece şiddet tehdidi veya fizikî güç kullanımının gerçekleştirilmesine bağlı değildir. Suiistimaller para, mal veya hizmet sağlamak, hizmet kaybından veya ödeme yapmaktan kaçınmak veya şahsıyla veya işle ilgili bir avantaj elde etmek amaçlarıyla çeşitli *taraflar* ve kurumlar tarafından gerçekleştirilebilir.

**Uyum/Uygunluk (Compliance)**
Plan, prosedür, kanun, düzenleme, sözleşme ve diğer gereklere riayet ve bağlılıktır.

**Yeterli Kontrol (Adequate Control)**
Yeterli kontrol, yönetimin planlama ve organizasyonu, risklerin etkin bir şekilde yönetileceğine ve kurumun hedef ve amaçlarına verimli ve ekonomik bir şekilde ulaşılacağına dair makul bir güvence sağlayacak tarzda yapmasıyla var olabilir.

**Yönetişim/Kurumsal Yönetim (Governance)**
Üst yönetim, yönetim kurulu ve denetim kurulu tarafından, kurumun amaçlarına ulaşmaya yönelik olarak, kurumun faaliyetlerinin yönlendirilmesi, yönetilmesi ve gözlenmesi gayesiyle uygulanan yapı ve süreçlerin bir birleşimidir.

**Yönetmelik (Charter)**
İç denetim faaliyetinin yönetmeliği, faaliyetin amaç, yetki ve sorumluluklarını tanımlayan resmî nitelikte yazılı bir belgedir. Yönetmelik (a) iç denetim faaliyetinin kurum içindeki konumunu belirlemeli, (b) denetim görevlerinin yerine getirilmesi için gereken kayıtlara, personele, demirbaşlara ve ilgili mahallere erişim yetkisini düzenlemeli ve (c) iç denetim faaliyetlerinin kapsamını tanımlamalıdır.

# UYGULAMA ÖNERİLERİ

# Uygulama Önerisi 1000-1: İç Denetim Yönetmeliği

Uluslararası İç Denetim Standartlarından
Standart 1000'in Yorumu

## İlgili Standart

**1000 Amaç, Yetki ve Sorumluluklar**
İç denetim faaliyetinin amaç, yetki ve sorumlulukları, *Standartlar*la uyumlu olan ve denetim komitesi ve yönetim kurulu tarafından da onaylanan bir yönetmelikte açıkça tanımlanmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler bir iç denetim yönetmeliği hazırlarken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun, bir yönetmelik hazırlanırken dikkate alınması gereken hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetim faaliyetinin amaç, yetki ve sorumlulukları bir yönetmelikte tanımlanmalıdır. İç Denetim Yöneticisi, yönetmeliğin üst yönetimin onayından geçirilmesini ve denetim komitesi ve yönetim kurulu tarafından benimsenmesini sağlamalıdır. Yönetmeliğin onaylandığı, denetim komitesi ve yönetim kurulunun tutanaklarına geçirilmelidir. Yönetmelik (a) iç denetim faaliyetinin kurum içindeki konumunu belirlemeli; (b) denetim görevlerinin yerine getirilmesi için gereken kayıtlara, personele, demirbaşlara ve ilgili mahallere erişim yetkisini düzenlemeli ve (c) iç denetim faaliyetlerinin kapsamını tanımlamalıdır.

2. İç denetim faaliyetinin yönetmeliği *yazılı* olmalıdır. Yönetmeliğin yazılı olması, yönetimin gözden geçirme ve onayı ve denetim komitesi ve yönetim kurulunun kabulü için resmî bir zemin oluşturur. Yönetmelik, iç denetim faaliyetinin amaç, yetki ve sorumluluklarının yeterliliğinin dönemsel olarak değerlendirilmesini

de kolaylaştırır. İç denetim faaliyetinin yönetmeliği de içeren resmî ve yazılı bir belgeye sahip olması, kurum içinde denetim işlevinin yönetilmesi için hayatî öneme sahiptir. İç denetim faaliyetinin rol, işlev ve görevlerini belirlemek ve üst yönetime, denetim komitesine ve yönetim kuruluna bu iç denetim faaliyetinin çalışmalarını değerlendirmek için bir temel oluşturmak amacıyla, iç denetim faaliyetinin *amaç, yetki* ve *sorumlulukları* tanımlanmalı ve açıklanmalıdır. Herhangi bir sorunun ortaya çıkması hâlinde, yönetmelik, iç denetim faaliyetinin kurum içindeki görev ve sorumlulukları hakkında üst yönetim, denetim komitesi ve yönetim kuruluyla yapılmış resmî ve yazılı bir anlaşma işlevini de görür.

3. İç Denetim Yöneticisi, yönetmelikte açıklanan ve tanımlanan amaç, yetki ve sorumlulukların iç denetim faaliyetinin hedeflerine ulaşması için yeterli olmaya devam edip etmediğini dönemsel olarak değerlendirmeli ve incelemelidir. Bu dönemsel değerlendirmenin sonuçları da üst yönetime, denetim komitesine ve yönetim kuruluna bildirilmelidir.

# Uygulama Önerisi 1000.C1-1: İç Denetçilerce Danışmanlık Faaliyetlerinin Yürütülmesine İlişkin İlkeler

Uluslararası İç Denetim Standartlarından
Standart 1000.C1'in Yorumu

## İlgili Standart

**1000.C1** Danışmanlık hizmetlerinin niteliği, iç denetim yönetmeliğinde tanımlanmalıdır.

***Bu Uygulama Önerisinin Niteliği:*** *İç denetimin tanımı şöyledir: "İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur." İç denetçiler, iç denetçilerle ilgili 'nitelik ve performans standartları'nın hem güvence hem de danışmanlık işlev ve görevlerini kapsadığını unutmamalıdır.*

*Bu Uygulama Önerisi, bütün danışmanlık görevlerinde dikkate alınması gereken geniş kapsamlı parametreler üzerinde durmakta ve odaklanmaktadır. Danışmanlık işlevi; yazılı anlaşmalarla tanımlanan resmî görevlerden daimî veya geçici yönetim komitelerinde veya proje ekiplerinde yer almak gibi danışmanlık hizmet ve faaliyetlerine kadar farklı ve değişik kapsamlarda olabilir. İç denetçilerden, bu Uygulama Önerisindeki tavsiyelerin, karşılaştıkları her farklı durumda, ne ölçüde uygulanabileceğini belirlemek için, meslekî muhakemelerini kullanmaları beklenir. Zira, bir birleşme veya devralma projesine veya felâket sonrası toparlanma (disaster recovery activities) benzeri âcil durum görevlendirmelerine katılmak gibi istisnaî danışmanlık görevleri, normal prosedürlerden ayrılmayı gerekli kılabilir.*

*İç denetçiler, danışmanlık görevlerini yerine getirirken aşağıdaki yol gösterici ilkeleri gözönüne almalıdır. Bu kılavuzun, bir danışmanlık görevinin yapılmasında gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur. İç denetçiler, kurum yönetiminin, denetim komitesinin ve yönetim kurulunun, danışmanlık*

*hizmetlerinin yürütülmesi için gereken kavramları, işletme ilkelerini ve raporlamaları anladığından ve kabul ettiğinden emin olmak için ek tedbirler almalıdır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. **İç Denetimin Katma Değeri:** İç denetim, kurumun kültürüne ve kaynaklarına uygun bir şekilde ve tarzda iç denetçiler çalıştıran her kurumda, katma değer sağlar. İç denetim faaliyetinin tanımında da saklı olan bu katma değer düşüncesi, yönetişim, risk ve kontrol alanlarında getirdiği sistemli ve disiplinli yaklaşımla kuruma değer katacak biçimde tasarlanmış *güvence* ve *danışmanlık* faaliyetlerini de içine alır.

2. **İç Denetimin Tanımına Uygunluk:** Disiplinli ve sistemli bir değerlendirme yöntemi, her iç denetim faaliyetinin parçasıdır. Hizmetlerin listesi, genel olarak, güvence ve danışmanlığın geniş sınıflandırmasına dahil edilebilir. Ancak bu hizmetler, iç denetimin geniş tanımıyla uyumlu olan katma değer sağlayıcı hizmetlerin yeni gelişen biçimlerini de içerebilir.

3. **Güvence ve Danışmanlığın Ötesindeki Denetim Faaliyetleri:** Çok sayıda iç denetim hizmeti vardır. Güvence ve danışmanlık hizmetleri, birbirlerini tamamlayıcı oldukları gibi araştırma ve denetim-dışı görevler gibi başka denetim hizmetlerini de engellemez. Pek çok denetim hizmetinin hem güvence hem de danışmanlık rolü vardır.

4. **Güvence ve Danışmanlık Arasındaki İlişki:** Danışmanlık hizmetleri, iç denetimin katma değer sağlayıcı yönünü zenginleştirir. Danışmanlık hizmeti genellikle güvence hizmetlerinin doğrudan sonucu olmakla birlikte, güvence işlevinin danışmanlık görevlerinden çıkabileceği de kabul edilmelidir.

5. **İç Denetim Yönetmeliğiyle Danışmanlık Yetkisinin Verilmesi:** İç denetçiler, geleneksel olarak, geliştirilmekte olan sistemlerdeki

kontrolleri ve güvenlik ürünlerini analiz etmek, faaliyetleri analiz etmek ve tavsiyelerde bulunmak amacıyla görev gruplarında yer almak ve benzeri görevlere kadar pek çok farklı türde danışmanlık hizmeti verir. Yönetim kurulu (veya denetim komitesi), denetim komitesine karşı olan yükümlülüklerine aykırı olmaması veya çıkar çatışması yaratmaması kaydıyla, iç denetim faaliyetine, ek bazı görevler yapma yetkisini de vermelidir. Bu yetkinin de iç denetim yönetmeliğinde açıkça gösterilmesi gerekir.

6. **Objektiflik (Nesnellik):** Danışmanlık hizmeti, denetçinin güvence göreviyle bağlantılı iş süreçlerini veya sorunlarını daha iyi anlamasını sağlayabilir; bunun, denetçinin veya iç denetim faaliyetinin objektifliğini mutlaka bozacağı iddia edilemez. İç denetimin, *idarî bir karar alma* işlevi yoktur; iç denetimin, danışmanlık hizmeti sonucunda önerdiği tavsiyeleri uygulama kararı, ancak kurumun yöneticileri tarafından alınabilir. Bu nedenle, kurum yönetiminin aldığı kararların, iç denetimin objektifliğini bozmaması gerekir.

7. **İç Denetimin Danışmanlık Hizmetine Sağladığı Zemin:** Verilen danışmanlık hizmetlerinin çoğu, güvence ve araştırma hizmetlerinin doğal bir uzantısıdır ve gayriresmî veya resmî öneri, analiz veya değerlendirmeleri içerebilir. İç denetim faaliyeti, (a) en yüksek objektiflik standartları ve ilkelerine bağlılığı, (b) kurumun süreçleri, riskleri ve stratejileri hakkında sahip olduğu geniş bilgi temeli sayesinde, bu tür danışmanlık işlerini yapmak hususunda istisnaî bir konuma sahiptir.

8. **Temel Bilgilerin İletilmesi:** İç denetimin kuruma kazandırdığı temel değerlerden biri de, üst yönetime ve denetim komitesi üyelerine güvence sağlamaktır. Danışmanlık görevi, İç Denetim Yöneticisinin (İDY) kanaatiyle, görüş ve inancına göre kurumun üst düzey yöneticilerine ve yönetim kurulu üyelerine sunulması gereken bilgileri gizleyen bir tarzda yürütülmemelidir. Danışmanlık

hizmet ve görevlerinin hepsi, bu ilkenin ışığında benimsenmeli ve uygulanmalıdır.

9. **Danışmanlık İlkeleri Kurum Çapında Anlaşılmalıdır:** Kurumların danışmanlık işlevlerinin ve hizmetlerinin yürütülmesine zemin oluşturan ve kurumun bütün çalışanları tarafından anlaşılan *temel kuralları* bulunmalıdır. Bu kurallar, iç denetim yönetmeliğinde belirtilmeli ve tüm kuruma ilân edilmelidir.

10. **Resmî Danışmanlık Görevleri:** Yönetim, önemli ve uzun bir süreyle devam eden resmî danışmanlık görevleri için genellikle dış danışmanlar tutar. Ancak bir kurum, bazı resmî danışmanlık işleri ve görevleri için kendi iç denetim birimini yetkin ve uygun görebilir. Kurumun kendi iç denetim birimi, resmî bir danışmanlık görevi üstlendiği takdirde, bu görevi, sistemli ve disiplinli bir yaklaşım ile yerine getirmelidir.

11. **İç Denetim Yöneticisinin Sorumlulukları:** Danışmanlık hizmetleri, İç Denetim Yöneticisinin belirli yönetim sorunlarını ele almak ve çözümlemek amacıyla yönetimle diyaloga girmesine olanak sağlar. Bu diyalogda, görevin kapsamı, zamanlaması ve programı, yönetimin ihtiyaç ve isteklerine uygun hâle getirilir. Ancak, elde edilen sonuçların niteliği ve ehemmiyeti, kurum açısından önemli risklere işaret ediyorsa, denetim tekniklerini belirleme imtiyazı ve kurumun üst düzey yöneticilerine ve denetim komitesi üyelerine raporlama hakkı İç Denetim Yöneticisine aittir.

12. **İhtilâfların veya Sorunların Çözüm Kıstasları:** Bir iç denetçi, her şeyden önce bir iç denetçidir. Dolayısıyla, bütün hizmet ve görevlerinin ifasında, iç denetçi, IIA *Etik Kurallarını ve Uluslararası İç Denetim Standartları*ndan *Nitelik* ve *Performans* Standartlarını kendine rehber edinmelidir. Öngörülemeyen ihtilâf veya faaliyetler, bu *Etik Kurallarına* ve *Standartla*ra uygun bir şekilde çözümlenmelidir.

# Uygulama Önerisi 1000.C1-2: Resmî Danışmanlık Görevlerine İlişkin Ek Hususlar

Uluslararası İç Denetim Standartlarından Standart 1000.C1'in
(Ve İlgili Diğer Danışmanlık Uygulama Standartlarının) Yorumu

## İlgili Standart

**1000.C1** Danışmanlık hizmetlerinin niteliği, iç denetim yönetmeliğinde tanımlanmalıdır.

Bu Uygulama Önerisi ve ilgili Standartlara ilişkin özel not: Bu Uygulama Önerisi, birden fazla *Danışmanlık Uygulama Standardına* ilişkin yol gösterici ilkeleri içermektedir. Bu ilkeler, *Standart* 1000.C1'in yanı sıra, 1130.C1 ve C2; 1210. C1; 1220.C1; 2010.C1; 2110.C1 ve C2; 2120.C1 ve C2; 2130.C1; 2201.C1; 2210.C1; 2220.C1; 2240.C1; 2330.C1; 2410.C1; 2440.C1 ve C2 ve 2500.C1 standartlarını da kapsamaktadır. Sayılan bu standartlara yapılan atıflar, bu Uygulama Önerisinin başlıklarında parantez içinde gösterilmektedir.

**Bu Uygulama Önerisinin Niteliği:** *Bu Uygulama Önerisi, özü itibariyle, Danışmanlık Hizmetlerinin Yürütülmesine İlişkin İlkeler'in ele alındığı ve tartışıldığı 1000.C1-1 sayılı uygulama önerisine benzemektedir. Danışmanlık faaliyetlerinin yürütülmesinde her ikisi de iç denetçiler için faydalıdır. İç denetimin tanımı şöyledir: "İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur." İç denetçiler, iç denetçilerle ilgili 'Nitelik ve Performans Standartları'nın hem güvence hem de danışmanlık işlev ve görevlerini kapsadığını unutmamalıdır.*

*Bu uygulama önerisi, bütün danışmanlık görevlerinde dikkate alınması gereken geniş kapsamlı parametreler üzerinde durmakta ve odaklanmaktadır. Danışmanlık işlevi; yazılı anlaşmalarla tanımlanan resmî görevlerden daimî veya geçici yönetim komiteleri veya proje ekiplerinde yer almak gibi danışmanlık hizmet ve etkinliklerine kadar farklı ve değişik kapsamlarda olabilir. İç denetçilerden, bu Uygulama*

*Önerisindeki tavsiyelerin, karşılaştıkları her farklı durumda, ne ölçüde uygulanabileceğini belirlemek için, meslekî muhakemelerini kullanmaları beklenir. Zira, bir birleşme veya devralma projesine veya felâket sonrası toparlanma benzeri (disaster recovery activities) âcil durum görevlendirmelerine katılmak gibi istisnaî danışmanlık görevleri, normal prosedürlerden ayrılmayı gerekli kılabilir.*

*İç denetçiler, danışmanlık görevlerini yerine getirirken aşağıdaki yol gösterici ilkeleri göz önüne almalıdır. Bu kılavuzun, bir danışmanlık görevinin yapılmasında gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur. İç denetçiler, kurum yönetiminin, denetim komitesinin ve yönetim kurulunun danışmanlık hizmetlerinin yürütülmesi için gereken kavramları, işletme ilkelerini ve raporlamaları anladığından ve kabul ettiğinden emin olmak için ek tedbirler almalıdır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

## Danışmanlık Hizmetlerinin Tanımı

1. *Standartlar*da bulunan terimler sözlüğünde, "*danışmanlık hizmetleri*" şöyle tanımlanmaktadır: "Her hangi bir idarî sorumluluk üstlenmeden, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı müşteri/denetlenen ile birlikte kararlaştırılan istişarî faaliyetler ve bunlarla bağlantılı diğer hizmetlerdir. Usul ve yol göstermek, tavsiyede bulunmak, işleri kolaylaştırmak ve eğitim vermek, bu kapsamdaki faaliyet örnekleridir."

2. İç Denetim Yöneticisi, kurum içindeki görevlerin sınıflandırılmasında kullanılacak yöntemi belirlemelidir. Bazı durumlarda, danışmanlık ve güvence faaliyetlerinin unsurlarını birleştiren bir yaklaşımla "*karma*" bir görevlendirme yapmak da uygun olabilir. Bazen ise, görevin güvence ve danışmanlık unsurlarını birbirinden ayırmak, daha uygun olabilir.

3. İç denetçiler, danışmanlık hizmetlerini normal veya rutin çalışmalarının bir parçası olarak ya da kurum yönetiminin talepleri üzerine yürütebilir. Her kurum, yapılacak danışmanlık faaliyetlerinin türünü göz önünde bulundurmalı ve her tür için ayrı bir politika

veya prosedür gerekip gerekmediğinin kararını vermelidir. Muhtemel görev sınıflamaları arasında şunlar sayılabilir:

- *Resmî danışmanlık görevleri:* Planlanmış ve yazılı bir anlaşmaya tâbi olan görevler.

- *Gayriresmî danışmanlık görevleri:* Daimî komitelere katılmak, sınırlı süreli projeler, belli bir proje veya amaca yönelik (ad-hoc) toplantılar ve olağan bilgi alışverişi gibi rutin faaliyetler.

- *Özel danışmanlık görevleri:* Bir birleşme ve devralma ekibine ya da sistem dönüştürme ekibine katılmak.

- *Âcil durum danışmanlık görevleri:* Bir felâket veya olağanüstü nitelikte başka bir olay sonrasında, faaliyetlerin sürdürülmesi veya toparlanması amacıyla kurulan bir ekibe katılmak ya da özel bir talebi karşılamaya veya âcil bir işi yetiştirmeye yardımcı olmak için, geçici yardım vermek amacıyla kurulmuş bir ekibe katılmak.

4. Denetçilerin, ilke olarak, bir *güvence* görevi olarak yürütülmesi daha uygun olan bir hizmetin, *danışmanlık* hizmeti olarak ele alınmasını temin etmek amacıyla, bu hizmetin güvence hizmeti olarak ele alınmasını gerektiren hususların saklanmasına yardımcı olmamaları gerekir. Ancak bu, güvence görevi olarak yapıla gelmekte olan olan hizmetlerin, artık danışmanlık görevi olarak yapılmasının daha uygun olduğuna kanaat getirildiği bir durumda, yöntemde gerekli ayarlamanın yapılmasına da mâni değildir.

## Danışmanlık Görevlerinde Bağımsızlık ve Objektiflik (Standart 1130.C1)

5. İç denetçilerden, bazen, daha önce sorumlu oldukları ya da güvence hizmeti verdikleri faaliyetlerle ilgili danışmanlık hizmeti talep

edilir. Bu tür bir danışmanlık hizmeti vermeden önce, İç Denetim Yöneticisi, denetim komitesinin danışmanlık hizmeti verme kavramını anlayıp anlamadığını ve buna onay verip vermediğini tespit ve teyit etmelidir. Bu onay verildikten sonra, iç denetim yönetmeliğinde değişiklik yapılmalı, danışmanlık hizmetleri ile ilgili yetki ve sorumluluklar da tüzüğe dahil edilmeli ve iç denetim faaliyeti sonucunda, bu tür faaliyetlerin yürütülmesi için uygun politika ve prosedürler geliştirilmelidir.

6. İç denetçiler, hüküm verirken ve yönetime tavsiyelerde bulunurken objektifliklerini korumalıdır. Danışmanlık görevine başlamadan önce, bu bağımsızlık veya objektifliği bozabilecek şartlar mevcutsa veya görev sırasında ortaya çıkarsa, bunların yönetime derhal bildirilmesi gerekir.

7. Bir resmî danışmanlık görevinden sonra *bir yıl içinde* güvence hizmeti verildiği takdirde bağımsızlık ve objektiflik bozulabilir. Hizmetlerin her biri için ayrı denetçiler görevlendirilerek, bağımsız gözetim ve kontrol kanalları kurularak, projelerin sonuçları için ayrı sorumluluklar tespit edilerek ve varsayılan bozulma açıklanarak, bu bozulmanın etkilerini asgarî düzeye indirmek amacına yönelik adımlar atılmalıdır. İlgili tavsiyeleri kabul etmekten ve uygulamaktan, yönetim sorumlu olmalıdır.

8. İç denetçilerin, ilgili görevin başlangıcında belirlenen kapsam ve amaçta yeri olmayan bir *yönetim sorumluluğunu*, uygunsuz veya kasıtsız olarak *üstlenmelerini* engellemek amacıyla, özellikle, niteliği gereği devamlı veya kesintisiz olan danışmanlık görevlerinde çok dikkat edilmelidir.

## Danışmanlık Görevlerinde Azamî Meslekî Özen ve Dikkat (1210.C1, 1220.C1, 2130.C1 ve 2201.C1 Sayılı Standartlar)

9. İç denetçiler, bir resmî danışmanlık görevi yaparken, özellikle

aşağıdakileri anlamalı ve azamî meslekî özen ve dikkati göstermelidir:

- Görev sonuçlarının niteliğine, zamanlamasına ve raporlanmasına yönelik yöneticilerin talep ve öncelikleri,
- Hizmeti talep edenlerin, taleplerinin ardındaki sebep ve saikler,
- Amaca ulaşmak için gereken işlerin kapsam ve niteliği,
- Görev için gereken beceri ve kaynaklar,
- Denetim komitesinin daha önce onayladığı denetim planının kapsamına etkisi,
- Gelecekteki denetim görevleri ve taahhütleri üzerindeki muhtemel etkileri,
- Kurumun bu görevden elde edebileceği yararlar.

10. Yukarıda açıklanan bağımsızlık ve objektiflik değerlendirmesine ve gereken meslekî özen ve dikkate ilişkin düşüncelere ek olarak, iç denetçi şu hususları da dikkate almalıdır:
    - Verilecek hizmetin niteliğini ve kapsamını tespit etmek ve değerlendirmek amacıyla uygun toplantılar düzenlemek ve gereken bilgileri toplamak.
    - Hizmeti alanların, iç denetim yönetmeliğinde açıklanan ilgili ilkeleri, iç denetim faaliyetlerinin politika ve prosedürlerini ve danışmanlık görevlerinin yerine getirilmesiyle ilgili başka yol gösterici ilkeleri anlayıp anlamadıklarını ve bunları kabul edip etmediklerini tespit ve teyit etmek. İç denetçi, iç denetim yönetmeliğinin yasakladığı, iç denetim faaliyetlerinin politika ve prosedürlerine aykırı olan ya da ilgili kurumun çıkarlarına uygun olmayan ve ilgili kuruma değer katmayan danışmanlık görevlerini üstlenmeyi ve yapmayı reddetmelidir.
    - Danışmanlık görevinin iç denetim faaliyetleriyle ilgili genel görev planına uygunluğunu değerlendirmek. İç denetim faaliyetine ilişkin *risk esaslı görev planı*, kurumun ihtiyaç

duyduğu denetim kapsamını sağlamak amacıyla, uygun olduğu ölçüde, danışmanlık görevlerini de içerebilir ve bunlara da dayanabilir.

- Resmî danışmanlık görevinin genel unsurlarını, yorum esaslarını, sonuçta elde edilebilecekleri ve diğer temel etkenleri yazılı bir anlaşma veya plana kaydetmek. Hem iç denetçinin hem de danışmanlık hizmetini alanların ilgili raporlama ve iletişim gereklerini bilmesi, anlaması ve kabul etmesi çok önemlidir.

## Danışmanlık Görevlerinde İşin Kapsamı
**(2010.C1, 2110.C1 ve C2, 2120.C1 ve C2, 2201.C1, 2210.C1, 2220.C1, 2240.C1 ve 2440.C2 Sayılı Standartlar)**

11. Yukarıda belirtildiği gibi, iç denetçiler, hizmeti alanlarla, danışmanlık görevinin hedefleri ve kapsamı hakkında bir anlayış birliğine varmalıdır. Danışmanlık görevinin değeri, faydaları veya muhtemel olumsuz etkilerine ilişkin çekincelerin hizmeti alanlara bildirilmesi gerekir. İç denetçiler, üstlendikleri işin kapsamını, iç denetim faaliyetinin profesyonelliğini, dürüstlüğünü, itibarını ve ismini koruyacak bir şekilde tespit etmeli ve tasarlamalıdır.

12. Resmî danışmanlık görevlerinin planlanması aşamasında, iç denetçiler, hizmetin hedeflerini, bu hizmetleri alan yönetim yetkililerinin uygun istek ve ihtiyaçlarına yanıt verecek şekilde belirlemeli ve tasarlamalıdır. Yönetimin özel taleplerde bulunması hâlinde, hedeflenmesi gereken amaçların yönetimin özel taleplerinin ötesinde olduğuna inandıkları takdirde, iç denetçilerce, aşağıdaki eylemler düşünülebilir:

    - Yönetimi, danışmanlık görevinin kapsamına ek hedef ve amaçlar ilâve etmek konusunda ikna etmek,
    - Hedeflere ulaşılamaması hâlinde durumu tespit etmek ve bu gözlemini danışmanlık görevi sonuçlarına ilişkin son raporunda açıklamak,

- Hedefleri ayrı ve daha sonraki bir güvence görevinin kapsamına almak.

13. Resmî danışmanlık görevlerinin iş programları, hem görevin kapsamını ve hedeflerini hem de bu hedeflere ulaşmak için kullanılacak yöntemi tanımlamalı ve içermelidir. Programın şekli ve içeriği, görevin niteliğine bağlı olarak değişebilir. Görev kapsamının belirlenmesinde, iç denetçiler, bu görevin kapsamını, yönetimin taleplerine göre genişletebilir ya da sınırlandırabilir. Ancak iç denetçi, projelendirilen iş kapsamının görevin hedeflerine ulaşmak için yeterli ve uygun olduğundan emin olmalıdır. Görevin hedefleri, kapsamı ve koşulları işin devamı sırasında, dönemsel olarak yeniden gözden geçirilmeli ve gerekiyorsa ayarlamaya tâbi tutulmalıdır.

14. İç denetçiler, resmî danışmanlık görevleri sırasında uygulanan risk yönetimi ve kontrol süreçlerinin verimliliğini izlemeli ve bu konuda dikkatli olmalıdır. Tespit edilen büyük risk ve risk maruziyetleri veya önemli kontrol zayıflıkları, yönetimin dikkatine sunulmalı ve rapor edilmelidir. Bazı durumlarda, denetçinin kaygılarının da üst yönetime, denetim komitesine ve/veya yönetim kuruluna bildirilmesi gerekir. İç denetçiler (a) risklerin, zayıflıkların önem düzeyini ve bunları azaltmak veya düzeltmek için alınan veya alınması öngörülen tedbirleri tespit etmek için ve (b) bu risklerin veya zayıflıkların rapor edilmesi konusunda, üst yönetim, denetim komitesi ve yönetim kurulunun beklentilerini araştırıp bulmak için meslekî muhakemelerini kullanmalıdır.

## Danışmanlık Görevlerinin Sonuçlarının Rapor Edilmesi (2410.C1 ve 2440.C1 Sayılı Standartlar)

15. Danışmanlık görevlerine ilişkin ilerleme ve sonuç raporlarının şekli ve içeriği, görevin niteliğine ve denetlenenin ihtiyaçlarına bağlı olarak değişir. Raporlama gerekleri, genellikle, danışmanlık hizmetini *talep eden* kişiler tarafından tespit edilir ve bu gereklerin yönetimle birlikte tesbit edilen ve kararlaştırılan hedeflere uygun

olması gerekir. Bununla birlikte, danışmanlık görevi sonuçlarının raporlama formatında, hem görevin niteliğini hem de bu bilgileri kullananların bilmesi gereken *sınırlamalar, kısıtlamalar* veya diğer etkenler açıkça gösterilmeli ve tanımlanmalıdır.

16. Bazı durumlarda, iç denetçi, görev sonuçlarının sadece hizmeti alan veya talep edenlere değil başka kişilere de rapor edilmesi gerektiğine hükmedebilir. Bu durumlarda iç denetçi görev sonuçlarının uygun kişi ve taraflara bildirilmesini sağlayacak şekilde raporlama kapsamını genişletmelidir. Raporlama kapsamının başka tarafları da kapsayacak şekilde genişletilmesinde, denetçi, sonuçtan ve çözümden tatmin olana kadar aşağıdakileri yapmalı ve uygulamalıdır:

    - İlk olarak, danışmanlık görevine ilişkin anlaşmada ve ilgili bildirimlerde hangi yönün gösterildiğini ve nelerin istendiğini tespit etmek,
    - İkinci olarak, hizmeti alanları veya talep edenleri, raporlama kapsamını başka uygun kişi ve tarafları da kapsayacak şekilde, gönüllü olarak genişletmeye ikna etmek,
    - Üçüncü olarak, iç denetim yönetmeliğinde veya denetim faaliyeti politika ve prosedürlerinde danışmanlık görevi sonuç raporları hakkında öngörülen ilkeleri tespit etmek,
    - Dördüncü olarak, ilgili kurumun *Davranış Kuralları, Etik Kuralları* ve ilgili diğer politikaları, idarî yönetmelikleri veya prosedürlerinde öngörülen ilke ve kuralları tespit etmek,
    - Beşinci olarak, *IIA Standartları ve Etik Kuralları*nda, denetçiyle ilgili diğer standartlarda, kurallarda, denetim konusuna ilişkin kanunlarda ve mevzuatta öngörülen ilke ve kuralları tespit etmek,

17. İç denetçiler, iç denetim faaliyetlerine ilişkin diğer raporlarla birlikte, resmî danışmanlık görevlerinin niteliği, kapsamı ve genel sonuçlarını da ilgili kurumun yönetimine, denetim komitesine ve

yönetim kuruluna veya başka yönetim birimlerine açıklamalı ve bildirmelidir. İç denetçiler, üst yönetimi ve denetim kurulunu, denetim kaynaklarının nasıl kullanıldığı hakkında sürekli bilgilendirmelidir. Bu danışmanlık görevlerinin ayrıntılı raporlarının ya da özel sonuçların ve tavsiyelerin rapor edilmesine gerek yoktur. Fakat bu görev türlerinin uygun bir tanımının ve önemli tavsiyelerin raporlanması gerekir ve iç denetçilerin *2060 sayılı Standarta (Denetim Komitesine, Yönetim Kuruluna ve Üst Yönetime Raporlama)* uyma sorumluluğunun yerine getirilmesi için bu raporlama şarttır.

## Danışmanlık Görevleri İçin Kayda Geçirme Gerekleri (Standart 2330.C1)

18. İç denetçiler, üstlendikleri resmî danışmanlık görevinin hedeflerine ulaşmak ve sonuçlarına destek olmak amacıyla yaptıkları işleri kaydetmelidir. Ancak, güvence görevleri için geçerli kayıt zorunlulukların, mutlaka danışmanlık görevlerine de uygulanması gerekmez.

19. Kayıtlara ulaşma talepleri hakkında muhtemel yanlış anlamalardan kaçınmak ve ilgili kurumu yeterince korumak amacıyla, denetçilerin uygun kayıt tutma politikalarına uymaları ve danışmanlık görevi kayıtlarının sahipliği gibi sorunlara dikkat etmeleri teşvik edilir. Hukukî davalar, mevzuata uyum sorunları, vergi sorunları ve muhasebe sorunları gibi durumlarda, belirli danışmanlık görevi kayıtlarına özel dikkat ve özen gösterilmesi gerekebilir.

## Danışmanlık Görevlerinin Gözlenmesi (Standart 2500.C1)

20. İç denetim faaliyeti, denetlenenle kararlaştırılan sınırlar içinde, danışmanlık görevlerinin sonuçlarını gözlemi de kapsamalıdır. Farklı türlerde danışmanlık görevleri için farklı gözlem yöntemleri

gerekebilir. Bu gözlem çabaları; yönetimin danışmanlık görevine açık ilgisi ya da iç denetçinin projenin riskleri veya kuruma kattığı değerle ilgili değerlendirmesi gibi etkenlere bağlı olabilir.

# Uygulama Önerisi 1000.C1-3 İdarî Kurumsal Düzenlemelerdeki Danışmanlık Görevlerine İlişkin Ek Hususlar

Uluslararası İç Denetim Standartlarından
Standart 1000.C1'in (ve ilgili diğer Danışmanlık Uygulama Standartlarının) Yorumu

## İlgili Standart

**1000.C1** Danışmanlık hizmetlerinin niteliği, iç denetim yönetmeliğinde tanımlanmalıdır.

***Bu Uygulama Önerisinin Niteliği:*** *Bu Uygulama Önerisi, özü itibariyle, Danışmanlık Hizmetlerinin Yürütülmesine İlişkin İlkeler'in ele alındığı ve tartışıldığı 1000.C1-1 ve C1-2 sayılı uygulama önerilerine benzemektedir. Danışmanlık faaliyetlerinin yürütülmesinde her ikisi de denetçiler için faydalıdır. İç denetim tanımı şöyledir: "İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur." İç denetçiler, iç denetçilerle ilgili Nitelik ve Performans Standartları'nın hem güvence hem de danışmanlık işlev ve görevlerini kapsadığını unutmamalıdır.*

*Bu Danışmanlık Önerisi, IIA Standartlarına uygun faaliyet gösteren ancak yerel yönetişim kuralları, denetim standart, politika ve/veya düzenlemelerini güvence harici (danışmanlık) hizmetleri konusunda daha sıkı bir şekilde sınırlayan idari denetim kurumları için kılavuzluk sağlamaktadır. Güvence harici (danışmanlık) hizmeti vermeyi planlayan bir kurumun parametreleri, iç denetim yönetmeliğinde belirtilmeli ve iç denetim faaliyetlerinin politika ve prosedürlerince de desteklenmelidir. Bu Uygulama Önerisi'nde gösterilen yöntemler, danışmanlık hizmetlerini yönetmede ilgili dil ve politikalar üretmede kuruma yardımcı olabilir.*

*İç denetçilerden, bu uygulama önerisindeki tavsiyelerin, karşılaştıkları her farklı durumda, ne ölçüde uygulanabileceğini belirlemek için, meslekî muhakemelerini kullanmaları beklenir. İç denetçiler, danışmanlık görevlerini yerine getirirken aşağıdaki yol gösterici ilkeleri göz önüne almalıdırlar.*

1. **Arkaplan:** IIA, danışmanlık hizmetlerini şu şekilde tanımlamaktadır: "İç denetçinin her hangi bir idarî sorumluluk üstlenmeden, bir kurumun yönetişim, risk yönetim ve kontrol süreçlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı müşteri ile birlikte kararlaştırılan danışmanlık ve bununla bağlantılı müşteri hizmet faaliyetleridir. Usûl ve yol göstermek, tavsiyede bulunmak, işleri kolaylaştırmak ve eğitim vermek bu kapsamdaki faaliyet örnekleridir."

2. **Denetçilerin Rollerinin Temel Unsurları:** Güvence (denetim) faaliyetleri süresince, denetçiler, yönetimin kurumsal hedeflere ulaşmasına ve faaliyet ve işlerin nasıl yürütüldüğüne dair iç ve dış gereklerle uyum içinde bulunmasına yardımcı olmalıdırlar. Bütün bu faaliyetler, gelişmek için yapılan tavsiyeleri içeren yardım boyutunu kapsasa da, denetçi, operasyonel gelişmenin uygulanması veya onaylanmasında nihai sorumluluğu üstlenmez. Faaliyetlerin uygulanması veya onaylanmasında denetçiler sorumluluk alırsa, ister denetim (güvence) sırasında tavsiye edilmiş olsun ister denetim dışı (danışmanlık) ayrı bir faaliyet olsun, denetçi, denetim rolü için gerekli olan bağımsızlık ve objektifliği büyük ihtimalle tehlikeye atmaktadır.

   Bir kuruma, denetim dışı (danışmanlık) faaliyetleri ile yardımcı olurken bile, denetçiler faaliyetlerini, denetim faaliyetlerinin özünde tanımlanmış sınırlar içinde tutmalıdırlar. Bu faaliyetlerin özünde şunlar vardır:

   Denetçiler, bağımsız olmalı ve denetçilerin objektifliği ile ters düşen ilişki ve durumlardan kaçınmalıdırlar.[1]

   Denetçiler kendi işlerini denetlememelidirler.[1]

   Denetçiler, yönetimle ilgili faaliyetlerde bulunmamalı ve yönetimle ilgili kararlar vermemelidirler.[1]

[1] Bu ilke, birçok kural koyucu kuruluş tarafından dile getirilmiştir. Bunlara, IAASB/IFAC'nin hazırladığı Meslekî Etik Yönetmeliği ve ABD Yönetim Güvenirlik Bürosu'nun Genel Kabul Görmüş Yönetim Denetleme Standartları da dahildir.

Bunlar, işin özünü oluşturan özelliklerdir, çünkü denetimin temel değerlerini yani, yönetimin iddialarının güvenilirliğini sınayan (veya güvence teşkil eden) tarafsız üçüncü parti prensibini desteklemektedir. Buna göre, güvence sağlama becerilerini korumak için, denetçiler, aynı denetim faaliyeti danışmanlık hizmeti de verirken ortaya çıkabilecek olan denetçilerin bağımsızlıklarına karşı muhtemel tehditleri en aza indirmelidirler.

Yukarıdaki temel unsurlara ek olarak, denetim dışı (danışmanlık) işi de dahil olmak üzere, denetçilerin bağımsızlığına karşı diğer tehditler:

karşılıklı menfaat yaratır; veya denetçiyi şirketin avukatı haline getirir.[2]

3. **Yönetim Kuralları**: Denetçinin, denetim (güvence) rolü dışındaki işlerine sınırlama getiren özel yetki gerektiren kurallar, sadece dış (finansal yönetim veya yasal) denetim yapan denetçilere veya her tip denetimi yapan denetçilere uygulanabilir. Ayrıca, bu kurallar gözetim veya denetim kurumları tarafından empoze edilen denetim faaliyetinin kurallarında yer almış olabilir, veya özel kurumların veya bölgelerin denetimleri için gereken denetim standartları veya etik kurallara eklenebilir. [3] Denetim faaliyetinin yönetmeliğinin, politika ve prosedürlerinin, ilgili yönetim kuralları ile uyumlu olmasını sağlamak Başdenetçinin sorumluluğundadır.

Denetim faaliyetinin, denetim dışı (danışmanlık) hizmetlerini sınırlayan yönetim kurallarına tabi olmadığı yerlerde bile,

[2] Bu risk, Mali Raporlandırma Konseyi'nce atanan ve ICAEW (İngiltere ve Galler İmtiyazlı Muhasebeciler Enstitüsü) tarafından yayınlanan Denetim Komiteleri ve Birleşik Yönetmelik Kılavuzu ile ilgili Aralık 2003 Smith Raporu'nda ortaya çıkmıştır.

[3] Özel sınırlandırmalara verilebilecek örnekler arasında, İngiliz Kamu İç Denetim Standartları 2.4.2 de vardır. Şuna değinmektedir: Objektifliğin, bireysel denetçilerin, daha önceden yönetim sorumluluğu taşıdıkları veya danışmanlık görevi yaptıkları bir faaliyeti gözden geçirdiklerinde bozulduğuna inanılmaktadır. Bu standart, 'Danışmanlığa Dair Örnek Uygulama Kılavuzu'nda ek olarak verilmekte ve şu belirtilmektedir: Bu rolde, iç denetçinin yönetime önerilerde bulunması ve yönetim adına bir görev üstlenmemesi önemlidir. İç denetçi tarafından yapılan önerinin yönetim tarafından kabul edilmesi, kendi sorumluluk alanlarında yönetimin güvenilirliğini azaltmayacaktır. (3.5.3)

Başdenetçilerin, denetçilerin bağımsızlık ve objektifliğine karşı olabilecek tehditleri yönetmek veya en aza indirmek için tasarlanmış kalite güvence sistemini sağlama almaları gerekecektir. Aksi takdirde, denetim dışı (danışmanlık) görevlerinin, denetim görevinin denetim (güvence) faaliyetlerini yerine getirmesini tehlikeye atmasında uzun süreli etkileri olabilecektir. Ayrıca, bağımsızlığı tehlikeye sokan denetim dışı (danışmanlık) işindeki bir denetim faaliyeti, diğer denetçilerin, denetim faaliyetine güvenmelerini engelleyecektir.

4. **Objektiflik veya Bağımsızlığı Tehlikeye Sokan Faaliyetler:** Denetçinin, bağımsızlığını tehlikeye sokmadan, denetim dışı (danışmanlık) işinde bulunması, tavsiye anlamında yardım etme veya danışmanlık ile öneri verme ve yönetimin sorumluluğunda olan işi yapmaya yardım etme arasındaki çizgiyi nerede çektiğine bağlıdır. Örneğin, sistem tasarımı sırasında, yönetimin bunları kabul veya reddedeceğini bilerek belli kontrollerle ilgili önerilerde bulunmak, gelecekte söz konusu sisteme yönelik denetçinin objektifliği üzerinde sınırlı bir etki yaratacaktır. Diğer taraftan, eğer denetçi, sistem tasarım takımını idare ederse, hangi kontrollerin seçileceğine karar verirse veya tavsiye edilen kontrollerin uygulamasını teftiş ederse, sistemin gelecekte denetçi tarafında objektif bir şekilde değerlendirilmesi zorlaşacaktır. Ancak diğer denetim dışı görevler, bu kadar belirgin olmayabilir. Buna göre, denetim görevleri, muhtemel danışmanlık (denetim dışı) görevlerini gözden geçirmek ve bunların bağımsızlık veya objektifliğe karşı bir tehdit oluşturup oluşturmadığını ortaya çıkarmak için prosedürler geliştirmelidir. Gelecekteki bağımsızlık ve objektiflik üzerindeki etkilerini ortaya çıkarmak için yapılan gözden geçirmeler belgelenmelidir. Bu belgeler, QAR görevi sırasında dış kalite kontrol gözden geçirme uzmanlarına verilmelidir.

5. **Objektiflik veya Bağımsızlığa Karşı Tehditlerin En Aza İndirilmesi Süreçleri:** Denetim görevi, danışmanlık görevlerindeki

bireysel denetçilerin objektifliğini veya denetim faaliyetinin tamamının bağımsızlığını tehlike sokacak potansiyeli azaltan kontrolleri uygulamaya sokmalıdır. Bu teknikler şunlardır:

a. Denetim dışı (danışmanlık) hizmeti parametrelerini tanımlayan yönetim dili.

b. Denetim dışı (danışmanlık) projelerinde yer alma seviyesini, tipini ve özelliğini sınırlayan politika ve prosedürler.

c. Objektifliği tehdit edebilecek görevleri kabul etmede sınırlamalar getirerek, denetim dışı (danışmanlık) projelerinde bir ön görüşme sürecini kullanmak.

d. Aynı denetim görevi içindeki denetim dışı (danışmanlık) birimlerini, denetim (güvence hizmetleri) yapan birimlerden ayırmak.

e. Görevdeki denetçilerin sıra ile görev yapması.

f. Denetim dışı (danışmanlık) görevlerinde veya denetim fonksiyonunun daha önce denetim dışı (danışmanlık) görevinde bulunmasından dolayı objektifliğe/bağımsızlığa zarar verdiğine kanaat getirilen güvence hizmetleri denetiminde dış tedarikçileri çalıştırmak.

g. Önceki bir denetim dışı (danışmanlık) projesinde yer alarak objektifliğin zedelendiğine dair raporların ifşa edilmesi. Ek A'da bu tip kontrol teknikleri için ilgili dil örnekleri verilmektedir.

## Ek A
## Denetçi Bağımsızlığına Karşı Tehditleri En Aza İndiren Kontrol Tekniklerinde Dil Örnekleri

**Denetim dışı (danışmanlık) hizmeti parametrelerini tanımlayan yönetim dili.**

Yönetim dili, denetim görevinin yürütüleceği sınırları belirler ama verilen veya verilmeyen özel hizmetlerin ayrıntılarını vermesi

beklenmez. Buna göre, bağımsızlık için alt sınırın neresi olduğu Yönetmelik'te tanımlanmışsa veya belirtilen özellikle uygulanabilir denetim standartlarına dâhil edilmişse; Yönetmeliğin, yalnızca verilecek hizmetler için parametrelerin konmasındaki diğer ihtiyaçlara işaret etmesi gerekebilir. Aşağıdaki üç örnekte, denetim dışı (danışmanlık) hizmetlerinin, bağımsızlık veya objektifliğin tehlikeye girmediği yerlerle sınırlı olduğu iki durumda ve denetim görevinden normal yönetim sorumluluğunu alması istenen bir durumda kullanılan dil gösterilmektedir.

- Denetim görevinin, objektiflik veya bağımsızlığın tehlikeye girmediği danışmanlık hizmetlerinde:

  "Denetçi, belediye başkanına, Şehir Meclisine ve idarî personelin sorumluluklarını yerine getirmede, *objektif ve zamanında bilgiler sağlayarak, şehirdeki faaliyetlerinin yürütülmesi veya uygun yönetim kontrolleri konusunda önerilerde bulunarak,* (ilgili X başlıklı) Denetim Standartları'na uygun bir şekilde yardımcı olabilir."

  "İç denetim bölümü, *bu Yönetmeliğin diğer bölümleriyle uyumlu bir şekilde,* diğer denetim-dışı görevleri yürütebilir ve Komisyon tarafından verilen diğer raporlandırma görevlerini yerine getirebilir."

- Denetim biriminin denetim-dışı hizmetler yaptığı durumda, bu hizmetlerin bazıları objektifliği ve bağımsızlığı tehikeye soksa da:

"Zaman zaman denetçinin, kurumun denetim-dışı faaliyetlerinde yer alması, genel müdüre ve müdürlere görevlerini yürütmelerinde, denetim komitesince yetkilendirildiği şekilde, yardım etmesi istenebilir."

**Danışmanlık projelerine katılım seviyesinin, tipi ve özelliğini sınırlayan politika ve prosedürlerin veya denetim dışı görevlerde yer alma sebebiyle objektiflik veya bağımsızlığa karşı oluşan tehditleri en aza indirecek kontrollerin kurulması.** Eğer denetçiler, kuruluşlarda yönetim görevlerini yerine getiriyorsa, denetim birimi,

ilgili politika ve prosedürleri geliştirmelidir. Özellikle, politikalarla bu kişiler, denetim dışı (danışmanlık) hizmeti içeren alanların denetimlerinin planlanması, yürütülmesi ve gözden geçirilmesi işlerinden men edilmelidir. Dahası, eğer denetim birimi, bütün denetim biriminin bağımsızlığını veya objektifliğini tehlikeye sokacak bir denetim dışı (danışmanlık) işi yerine getirirse, denetim fonksiyonundan sorumlu birim (meselâ denetim komitesi), denetim başlamadan önce, bu alanda daha sonra yapacağı bir denetiminde, denetim bağımsızlığının tehlikeye gireceği konusunda uyarılmalıdır. Eğer denetim görevi, tehlikenin olduğu alanda devam ederse, bu durum, denetim raporunda belirtilmelidir.

Bu tip yasaklamalar, yardımcılık işi yapıldıktan sonra söz konusu alanda önemli değişikler olduğunda veya yardımcılık görevi, 40 saatin altında olmak gibi *de minimums* durumunda ise, serbest hâle getirilebilir.

Aşağıdaki örnek politika ve prosedür, denetim dışı (danışmanlık) hizmetleri tanımlamakta ve denetçilerin bağımsızlık ve objektifliğine karşı tehditleri en aza indiren parametrelerdeki hizmetleri sınırlayan dili (bkz. altı çizili metin) içermektedir.

> **Politika:** Denetim hizmetlerine ek olarak, Denetçiler Ofisi, yöneticilere verilen diğer üç tip hizmeti de temin etmektedir: Devam eden projeler için Kalite Güvence Hizmetleri, Danışmanlık Hizmetleri ve Eğitim, Kontrol Özdeğerlendirme İçerikli Atölye Çalışmaları.
>
> Her tip hizmet için parametre aşağıda belirtilmiştir.
>
> **Kalite Güvence Hizmetleri:**
> Kalite güvence hizmetlerinde, Şehir Denetçiler Kurulu şu konularda *karar vererek* devam eden *projeleri izleyecek ve yardımcı olacaktır:*
>
> Proje hedefleri erişilebilir ve makul mu ?
>
> Tüm seçenekler teşhis edilip tam anlamıyla analiz edildi mi ?

Nitel ve nicel analizler tam ve doğru mu?
Bir proje planı yapılmış mı ve proje çalışanları plana riayet ediyorlar mı?

Projenin hedeflerine ulaşmak için diğer bölgeler tarafından kullanılan en iyi uygulamalar Şehir'e uygulanabilir mi ?

**Danışmanlık Hizmetleri ve Eğitim**
Denetim personeli, belediye personeline, yönetim güven sistemleri ve faaliyetlerin yeniden tasarlanması konusunda yardım ve eğitim verebilir. *Denetim personeli, sadece danışmandır ve yönetim, önerilerin uygulanmasındaki sorumluluğu kabul etmelidir.*

**Kontrol Özdeğerlendirme İçerikli Atölye Çalışmaları:**
Bu denetim sürecinde, çalışanlardan oluşan bir takım, denetçilerle bir araya gelip, hedeflere en etkili ve verimli şekilde nasıl ulaşılacağı konusunda kararlar alır. Resmî bir denetim raporundan ziyade, faaliyet planları, hedef(ler)in önündeki engellere yönelik olarak geliştirilir. *Çalışanlardan oluşan takım, faaliyet planındaki adımların atılmasından sorumludur.*

Aşağıdaki örnek prosedürler, denetim biriminin ileride bağımsızlık ve objektifliği tehdit eden denetim-dışı (danışmanlık) görevleri kabul ettiğinde, denetim birimi tarafından alınması gereken önlemleri açıklığa kavuşturan bir dil içermektedir:

Denetim komitesi tarafından denetimden, İDY tarafından bireysel denetçinin denetim görevini yerine getirmede objektifliğinin tehlikeye girdiğinin tespit edilmesi hâlinde, denetim-dışı görev yapması istendiğinde, aşağıdaki prosedürler işleme girer:

1. Denetim-dışı göreve başlamadan önce, İDY, denetim komitesi ile yazılı iletişime girerek, istenen görevin, bağımsızlık veya objektifliği tehlikeye düşüreceğini; tehlikenin yapısını, daha sonraki denetim görevlerinde bu tehlikenin sonuçlarını (meselâ, denetim işlevinin bu alanda gelecekteki denetimlere zeval getireceğini veya denetim komitesinin gelecekteki denetimler için üçüncü

bir tedarikçi ile anlaşması gerektiğini) bildirir. İDY, denetim komitesinden, denetim işlevinin ya denetim-dışı bir görev vermesini ya da bitirmesini belirten yazılı bir cevap ister.

2. Eğer denetim komitesi denetim işlevinin, denetim-dışı görev ile devam etmesini emrederse, İDY, tehlikeye şu belgelerde temas edecektir:
    - Denetim-dışı görevin belgelenmesi, denetim-dışı görevden sorumlu yönetime bir nüsha
    - Denetim işlevinin yıllık proje planlama prosedürleri
    - Bir sonraki kalite güvence denetiminde, dış kalite güvence sağlayıcı ile denetim işlevinin iletişime girdiği belge.

Eğer denetim komitesi, denetim işlevi tarafından bir önceki denetim-dışı görevinin bir parçası olarak yürütülen ve İDY tarafından önceden gelecekteki denetim işlerinde bir tehlikeye sebep olabileceği bildirilmiş olan faaliyet veya işlemleri içeren bir denetimi yönetmek amacıyla denetim yaparsa, aşağıdaki prosedürler işlemelidir:

1. Denetimi başlatmadan önce, İDY, denetim komitesi ile yazılı iletişime girerek, tehlikeye ve tehlikenin özelliklerine dikkat çeken ve objektiliğin en üst derece olması gerektiğine dair (örneğin, üçüncü parti bir tedarikçi ile anlaşılması gerektiğini belirten veya ortakların denetçilerin yardımını isteyen) bilgi verir.

2. Eğer denetim komitesi denetim işlevinin, denetim-dışı görev ile devam etmesini emrederse, İDY, tehlikeye şu belgelerde değinecektir:
    - Denetim planlaması belgeleri
    - Nihaî Denetim raporu.
3. Ayrıca, İDY, vukuatı ekler ve denetim işlevinin dış kalite güvence sağlayıcılarına bir sonraki kalite güvence denetiminde bütün belgeleri sağlar.

**Denetim dışı (danışmanlık) projeleri için ön görüşme süreci:** Danışmanlık işini kabul ederken ve yerine getirirken, denetçiler bu hizmeti sağlamalarının arkasındaki mantığı belgelemeli ve hizmetlerin denetim rolünün özünü bozmayacağına dair yargılarını ortaya koymalıdırlar. Bu bigi, dış kalite güvence denetçilerine de verilmelidir. Ön görüşme için örnek bir politika aşağıda verilmiştir:

1. Denetim dışı (danışmanlık) hizmetleri ile ilgili isteğin gelmesi üzerine, İç Denetim Bölümü, bu hizmetlerin verilmesinin, aynı alanda daha sonra denetimler yapacak kişinin objektifliği ve bölümün bağımsızlığı açısından bir tehlike oluşturup oluşturmayacağını dikkate alacaktır. Böyle bir tehlikenin söz konusu olması durumunda, istek reddedilecektir. Reddedilme durumda, etkenler ve sonuç, bir muhtıra ile hizmeti almak isteyenlere hitaben bildirilecektir.

2. Denetim-dışı (danışmanlık) hizmetlerini vermeden önce, görevli denetçi, bu hizmeti almak isteyenin işin sonuçlarından sorumlu olduğunu belgeleyecektir ve bu yüzden denetim-dışı (danışmanlık) işinin sonuçlarıyla ilgili bilgi verme sorumluluğunu taşımaktadır. İç Denetim Bölümü, hizmeti almak isteyen(ler) ile hedefler, içerik ve denetim-dışı (danışmanlık) hizmetlerine konan sınırlar doğrultusunda bir anlaşma yapacaktır.

# Uygulama Önerisi 1100-1: Bağımsızlık ve Objektiflik

Uluslararası İç Denetim Standartlarından
Standart 1100'ün Yorumu

## İlgili Standart

**1100 Bağımsızlık ve Objektiflik**
İç denetim faaliyeti bağımsız olmalı ve iç denetçiler görevlerini yaparken objektif davranmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bağımsızlık ve objektifliği değerlendirirken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu tür bir değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçiler, işlerini *serbest* ve *objektif* bir şekilde yapabildiklerinde *bağımsız* sayılır. Bağımsızlık, iç denetçilerin tarafsız ve önyargısız bir şekilde hüküm verebilmelerini mümkün kılar; bu, görevlerin usulüne uygun yapılması için şarttır. Bu hedefe, kurum içi statü ve objektiflikle ulaşılır.

# Uygulama Önerisi 1110-1: Kurum İçi Bağımsızlık

Uluslararası İç Denetim Standartlarından
Standart 1110'un Yorumu

## İlgili Standart

**1110 Kurum içi Bağımsızlık**
İç Denetim Yöneticisinin, kurum içinde, iç denetim faaliyetinin sorumluluklarını yerine getirmesine imkân sağlayan bir yönetim kademesine bağlı olması gerekir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, kurum içi bağımsızlığı değerlendirirken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu tür bir değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçilerin, denetlenenlerin işbirliğini sağlayabilmek ve işlerini her türlü müdahaleden uzak bir şekilde yapabilmek için, üst yönetim, denetim komitesi ve yönetim kurulu tarafından desteklenmeleri gerekir.

2. İç Denetim Yöneticisi, kurum içinde, geniş bir denetim kapsamı ve alanı oluşturmak, görevle ilgili raporlamalara yeterli ilginin gösterilmesini sağlamak ve görev sonucunda verilen tavsiyelere göre uygun tedbirlerin alınmasını sağlamak konusunda yeterli yetkiye sahip bir kişiye bağlı olmalıdır.

3. İdeal olan, İç Denetim Yöneticisinin işlevsel olarak denetim komitesi ve yönetim kuruluna, idarî olarak da kurumun başkanına bağlı ve sorumlu olmasıdır.

4. İç Denetim Yöneticisinin denetim komitesi ve yönetim kuruluyla doğrudan iletişimi bulunmalıdır. Denetim komitesi ve yönetim

kuruluyla düzenli iletişim kurmak, bağımsızlığın güvence altına alınmasına yardımcı olur ve komite ve kurul ile, İç Denetim Yöneticisinin karşılıklı ilgi alanlarına giren konularda birbirlerini haberdar etmelerine imkân sağlar.

5. Bu doğrudan iletişim, İç Denetim Yöneticisinin denetim komitesinin ve yönetim kurulunun denetim, mali raporlama, kurumsal yönetişim ve kontrolle ilgili genel gözetim sorumluluklarına ilişkin *toplantılarına düzenli olarak katılması* yoluyla sağlanır. İç Denetim Yöneticisinin bu toplantılara katılması, stratejik planların, faaliyetlere ilişkin gelişmelerin değerlendirilmesini ve yüksek seviyedeki risklerin, sistemlerin, prosedürlerin veya kontrol gibi meselelerin erken aşamalarda ele alınmasını sağlar; ayrıca iç denetim faaliyet planları ve çalışmaları hakkında bilgi alışverişinde bulunma fırsatı yaratır. İç Denetim Yöneticisi, denetim komitesi ve yönetim kuruluyla, *en azından yılda bir* defa özel bir toplantı yapmalıdır.

6. İç Denetim Yöneticisinin tayin veya azlinde denetim komitesi ve yönetim kurulunun onayının ve mutabakatının alınması, bağımsızlığı güçlendirir.

# Uygulama Önerisi 1110.A1-1: Bilgi Talebinin Sebebinin Açıklanması

Uluslararası İç Denetim Standartlarından
Standart 1110.A1'in Yorumu

## İlgili Standart

**1110.A1** İç denetim faaliyeti, iç denetimin kapsamının tayin edilmesi, iç denetim işlerinin yapılması ve sonuçların raporlanması konularında her türlü müdahaleden uzak ve serbest olmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bilgi taleplerinin sebeplerini açıklamaları istendiğinde, aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu durumda gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

Denetlenenler veya üçüncü şahıslar, zaman zaman, iç denetçiden, talep ettiği bir belgenin görevle ne tür bir ilgisi olduğuna açıklık getirmesini isteyebilir. Belgelerin talep edilmesinin sebeplerinin görev sırasında açıklanması veya açıklanmaması kararı, içinde bulunulan duruma bağlıdır. Önemli ve büyük usulsüzlükler, açıklama yapmanın daha faydalı olacağı normal şartlara göre, daha az açık bir ortamı mecbur kılar. Ancak, bu kararın özel durumların ışığında *İç Denetim Yöneticisi tarafından* alınması gerekir.

# Uygulama Önerisi 1110-2: İç Denetim Yöneticisi-Hiyerarşik İlişkiler

Uluslararası İç Denetim Standartlarından
Standart 1110'un Yorumu

## İlgili Standart

**1110 Kurum İçi Bağımsızlık**
İç denetim yöneticisinin, kurum içinde, iç denetim faaliyetinin sorumluluklarını yerine getirmesine imkân sağlayan bir yönetim kademesine bağlı olması gerekir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, İç Denetim Yöneticisinin bağlı olduğu görevlilerle ilişkilerini ve hiyerarşik ilişkileri belirlerken veya değerlendirirken aşağıdaki ilkeleri göz önüne almalıdır. Ancak bu kılavuzun, böyle bir değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

**(1)** IIA'nın Uluslararası *İç Denetim Standartlarına ("Standartlar")* göre, İç Denetim Yöneticisi, kurum içinde, iç denetim faaliyetinin sorumluluklarını yerine getirmesini mümkün kılan bir yönetim kademesine sorumlu olmalıdır. IIA, gerekli kurum içi bağımsızlığın sağlanabilmesi için, İç Denetim Yöneticisinin işlevsel olarak denetim komitesine veya dengi bir yönetim kademesine bağlı olması gerektiğini şiddetle savunmaktadır. İdarî amaçlarla, çoğu durumda, İç Denetim Yöneticisinin doğrudan doğruya ilgili kurumun başkanına bağlı olması gerekir. IIA'nın "işlevsel hiyerarşi" ve "idarî hiyerarşi" terimleri için yaptığı aşağıdaki tanımlar, bu Uygulama Önerisinin konusunu oluşturan tartışmada yararlı olacağı ümidiyle verilmektedir.

- *İşlevsel Hiyerarşi:* İç denetim fonksiyonu/birimi için işlevsel hiyerarşi, onun bağımsızlığı ve yetkisinin nihaî kaynağıdır. Bu konuda, IIA, İç Denetim Yöneticisinin işlevsel olarak ve işlevleri konusunda denetim komitesi, yönetim kurulu veya uygun başka bir yönetim birimine bağlı olmasını tavsiye etmektedir. Bu bağlamda geçen "işlevsel hiyerarşi" terimi, ilgili yönetim birimi ve yetkilisinin:
  - iç denetim faaliyetinin yönetmeliğini onaylama,
  - iç denetim risk değerlendirmelerini ve ilgili denetim planını onaylama,
  - İç Denetim Yöneticisi ile yönetimin bulunmadığı özel toplantılar yapmak da dahil, iç denetim faaliyetlerinin sonuçları hakkında ya da İç Denetim Yöneticisinin gerekli gördüğü başka konularda İç Denetim Yöneticisinden raporlar alma,
  - İç Denetim Yöneticisinin tayini veya azliyle ilgili tüm kararları onaylama,
  - İç Denetim Yöneticisinin yıllık ücretini ve ücret ayarlamalarını onaylama,
  - iç denetim faaliyetinin sorumluluk ve görevlerini yerine getirmesine engel olan kapsam veya bütçe kısıtlamaları olup olmadığını tespit etmek amacıyla, İç Denetim Yöneticisi ve yönetim nezdinde uygun inceleme ve araştırmaları yapma

  yetkilerine sahip olması anlamına gelir.
- *İdarî Hiyerarşi:* İdarî hiyerarşi, kurumun yönetim yapısı içinde kurulan ve iç denetim biriminin günlük iş ve işlemlerini kolaylaştıran hiyerarşik ilişkidir. İdarî hiyerarşi normal olarak
  - bütçeleme ve yönetim muhasebesi,
  - personel değerlendirmeleri ve ücretleri de dahil insan kaynakları yönetimi,

- iç haberleşme ve bilgi akışları,
- kurumun kendi iç politikaları ve prosedürlerinin yönetimi konularını kapsar.

**(2)** Bu Uygulama Önerisi, İç Denetim Yöneticisi hiyerarşik ilişkilerinin kurulması veya değerlendirilmesine ilişkin mülâhaza ve konulara odaklanmıştır. Bir iç denetim biriminin görev ve yükümlülüklerini etkin ve amaca uygun bir şekilde yerine getirmesi amacıyla gereken bağımsızlık, objektiflik ve kurum içi önem kıstaslarına ulaşmak için uygun hiyerarşik ilişkiler kurmak hayatî öneme sahiptir. İç Denetim Yöneticisinin hiyerarşik ilişkileri, denetim faaliyetlerinin sonuçlarının rapor edilmesinde ve risk değerlendirmesinde temel oluşturan uygun bilgi akışının sağlanması ve önemli anahtar yöneticiler ve müdürlere erişimin sağlanması için de hayatî öneme sahiptir. Öte yandan, İç Denetim Yöneticisi, iç denetim biriminin bağımsızlığına ve etkin çalışmasına engel oluşturan hiyerarşik ilişkileri ciddî bir kapsam sınırlaması olarak görmeli ve bu durumları, denetim komitesinin veya dengi birimlerin dikkatine sunmalıdır.

**(3)** Bu Uygulama Önerisinde, ayrıca, İç Denetim Yöneticisinin hiyerarşik ilişkilerinin ilgili kurumun niteliğinden (kamu veya özel sektör kurumu ve kurumun nisbî büyüklüğü), her ülkenin yaygın uygulamalarından, kurumların giderek daha da karmaşık hâle gelen yapısından (ortak girişimler, iştirakleri bulunan çokuluslu şirketler) ve müşterileriyle ilgili öncelikler ve kapsam konusunda giderek artan bir işbirliği gerektiren katma değerli hizmetler sunan iç denetim gruplarına yönelik eğilimden etkilendiği de kabul edilmektedir. Bunun sonucu olarak, IIA, işlevsel hiyerarşi konusunda denetim komitesine ve idarî hiyerarşi konusunda kurum başkanına (CEO'ya) bağlı olmanın en ideal hiyerarşik yapı olduğuna inanmasına rağmen, işlevsel ve idarî hiyerarşik ilişkiler arasında açık ve net bir ayrımın yapılması hâlinde ve faaliyetlerin kapsamının ve bağımsızlığının sağlanabilmesi için uygun tedbirlerin alınması hâlinde, başka türde ilişkiler de etkili olabilir. İç denetçilerden, bu Uygulama Önerisinde verilen önerilerin hangilerinin her özel

durumda, hangi sınırlar içinde uygulanabileceğini tespit etmek için meslekî muhakemelerini kullanmaları beklenmektedir.

**(4)** *Standartlar*, İç Denetim Yöneticisinin bağımsızlığını sağlayabilmek ve geniş bir denetim kapsamı uygulanmasını sağlamak için İç Denetim Yöneticisinin uygun ve yeterli yetkiye sahip bir kişiye bağlı olmasının önemini vurgulamaktadır. Ancak *Standartlar* bu hiyerarşik ilişkiler konusunda bilerek biraz geniş tutulmuştur; çünkü Standartlar büyüklük veya başka etkenlere bakılmaksızın bütün kurumlara uygulanmak amacıyla tasarlanmıştır. "*Bir boy hepsine uyar*" ilkesini uygulanamaz hâle getiren etkenler arasında, kurumun büyüklüğü ve tipi (özel, kamu veya şirket) sayılabilir. Bundan dolayı, İç Denetim Yöneticisi, idarî hiyerarşik yapının uygunluğunu değerlendirirken aşağıdaki özellikleri göz önüne almalıdır.

- İlgili kişi, iç denetim biriminin etkinliğini sağlamak için kurum içinde yeterli yetkiye ve öneme sahip midir?
- İlgili kişi, İç Denetim Yöneticisine görevlerinde yardımcı olmak için uygun kontrol ve yönetişim zihniyetine sahip midir?
- İlgili kişinin denetim konularında İç Denetim Yöneticisine aktif destek olmak için yeterli zamanı var mı ve buna ilgi duyuyor mu?
- İlgili kişi, işlevsel hiyerarşik ilişkiyi anlıyor ve destekliyor mu?

**(5)** Ayrıca, idarî hiyerarşik yapıdan sorumlu olan kişinin kurum içinde iç denetime tâbi başka faaliyetlerin de sorumluluğunu üstlenmesi hâlinde, İç Denetim Yöneticisi, gereken uygun bağımsızlığın korunmasını da sağlamalıdır. Örneğin, bazı İç Denetim Yöneticileri, idarî açıdan kurumun muhasebe fonksiyonlarından da sorumlu olan finans müdürüne bağlıdır. İç denetim birimi, denetim planı için bu kapsamı uygun gördüğü takdirde, kurumun idarî işler yöneticisine de bağlı olan faaliyetleri denetlemekte ve denetim

sonuçlarını rapor etmekte serbest olmalıdır. Bu faaliyetlerin kapsamına veya faaliyet sonuçlarının raporlanmasına getirilen kısıtlamalar, denetim komitesinin dikkatine sunulmalıdır.

**(6)** Dünyada mali raporlamayla ilgili konularda daha sıkı bir mevzuata ve düzenlemeye yönelik son eğilim ve gelişmelerin ışığında, İç Denetim Yöneticisinin hiyerarşik ilişkileri, iç denetim biriminin denetim komitesinin veya diğer önemli birimlerin artan ihtiyaç ve isteklerine cevap verebilmesi için uygun olmalıdır. İç Denetim Yöneticisinin kurumun yönetişim ve risk yönetim faaliyetlerinde daha önemli rol üstlenmesi giderek artan bir şekilde istenmektedir. İç Denetim Yöneticisinin hiyerarşik ilişkileri, iç denetim biriminin bu beklentileri karşılamasını kolaylaştırmalıdır.

**(7)** Kurumun hangi hiyerarşik ilişki sistemini seçtiğine bakmaksızın, çeşitli temel eylemler, hiyerarşik yapı ve ilişkilerin iç denetim faaliyetinin etkinliğine ve bağımsızlığına destek olmasına ve bunu sağlamasına yardımcı olabilir.

- İşlevsel Hiyerarşi:
  - İşlevsel hiyerarşi, uygun bağımsızlık ve iletişim seviyesini sağlayabilmek için doğrudan doğruya denetim komitesine veya onun dengi bir mercie kadar ulaşmalıdır.
  - İç Denetim Yöneticisi, hiyerarşik ilişkisinin bağımsızlığını ve karakterini güçlendirmek için, denetim komitesi veya onun dengi bir birimle, yönetimden hiç kimsenin katılmadığı özel toplantılar yapmalıdır.
  - Yıllık denetim planını ve bu planda yapılan bütün önemli değişiklikleri inceleme ve onaylama konusunda nihai yetki, denetim komitesinde olmalıdır.
  - İç Denetim Yöneticisi, denetim komitesinin başkanına ve üyelerine veya gerekirse yönetim kurulu başkanına ve tüm üyelerine her zaman açık ve doğrudan erişim olanağına sahip olmalıdır.

- Denetim komitesi, İç Denetim Yöneticisinin performansını en az yılda bir kere incelemeli ve yıllık ücretini ve maaş ayarlamasını onaylamalıdır.
- İç denetim faaliyetinin yönetmeliği, hem bu birimle ilgili işlevsel ve idarî hiyerarşik ilişkileri, hem de her hiyerarşik kademeye kadar temel faaliyetleri açıkça düzenlemelidir.

• İdarî Hiyerarşi:

- İç Denetim Yöneticisinin idarî hiyerarşik ilişkisi, CEO'yla (baş icra sorumlusuyla) ya da ona günlük faaliyetlerini yürütme konusunda destek vermek için yeterli yetkiye sahip başka bir yöneticiyle olmalıdır. Bu destek, birimin ve İç Denetim Yöneticisinin kurum içi örgütlenme yapısında birime uygun önemin ve değerin verilmesini sağlayacak bir şekilde konumlandırılmasını da kapsamalıdır. Bir kurum içi örgütlenme yapısında iç denetim birimi ve İç Denetim Yöneticisinin çok düşük bir hiyerarşik kademeye bağlanması, iç denetim biriminin önemini ve etkinliğini olumsuz etkileyebilir.
- İç denetim birimi faaliyetlerinin kapsamı veya faaliyet sonuçlarının raporlanması konusunda nihai yetki, bu idarî hiyerarşik kademede olmamalıdır.
- İdarî hiyerarşik ilişkiler, iç denetim biriminin hem üst yönetimle hem de bölüm yönetimleriyle açık ve doğrudan iletişimini kolaylaştırmalıdır. İç Denetim Yöneticisi, CEO da (kurum başkanı) dahil her düzeyden yönetim kademesiyle doğrudan iletişim kurabilmelidir.
- İdarî hiyerarşik ilişkiler; kurum faaliyetleri, planları ve iş inisiyatifleri hakkında İç Denetim Yöneticisine ve iç denetim birimine yeterli ve zamanında bilgi akışının olması için gerekli ve yeterli bilgi akışını ve iletişimi sağlamalıdır.
- İdarî hiyerarşik yapı ve ilişkilerin getirdiği bütçe kontrolleri ve düşünceleri, iç denetim biriminin görevlerini yerine getirmesine engel olmamalıdır.

**(8)** İç Denetim Yöneticileri, başka kontrol ve gözlem fonksiyonlarıyla ve birimleriyle (risk yönetimi, mevzuata uyum, güvenlik, hukuk, etik, çevre, dış denetim) ilişkilerini de göz önüne almalı ve değerlendirmeli, önemli risk ve kontrol sorunlarının denetim komitesine rapor edilmesini kolaylaştırmalıdır.

# Uygulama Önerisi 1120-1: Bireysel Objektiflik

Uluslararası İç Denetim Standartlarından
Standart 1120'nin Yorumu

## İlgili Standart

**1120 Bireysel Objektiflik**
İç denetçilerin tarafsız ve önyargısız bir şekilde davranması ve her türlü çıkar çatışmasından kaçınması gerekir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bireysel objektifliği değerlendirirken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu tür bir değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Objektiflik, iç denetçilerin görevlerini yaparken almaları ve sürdürmeleri gereken bağımsız bir zihinsel tavırdır. İç denetçiler, denetim konularına ilişkin karar ve yargılarını, başkalarının fikir ve düşüncelerine bağlamamalıdır.

2. Objektiflik, iç denetçilerin görevlerini, iş sonucunda çıkan ürüne gerçekten ve dürüst bir şekilde inanacakları ve bu ürünün kalitesinden önemli bir taviz vermeyecekleri bir şekilde yapmalarını gerektirir. İç denetçiler, objektif hüküm veremeyecekleri durumlara girmemeli ve itilmemelidir.

3. Denetim personeli arasında görev dağılımı, mevcut ve muhtemel çıkar çatışmaları ve önyargılardan kaçınılacak bir şekilde yapılmalıdır. İç Denetim Yöneticisi, iç denetim personelinden, muhtemel çıkar çatışmaları ve önyargılar hakkında düzenli ve dönemsel olarak bilgi almalıdır. İç denetçiler arasında görev

dağılımı, bunun uygulanabilir olması hâlinde, dönemsel rotasyona bağlanmalıdır.

4. Denetim işinin objektif bir şekilde yapıldığından makul ölçüler içinde emin olmak için, görev raporları yayınlanmadan önce, sonuçların gözden geçirilmesi gerekir.

5. İç denetçinin personel, denetlenen, müşteri, tedarikçi veya işle ilgili başka kişilerden herhangi bir ücret, hediye veya eğlence kabul etmesi etik değildir. Aksi halde, denetçinin objektifliğinin bozulduğu izlenimi oluşabilir; bu ise o denetçinin hem yapmakta olduğu hem de yapacağı görevlere gölge düşürebilir. Üstlenilen görevlerin özel şartları, ücret veya hediye almayı haklı çıkartan bir etken olarak görülmemelidir. Genel olarak herkese verilen ve çok küçük bir değere sahip olan (kalemler, ajandalar veya numuneler gibi) tanıtım malzemelerinin alınması da iç denetçinin meslekî karar ve yargılarına engel olmamalıdır. İç denetçiler, kendilerine teklif edilen bütün değeri yüksek para veya hediyeleri kendi âmirlerine derhal bildirmelidir.

6. İç denetim faaliyeti, faaliyetlerini menfaat çatışmalarından kaçınacak şekilde yürütme ve muhtemel çıkar çatışmalarına yol açabilecek her hangi bir faaliyetini de açıklama taahhüdünü yerine getirecek bir politika benimsemelidir.

# Uygulama Önerisi 1130-1: Bağımsızlık veya Objektifliği Bozan Etkenler

Uluslararası İç Denetim Standartlarından
Standart 1130'un Yorumu

## İlgili Standart

**1130 Bağımsızlık veya Objektifliği Bozan Etkenler**
Denetçilerin bağımsızlığı veya objektifliği fiilen bozulduğu veya bozulduğu izlenimi doğduğu takdirde, bozulmanın ayrıntıları ilgili taraflara açıklanmalıdır. Bu açıklamanın kapsamı, bozucu etkenin niteliğine bağlıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bağımsızlık veya objektifliği bozan unsurları değerlendirirken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu tür bir değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçiler,bir çıkar çatışmasının, bir önyargının mevcut olduğu veya muhtemel görüldüğü durumları, İç Denetim Yöneticisine bildirmelidir. Bu durumda, İç Denetim Yöneticisi, bu iç denetçilere başka görevler vermelidir.

2. Kapsam sınırlandırması, iç denetim faaliyetine getirilen ve faaliyetin hedef ve planlarını gerçekleştirmesine engel olan bir kısıtlama anlamına gelir. Bir kapsam sınırlandırmasıyla, bir çok şey yanında,
   - iç denetim yönetmeliğinde tanımlanan yetki alanları,
   - görevlerin ifası için gereken kaynaklara,
   - personele, demirbaşlara ve ilgili mahallere erişim imkânı,

- onaylanmış görev iş programı,
- gereken görev prosedürlerinin uygulanması,
- onaylanmış personel planı ve mali bütçe de kısıtlanabilir.

3. Bir kapsam sınırlandırması ve bu sınırlandırmanın muhtemel etkileri, denetim komitesi ve yönetim kuruluna, tercihan yazılı olarak, bildirilmelidir.

4. İç Denetim Yöneticisi, daha önce denetim komitesi ve yönetim kuruluna bildirilmiş ve onlar tarafından kabul edilmiş bulunan *yetki sınırlandırmaları* hakkında, bu birimlere tekrar bilgi vermenin gerekli olup olmadığını değerlendirmelidir. Bu, özellikle kurumda, denetim komitesi, yönetim kurulu veya üst yönetimde değişiklik olduğunda veya benzer başka değişiklikler olduğunda gerekli olabilir.

# Uygulama Önerisi 1130.A1-1: İç Denetçilerin Daha Önceden Sorumlu Olduğu Faaliyetlere İlişkin Değerlendirmeleri

Uluslararası İç Denetim Standartlarından
Standart 1130.A1'in Yorumu

## İlgili Standart

**1130.A1** İç denetçiler, daha önceden kendilerinin sorumlu olduğu faaliyetlere ilişkin değerlendirme yapmaktan kaçınmalıdır. Bir iç denetçinin son bir yıl içinde kendisinin sorumlu olduğu bir faaliyet hakkında güvence hizmeti vermesinin, objektifliğini bozacağı varsayılır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, daha önceden kendilerinin sorumlu olduğu bir faaliyet hakkında denetim ve değerlendirme yapmakla görevlendirildikleri takdirde aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu tür bir değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçiler, icraî sorumluluklar üstlenmemelidir. Üst yönetim iç denetçilere denetim dışında iş ve görevler verdiği takdirde, iç denetçiler bu görevlerinde iç denetçi sıfatıyla çalışamaz. Ayrıca, iç denetçilerin, *son bir yıl içinde* kendilerinin yetkili veya sorumlu olduğu bir faaliyet hakkında güvence amaçlı inceleme veya denetim yapması durumunda, objektifliklerinin bozulacağı varsayılır. Denetim sonuçları rapor edilirken bu bozulma da dikkate alınmalıdır.

    - İç denetçilere, banka hesap mutabakatlarının yapılması ve hazırlanması gibi, objektifliklerini bozabilecek denetim dışı

görevler verildiği takdirde, İç Denetim Yöneticisi, üst yönetime, denetim komitesine ve yönetim kuruluna bu faaliyetin bir güvence denetim faaliyeti olmadığını ve dolayısıyla, bu faaliyetten denetimle ilgili sonuçlar *çıkartılmaması* gerektiğini bildirmelidir.

- Ayrıca, iç denetim faaliyetine icraî sorumluluklar verildiği takdirde, ilgili sorumluluk alanında daha sonra bir güvence görevi üstlenildiğinde, objektifliğin sağlanmasına özel bir dikkat gösterilmelidir. İç denetçilerin, *son bir yıl içinde* yetkili veya sorumlu oldukları bir faaliyeti denetlemeleri durumunda, objektifliklerinin bozulacağı varsayılır. Böyle bir durum, sonuçların rapor edilmesi sırasında açıkça beyan edilmelidir.

2. Denetimlerde, icraî bir yetkinin de üstlenilmesi söz konusu olursa, bu yetkiyle ilgili sahada denetim objektifliğinin bozulacağı varsayılır.

3. İç denetim faaliyetine katılan ya da geçici olarak iç denetimle görevlendirilenler, makul bir süre *(en az bir yıl)* geçmeden, daha önce kendilerinin yürüttüğü faaliyetleri denetlemekle görevlendirilmemelidir. Aksi halde bu kişilerin objektifliğinin bozulacağı varsayılır; bu sebeple o görevle ilgili denetimin gözetim ve kontrolünde ve görev sonuçlarının raporlanmasında ilâve özen ve dikkat gösterilmelidir.

4. İç denetçinin sistemler için kontrol standartları tavsiye etmesi veya uygulanmadan önce prosedürleri gözden geçirmesi, objektifliği olumsuz etkilemez. Fakat denetçinin sistem tasarlaması, kurması, işletmesi ve bu sistemlerin prosedürlerini yazmasının objektifliği bozacağı düşünülür.

5. İç denetçinin zaman zaman denetim dışı işler de yapması ve bunun raporlama sürecinde tam ve eksiksiz açıklanması, denetçinin bağımsızlığını zayıflatmaz. Ancak iç denetçinin objektifliğini etkileyebilecek olumsuzlukları önlemek için, hem iç denetçinin hem de yönetimin dikkatli hareket etmesi gerekir.

# Uygulama Önerisi 1130.A1-2: Diğer (Denetim Dışı) İşlevler Karşısında İç Denetçinin Sorumluluğu

Uluslararası İç Denetim Standartlarından
Standart 1130.A1'in Yorumu

## İlgili Standart

**1130.A1** İç denetçiler, daha önceden kendilerinin sorumlu olduğu faaliyetlere ilişkin değerlendirme yapmaktan kaçınmalıdır. Bir iç denetçinin son bir yıl içinde kendisinin sorumlu olduğu bir faaliyet hakkında güvence hizmeti vermesinin objektifliğini bozacağı varsayılır.

**Bu Uygulama Önerisinin Niteliği:** *Denetim dışı, icraî işlev ve görevler için sorumluluk üstlenme durumunda olan iç denetçilerin aşağıdaki ilkelere uymaları önerilir. Bu tür sorumlulukların üstlenilmesi, iç denetçinin bağımsızlık ve objektifliğini bozabilir ve mümkünse bundan kaçınılması gerekir. Ancak bu kılavuzun, bu tür görev veya sorumlulukları değerlendirmek amacıyla gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Bazı iç denetçiler, kurumun yönetimi açısından işlerle ilgili makul sebeplerle denetim dışı görevler kabul etmekte ya da bu tür görevlerle görevlendirilmektedir. İç denetçilerden, bağımsızlık veya objektifliklerini zayıflatacak görev ve sorumluluklar üstlenmelerinin istenmesi gittikçe daha sık karşılaşılan bir durum olmaktadır. Hem kamu hem de özel kurumlardan daha etkin ve verimli faaliyetler yapmaları ve bunu daha az kaynakla yapmaları konusundaki beklentinin artması nedeniyle, ilgili kurumun yönetimi, bazı iç denetim birimlerine, dönemsel olarak denetime tâbi faaliyetlerin de sorumluluğunu üstlenmeleri talimatını vermektedir.

2. Bir iç denetim birimi veya iç denetçi, kendisinin denetleyebileceği

bir faaliyetten sorumlu ise ya da kurum yönetimi ona böyle bir görev vermeyi düşünüyorsa, iç denetçinin bağımsızlık ve objektifliği bozulabilir. İç denetçi, bunun bağımsızlık ve objektifliği üzerindeki muhtemel etkilerini değerlendirirken aşağıdaki etkenleri dikkate almalıdır:

- *IIA Uluslararası İç Denetim Standartları* (Standartlar) ve *Etik Kuralları*nın gerekleri,
- Hissedarlar, yönetim kurulu, denetim komitesi, kurum yönetimi, idarî merciler, kamu kuruluşları, yasama organları ve toplumsal çıkar grupları gibi kişi ve tarafların beklentileri,
- İç denetim faaliyeti yönetmeliğinde verilen izinler ve/veya öngörülen kısıtlamalar,
- *Standartlar*ın gerektirdiği açıklamalar,
- İç denetçinin üstlendiği görev veya faaliyetlerin daha sonraki denetim kapsamı.

3. İç denetçiler, denetim dışı bir görev için sorumluluk üstlenme durumuyla karşı karşıya olduğunda, uygun hareket tarzını belirlemek için aşağıdaki etkenleri dikkate almalıdır:

**A.***IIA Etik Kuralları ve Standartları*, iç denetim faaliyetinin bağımsız olmasını ve iç denetçilerin işlerini yaparken objektif davranmalarını gerektirir.

- Mümkünse, iç denetçiler, dönemsel iç denetim incelemeleri ve değerlendirmelerine tâbi olan denetim dışı fonksiyon veya görevler için sorumluluk kabul etmekten ve üstlenmekten kaçınmalıdır. Bunun mümkün olmaması hâlinde:
- Bağımsızlık ve objektifliğin bozulduğunun, ilgili kişi ve taraflara açıklanması gerekir; bu açıklamanın niteliği ve kapsamı, bozucu etkene bağlıdır.

- Bir denetçinin son bir yıl içinde kendisinin sorumlu olduğu bir faaliyetle ilgili güvence hizmeti vermesinin, denetçinin objektifliğini bozacağı varsayılır.
- Yönetim zaman zaman iç denetçilerden denetim dışı iş ve görevler istediği takdirde, iç denetçilerin o iş ve görevlerde iç denetçi sıfatıyla çalışmadığı açıkça belirtilmelidir.

**B.** Hukukî gerekler de dahil, hissedar ve diğer menfaat sahiplerinin beklentileri, muhtemel objektifliği bozucu etkenle ilişkili olarak değerlendirilmelidir.

**C.** İç denetim faaliyeti yönetmeliği, iç denetçiye denetim dışı görevlerin verilmesi konusunda belirli özel kısıtlamalar içeriyor veya sınırlandırıcı bir dil kullanıyorsa, bu kısıtlamalar açıklanmalı, beyan edilmeli ve yönetimle tartışılmalıdır. Yönetim yine de bu görevlendirme üzerinde ısrar ediyorsa, denetçi bu konuyu denetim komitesine veya uygun başka bir yönetim birimine bildirmeli ve konuyu onlarla tartışmalıdır. Yönetmelik bu konuda herhangi bir hüküm içermiyorsa, aşağıdaki bentlerde verilen tavsiyelere uyulmalıdır. Aşağıdaki tavsiyeler, yönetmeliğin lâfzına bağlı olarak değerlendirilmelidir.

**D. Değerlendirme:** Değerlendirme sonuçları yönetimle, denetim komitesiyle ve/veya başka ilgili taraflarla tartışılmalıdır. Bazıları birbirini etkileyen bir dizi konu hakkında tespit yapılmalıdır:

- İlgili denetim dışı icraî görevin kurum açısından önemi (gelirler, giderler, itibar ve etki açılarından) değerlendirilmelidir.
- Görevin uzunluğu veya süresi ve üstlenilen sorumluluğun kapsamı değerlendirilmelidir.
- Görev ayrımının uygunluğu değerlendirilmelidir.
- Denetim sonuçları rapor edilirken, objektiflik veya

bağımsızlığı bozucu muhtemel etkenler veya böyle bir bozulma izleniminin olup olmadığı dikkate alınmalıdır.

**E. Denetim Dışı Faaliyetin Denetimi ve Açıklama:** İç denetim faaliyetinin icraî görevleri bulunduğu ve bu denetim dışı görevlerin, işletme denetim planının bir parçası olduğu dikkate alındığında, denetçinin düşünebileceği bir kaç çıkış yolu vardır:

- Denetim işi, sözleşmeli olarak üçüncü şahıs firmaya, dış denetçilere ya da iç denetim birimine yaptırılabilir. İlk iki durumda, kurumun dışından denetçilerin kullanılmasıyla objektifliğin bozulması tehlikesi asgarîye indirilebilir. Son durumda ise, objektifliğin bozulması söz konusudur.
- İcraî sorumlulukları bulunan denetçiler, ilgili faaliyetin denetim çalışmasına katılmamalıdır. Mümkünse, denetim değerlendirme çalışmasını yapan denetçi, bağımsızlığı veya objektifliği bozulmamış olanların yönetim ve nezaretinde olmalı ve denetim değerlendirme sonuçlarını onlara rapor etmelidir.
- Denetçinin denetim dışı faaliyetle ilgili icraî görev ve sorumlulukları, söz konusu faaliyetin kurum açısından önemi (gelirler, giderler veya ilgili diğer bilgiler açılarından) ve o faaliyeti denetleyenlerle iç denetçi arasındaki ilişki hakkında açıklama yapılmalıdır.
- Denetçinin icraî görev ve sorumlulukları, ilgili denetim raporunda ve denetçinin, denetim komitesine veya başka yönetim birimlerine sunduğu standart raporlarda açıklanmalıdır.

# Uygulama Önerisi 1200-1: Yeterlilik ve Azamî Özen ve Dikkat

Uluslararası İç Denetim Standartlarından
Standart 1200'ün Yorumu

## İlgili Standart

**1200 Yeterlilik ve Azamî Özen ve Dikkat**
Denetim görevleri, yeterlilik ve azamî özen ve dikkat gösterilerekyerine getirilmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görevlerini yaparken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu amaçla gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Meslekî yeterlilik, İç Denetim Yöneticisinin ve her iç denetçinin kendi sorumluluğudur. İç Denetim Yöneticisi, her görev için görevlendirilen kişilerin hepsinin görevi gerektiği gibi ve usulünce yapmak için gereken bilgi, beceri ve diğer vasıflara sahip olmasını sağlamalıdır.

2. İç denetçiler, meslekî davranış standartlarına uymalıdır. IIA'nın *Etik Kuralları*, iç denetimin tanımının ötesinde iki önemli unsur daha içermektedir:

   - İç denetim mesleği ve uygulamasıyla ilgili ilkeler: Dürüstlük, objektiflik, gizlilik ve yetkinlik,
   - İç denetçilerden beklenen davranış normlarını izah eden ve tanımlayan *Davranış Kuralları*. Bu kurallar, ilkelerin fiilî uygulamalara dönüştürülmesinde kullanılabilecek bir araçtır ve iç denetçilerin etik davranışlarını yönlendirmek amacına yöneliktir.

# Uygulama Önerisi 1210-1: Yeterlilik

Uluslararası İç Denetim Standartlarından
Standart 1210'un Yorumu

## İlgili Standart

**1210 Yeterlilik**
İç denetçiler, kişisel olarak, sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer vasıflara sahip olmalıdır. İç denetim faaliyeti de, toplu olarak, kendi sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer vasıflara sahip olmalı veya bunları edinmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, yeterliliğin değerlendirilmesinde aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu tür bir değerlendirme sırasında gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Her iç denetçi, belirli bilgi, beceri ve diğer vasıflara sahip olmalıdır:
    - Görevlerin ifası için, iç denetim standartları, prosedürleri ve tekniklerinin uygulanmasında meslekî yeterliliğe ihtiyaç vardır. Yeterlilik, geniş ve kapsamlı teknik araştırma ve yardımlardan istifade imkânı olmasa da, mevcut bilgiyi karşılaşılması muhtemel durumlara uygulama ve bu tür durumlarla başa çıkabilme yeteneği anlamına gelir.
    - Görevi kapsamında mali kayıt ve raporlarla çalışan denetçilerin muhasebe ilkeleri ve teknikleri hakkında yeterli olması gerekir.
    - Örnek iş uygulamalarından sapmaların önemini ve etkilerini anlamak ve değerlendirmek için, yönetim ilkelerinin anlaşılması gerekir. *Yönetim ilkelerini anlamak*, sahip olduğu geniş bilgiyi karşılaşılması muhtemel durumlara uygulama, bunlardan

önemli sapmaları fark etme ve makul çözümlere ulaşmak için gereken araştırmaları yapabilme yeteneği anlamına gelir.

- Muhasebe, ekonomi, ticaret hukuku, vergilendirme, finans, kantitatif yöntemler ve bilgi teknolojisi gibi bilim dalları ve konularının temellerini bilmek ve idrak etmek gerekir. "*İdrak*", mevcut veya muhtemel sorunları fark etme ve bu konuda yapılması gereken ek araştırmaları veya yardım alınması gereken konuları tespit etme *yeteneği* anlamına gelir.

2. İç denetçiler, insanlarla çalışma ve etkin iletişim kurma becerilerine sahip olmalıdır. İç denetçiler, insan ilişkilerinden anlamalı ve denetlenenlerle tatmin edici ilişkiler kurabilmelidir.

3. İç denetçiler; görevin hedefleri, değerlendirmeler, sonuçlar ve tavsiyeler gibi konuları açıkça, etkili bir şekilde açıklayabilmek için gereken sözlü ve yazılı iletişim yeteneklerine sahip olmalıdır.

4. İç Denetim Yöneticisi, ilgili işin kapsamını ve sorumlulukların düzeyini dikkate alarak, iç denetim kadrolarına atama yapılmasında aranacak olan uygun eğitim ve tecrübe kıstaslarını tespit etmelidir. Her müstakbel denetçinin meslekî vasıflarını ve yeterliliğini tevsik eden makul sertifikalar alınmalıdır.

5. İç denetim personeli, kurum içinde denetim görevinin yapılması için gerekli olan bilgi ve becerilere topluca sahip olmalıdır. İç denetim biriminin bilgi ve becerilerinin yıllık bir değerlendirmesi, *Sürekli Meslekî Gelişim*, işe alma veya aynı zamanda hizmeti kurum dışından alma yoluyla ele alınabilecek fırsat alanlarının belirlenmesine yardımcı olmak gayesiyle, gerçekleştirilmelidir.

6. *'Sürekli Meslekî Gelişim'*, iç denetim personelinin yeterliliğini temin için çok gereklidir. Bu konu için Uygulama Önerisi 1230-1'e bakınız.

7. Tam bir yeterliliğe sahip olunmayan faaliyet sahalarını desteklemek ve tamamlamak için, iç denetim birimi dışından uzmanların yardımı alınabilir. Bu konu için Uygulama Önerisi 1210.A1-1'e bakınız.

# Uygulama Önerisi 1210.A1-1: İç Denetim Faaliyetini Tamamlamak veya Desteklemek Amacıyla Hizmetlerin Dışarıdan Temini

Uluslararası İç Denetim Standartlarından
Standart 1210.A1'in Yorumu

## İlgili Standart

1210.A1 İç denetim personeli, görevin tamamını veya bir kısmını yapmak için gereken bilgi ve becerilerin veya diğer vasıfların hepsine sahip değilse, İç Denetim Yöneticisi kurum dışındaki uzmanlardan nitelikli tavsiye ve yardım temin etmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyetine destek olmak amacıyla dışarıdan ek hizmet almayı değerlendirirken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu amaçla gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetim faaliyetinin, muhasebe, denetim, iktisat, finans, istatistik, bilgi teknolojileri, mühendislik, vergi, hukuk ve çevre sorunları gibi bilim dallarında ve iç denetim faaliyetinin sorumluluklarını yerine getirebilmesi için gerek duyulan diğer alanlarda uzman personeli bulunmalı ya da bu konularda uzman olan dış hizmet sağlayıcılarından istifade etmelidir. Ancak iç denetim elemanlarının her birinin ilgili bütün bilim dallarında uzman olması gerekmez.

2. *Dış hizmet sağlayıcısı* (taşeron) terimi, belirli bir bilim dalında veya alanda özel bilgi, beceri ve deneyim sahibi olan ve kurumdan

bağımsız olan bir kişi veya firma anlamına gelir. Dış hizmet sağlayıcıları arasında, bunlarla sınırlı kalmamak kaydıyla, sigorta aktüerleri, muhasebeciler, kıymet takdir uzmanları (muhamminler), çevre uzmanları, suiistimal tahkikatı uzmanları, avukatlar, mühendisler, jeologlar, güvenlik uzmanları, istatistikçiler, bilgi teknolojisi uzmanları, kurumun kendi dış denetçileri ve başka denetim kurumları ve firmaları sayılabilir. Bir dış hizmet sağlayıcısı, denetim komitesi ve yönetim kurulu, üst yönetim veya İç Denetim Yöneticisi tarafından tutulabilir ve görevlendirilebilir.

3. İç denetim faaliyeti, dış hizmet sağlayıcılarını diğer amaç ve konuların yanı sıra aşağıda sayılan amaçlar için de kullanabilir:
    - Bilgi teknolojisi, istatistik, vergiler ve dil çeviri hizmetleri gibi uzmanlık bilgi ve becerilerine ihtiyaç olan ya da görev iş programında öngörülen amaçlara ulaşmak için uzmanlık bilgive becerilerine ihtiyaç olan denetim faaliyetleri,
    - Arazi ve binalar, sanat eserleri, değerli taşlar, mücevherler, yatırımlar ve karmaşık mali araçlar gibi varlıkların kıymet takdiri işleri,
    - Maden ve petrol kaynakları gibi belirli varlıkların miktarının veya fiziksel durumunun tespit edilmesi,
    - Devam eden sözleşme ve projelerde tamamlanan ve tamamlanacak işlerin ölçülmesi,
    - Suiistimal ve güvenlik soruşturmaları,
    - Personel ücret ve haklarıyla ilgili aktüeryal tespitler gibi, uzmanlık yöntemleri gerektiren tespit ve hesaplamalar,
    - Hukukî, teknik ve idarî koşul ve hükümlerin yorumlanması,
    - Standartlar Bölüm 1300'e uygun olarak iç denetim faaliyeti kalite geliştirme programının değerlendirilmesi,
    - Birleşme ve devralmalar,

- Risk yönetimi ve diğer konularla ilgili danışmanlık.

4. İç Denetim Yöneticisi, bir dış hizmet sağlayıcısının hizmetlerinden istifade etmek istediği takdirde, ilgili dış hizmet sağlayıcısının yapılacak olan görevle ilgili bağımsızlık ve objektifliğini ve bu konuda gereken vasıflara sahip olup olmadığını değerlendirmeli ve tespit etmelidir. Dış hizmet sağlayıcısının üst yönetim, denetim komitesi veya yönetim kurulu tarafından seçildiği ve İç Denetim Yöneticisinin o dış hizmet sağlayıcısının hizmetlerinden istifade etmek istediği durumlarda da bu değerlendirme ve tespit yapılmalıdır. Bu seçim başkaları tarafından yapıldığı ve İç Denetim Yöneticisi, kendi yaptığı değerlendirme sonucunda, o dış hizmet sağlayıcısının hizmetlerinden istifade etmesine gerek olmadığı sonucuna vardığı takdirde, yapılan bu değerlendirmenin sonuçları duruma göre üst yönetime, denetim komitesine ya da yönetim kuruluna rapor edilmelidir.

5. İç Denetim Yöneticisi, dış hizmet sağlayıcısının görevi yapmak ve yürütmek için gereken bilgi ve becerilere ve diğer vasıflara sahip olup olmadığını tespit etmelidir. Bu vasıfların değerlendirilmesi ve tespitinde, İç Denetim Yöneticisi aşağıdakileri dikkate almalıdır:

   - Dış hizmet sağlayıcısının ilgili bilim dalında yeterliliğini ve uzmanlığını kanıtlayan meslekî ruhsat, sertifika veya diğer belgeler,
   - Dış hizmet sağlayıcısının uygun bir meslek kuruluşuna üye olup olmadığı ve 'o kuruluşun etik kurallarına' uyup uymadığı,
   - Dış hizmet sağlayıcısının itibarı. Bu amaçla, dış hizmet sağlayıcısının iş ve hizmetlerini tanıyan başka kişi ve kurumlarla temas kurulabilir,
   - Dış hizmet sağlayıcısının düşünülen iş tipi hakkında deneyimi,
   - Dış hizmet sağlayıcısının o belirli görevle ilgili olan bilim dallarında aldığı eğitim ve öğretimin niteliği ve düzeyi,

- Dış hizmet sağlayıcısının, ilgili kurumun faaliyet gösterdiği sektördeki bilgi ve deneyimi.

6. İç Denetim Yöneticisi, görev sırasında bağımsızlık ve objektifliğin korunmasını sağlamak amacıyla, dış hizmet sağlayıcısının kurumla ve iç denetim birimiyle ilişkilerini de dikkate almalı ve değerlendirmelidir. Bu değerlendirme kapsamında, İç Denetim Yöneticisi, dış hizmet sağlayıcısının görevini ifa ederken veya sonuçları rapor ederken tarafsız ve önyargısız hüküm ve karar vermesine engel olabilecek herhangi bir mali, örgütsel veya kişisel ilişkisinin bulunmadığından emin olmalıdır.

7. Dış hizmet sağlayıcısının bağımsızlık ve objektifliğini değerlendirirken, İç Denetim Yöneticisi şu etkenleri dikkate almalıdır:

   - Dış hizmet sağlayıcısının kurumda herhangi bir mali çıkar veya pay sahibi olup olmadığı,
   - Dış hizmet sağlayıcısının kurum içinde denetim komitesi, yönetim kurulu, üst yönetim veya başka kişilerle kişisel veya meslekî ilişkisi,
   - Dış hizmet sağlayıcısının denetime konu olan kurumla veya faaliyetlerle geçmiş ilişkileri,
   - Dış hizmet sağlayıcısının kurum için yürütmekte olduğu diğer devam eden hizmetlerin niteliği ve kapsamı,
   - Dış hizmet sağlayıcısının ücreti veya başka gelir ve çıkarları.

8. Dış hizmet sağlayıcısı aynı zamanda kurumun dış denetçisi ise ve ilgili görev genişletilmiş denetim hizmetlerinden oluşuyorsa, İç Denetim Yöneticisi, yapılan işlerin dış denetçinin bağımsızlığını zayıflatmadığından emin olmalıdır. *Genişletilmiş denetim hizmetleri* terimi, dış denetçiler arasında genel kabul gören denetim standartı gereklerinin ötesindeki hizmetler anlamına gelir. Kurumun dış denetçileri aynı zamanda kurumun üst yöneticileri, yöneticileri veya çalışanları olarak görev yapıyorsa veya böyle görünüyorsa,

onların bağımsızlığı bozulmuş sayılır. Buna ek olarak, dış denetçiler kuruma vergi ve benzeri konularda danışmanlık gibi başka hizmetler de verebilir. Ancak, bağımsızlık, kuruma verilen hizmetlerin tamamı dikkate alınarak değerlendirilmelidir.

9. İç Denetim Yöneticisi, dış hizmet sağlayıcısının işlerinin kapsamı hakkında yeterli bilgi edinmelidir. Bu, iç denetim faaliyetinin amaçları karşısında, iş kapsamının yeterliliğini belirlemek için gereklidir. Bu konuların ve ilgili diğer konuların bir denetim bildirim yazısı (*engagement letter*) veya sözleşmeyle kayda geçirilmesi uygun olabilir. İç Denetim Yöneticisi, aşağıda sayılan konuları dış hizmet sağlayıcısı ile birlikte gözden geçirmelidir:
   - İşin hedefleri ve kapsamı,
   - Görev raporları ve bildirimlerine dahil edilmesi beklenen özel konular,
   - İlgili kayıtlara, personele, demirbaşlara ve ilgili mahallere erişim,
   - Uygulanacak prosedürler ve kullanılacak varsayımlar,
   - Varsa, görevle ilgili çalışma kâğıtlarının mülkiyeti ve zilyetliği,
   - Görevin ifası sırasında edinilen bilgilerin gizliliği ve bu konudaki kısıtlamalar,
   - Mümkünse, uluslararası iç denetim standartlarına ve iç denetim faaliyetinin çalışma standartlarına uyuma denetim bildirim yazısında atıfta bulunulması.

10. Dış hizmet sağlayıcısının iç denetim faaliyetleri de yaptığı durumlarda, İç Denetim Yöneticisi, bu işin Uluslararası İç Denetim Standartlarına uygun olması gerektiğini belirtmeli ve uygun olmasını sağlamalıdır. Bir dış hizmet sağlayıcısının yaptığı işi incelerken, İç Denetim Yöneticisi, yapılan işin yeterliliğini değerlendirmelidir. Bu değerlendirme, toplanan ve edinilen bilgilerin varılan sonuçlar için ve önemli anlaşmazlıkların ve

itirazların çözümlenmesi ya da başka olağandışı konular için makul bir temel yaratmak açısından yeterli olup olmadığı değerlendirmesini de kapsamalıdır.

11. Görevle ilgili raporların İç Denetim Yöneticisi tarafından düzenlendiği ve bir dış hizmet sağlayıcısından istifade edilen durumlarda, İç Denetim Yöneticisi, gerektiğinde, bu hizmetlere atıfta bulunabilir. Görevle ilgili raporlarda dış hizmet sağlayıcısının hizmetlerine atıfta bulunulmadan önce, bunun dış hizmet sağlayıcısına bildirilmesi ve gerekirse, onun onayının alınması gerekir.

# Uygulama Önerisi 1210.A2-1: Suiistimal Riskinin Değerlendirilmesi, Önlenmesi ve Tesbitinde Denetçinin Sorumlulukları

Uluslararası İç Denetim Standartlarından
Standart 1210.A2'nin Yorumu

## İlgili Standart

**1210.A2** İç denetçi, suiistimal belirtilerini tesbit edebilecek yeterli bilgiye sahip olmalıdır, fakat esas görev ve sorumluluğu suiistimalleri tesbit etmek ve soruşturmak olan bir kişinin uzmanlığına sahip olması beklenemez.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, suiistimaller konusunda aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun, gerekli bütün hususları ortaya koymak gibi bir amacı yoktur. Bunun yerine, suiistimal konusunda asgarî bir bilgi seviyesi vermeyi ve yapılabilecek bazı uygulamalar hakkında tavsiyede bulunmayı amaçlamaktadır. Bir denetim bölümü ve bölümdeki bireyler için gerekli olan eğitim ve tecrübe seviyesi, yönetim ve yönetim kurulunun İç Denetim Yöneticisinden beklediği danışmanlık ve meslekî hizmetlerin yanı sıra bölüm yönetmeliğinde kendileri için belirlenmiş rollere göre değişiklik göstermektedir. Bu yüzden, işin içine ne kadar derin girilirse o kadar yeterlik gerekmektedir.*

*Bu uygulama önerisi, 1210.A2-2, "Denetçinin, Suiistimalin Saptanması, Raporlanması, Çözüme Kavuşturulması ve İletişim İle İlgili Sorumlulukları" başlıklı uygulama önerisi ile birlikte okunmalıdır.*

### SUİİSTİMAL NEDİR?

*Suiistimal* terimi, kişinin yanlış olduğunu bildiği veya doğru olmadığına inandığı, kasdî aldatma veya yanlış yorumlama özelliklerine sahip bir dizi usûlsüzlük ve yaşa dışı eylem anlamına gelir. Bu uygulama

önerisinde ve U.Ö.1210.A2-2'de, kılavuz, yasal olarak tanımlanan ve/veya genel olarak yolsuzluk olarak bilinen bazı belli faaliyetleri "suiistimal" olarak tanımlayabilir. Suiistimal, kendisine, kuruluşa veya başka birine yaşa dışı bir menfaat sağlayacağını bilen kurum içi ve kurum dışı kişiler tarafından yapılabilir.

1. Kurumun *zararına* yapılan suiistimal, genellikle bir çalışanın, kurum dışı birinin veya başka bir kurumun dolaylı ya da dolaysız yararı için yapılır. Örnekler:
    - Rüşvet alma.
    - Genel olarak kuruma yarar sağlayacak bir işlemin bir çalışana ya da kurum dışından birine yönlendirilmesi.
    - Zimmete para geçirme ve ortaya çıkartılmasını zorlaştırmak için malî raporlarda oynama.
    - Faaliyetler, işlemler veya verilerin kasden gizlenmesi veya yanlış bildirilmesi.
    - Kurumda var olmayan hizmet veya malların var olduğunun iddia edilmesi.
    - Şirketin veya kanunların müdâhil olması gereken yerlerde kasden hatâ yapılması.
    - Gizli veya kişiye ait bilgilerin yetki alınmadan veya yasa dışı yollarla kullanılması.
    - Bilgi teknoloji ağları veya kullanılan sistemlerin yetki alınmadan veya yasa dışı yollarla kullanılması.
    - Hırsızlık.
2. Kurumun *yararına* tasarlanan suiistimal, bu faydayı, genellikle, dışarıdan kişileri de aldatabilecek bir haksız veya sahtekârca avantajı kullanarak sağlar. Bu tür suiistimalleri işleyenler, genellikle ikramiye veya terfi gibi dolaylı yollardan kişisel çıkar

sağlar. Kurumun yararına tasarlanan suiistimallere örnek olarak şunlar gösterilebilir:

- Devlet memurlarına, devlet memurlarının aracılarına, müşterilere veya tedarikçilere ödenen rüşvetler, benzer yasa dışı ödemeler ve yasa dışı siyasî bağışlar gibi usûlsüz ödemeler.
- Diğerlerinin yanı sıra, işlemler, aktifler, pasifler ve gelirlerin kasden yanlış beyan edilmesi veya kasden yanlış kıymet takdiri yapılması.
- Mali satış/devir fiyatlarının kasden yanlış beyan edilmesi (yani, ilgili kuruluşları arasında yapılan mal alım satımında yanlış kıymet takdiri yapılması). Fiyatlandırma tekniklerini kasden yanlış bir şekilde uygulayarak, yönetim, işleme taraf olan bir kurumun faaliyet sonuçlarını, işleme taraf olan diğer kurumun zararına, olduğundan daha iyi gösterebilir.
- Bir tarafın olağan ticarî şartlara tâbi bir işlemden elde edilemeyecek faydalar sağladığı, kasdî ve usûlsüz işlemler.
- Kurumun malî tablosunu dışarıdan kişilere olduğundan daha iyi gösterebilmek amacıyla önemli bilgilerin kasden kaydedilmemesi veya açıklanmaması.
- Hayalî veya yanlış kaydedilen aktiflerin satış veya beyan edilmesi.
- Şirketin veya kanunların müdahil olması gereken yerlerde kasden hatâ yapılması.
- Vergi borçlarını azaltmak için vergiye tabi faaliyetlerde kasdî hatâlar.
- Kanun, kural, yönetmelik veya sözleşmelere aykırı, yasaklanmış ticarî faaliyetler.

Yukarıdakilere ek olarak, suiistimallerin sınıflandırılmasında değişik hususlar vardır. Denetçi, meslekî muhasebe veya suiistimalin soruşturulması konusunda hizmet veren şirket ve kuruluşlar tarafından yayınlanan ve kendi kuruluşu için en uygun sınıflandırma yöntemini gösteren bilgileri araştırmak isteyebilir.

## SUİİSTİMAL NEDEN OLUR?

Suiistimale sebep olan genel anlamda üç etken vardır. Bunlar fırsat, saik (teşvik) ve rasyonalizasyondur (bahane bulmaktır).

### 1. Fırsat

- Bir süreç olağan durumlara özgü olarak uygun biçimde tasarlanmış olabilir. Ancak beklenmeyen ve arzulanmayan durumlarda ortaya çıkabilecek fırsat pencereleri kontrollerin başarısızlığına yol açabilecek olumsuz şartlar yaratabilir.
- Suiistimal fırsatı, yetersiz tasarlanan kontrol veya kontrol eksikliği sebebiyle ortaya çıkabilir. Örneğin, aktifleri korumak için geliştirilen bir sistem önemli bir kontrolü gözden kaçırabilir. Bu boşluğun farkında olan biri, fazla bir çaba sarf etmeden istediklerini alabilir.
- Yönetici pozisyonundaki kişiler, astlarının veya yetersiz kontrollerin kuralları atlatma şansı vermesinden dolayı, mevcut kontrolleri yok edecek fırsatlar oluşturabilirler.

**2. Saik** (teşvik ya da baskı da denebilir)

- İnsanlar yaptıklara şeylere bir bahane ararken, onları bu şekilde davranmaya yönelten bir saik olmalıdır.
- Güç, büyük bir saiktir. Güç, size aileniz veya çalışanlarınızın gözünde itibar kazandırabilir. Meselâ, bilgisayar suiistimallerinin çoğu, bilgisayar korsanlarının (hacker), kasdî bir zarar vermekten çok, korsanın bunu yapacak gücü olduğunu göstermek istemesinden kaynaklanmaktadır.
- Diğer bir saik de hırs veya bağımlılıktır.
- Üçüncü saik, fizikî streslerden veya dış dünyadan gelen baskıdır.

**3. Rasyonalizasyon**

- Çoğu insan, kötü şeyler yapsa da, kendini iyi insan olarak görür. Kendilerini, iyi insan olduklarına ikna etmek için, yaptıklarına *bahane bulur* (rasyonalize ederler) veya yaptıklarını inkâr ederler. Meselâ, bu kişiler eğer birine bir malzemeyi kullanma izni verildiyse veya bir yönetici bir kuralı bozmuşsa, diğer kişilerin de bunu yapmaya hakkı olduğunu düşünür.
- Bazı kişiler, kurum içinde kabul edilemeyen ama kendi kültürleri veya daha önceki iş yerlerinde kabul edilen davranışları yaparlar. Sonuçta, bu kişiler kendileri için bir anlam ifade etmeyen kurallara riayet etmeyeceklerdir.
- Bazı kişiler, bazı dönemlerde malî açıdan dayanamayacakları sıkıntıya düşebilirler, maliyetli bir bağımlılığa saplanabilirler veya diğer baskılara maruz kalabilirler. Bu hallerde, bu parayı ödünç aldıklarını, vaziyetleri düzeldiğinde geri koyacaklarına dair bir bahane üretirler. Diğerleri de, şirketten para çalmanın kötü bir şey olmadığını düşünerek, yapılan suiistimali kendi üzerlerinden atarlar.

Denetçiler, suiistimale sebep olan saik veya bahaneyi tam olarak bilememelerine rağmen, onlardan suiistimal *fırsatlarını* teşhis edecek iç kontroller hakkında yeterince bilgi sahibi olmaları beklenir. Denetçiler, suiistimali işaret eden ve önlenmesini sağlayan işaretlerin yanı sıra, suiistimal şekil ve senaryolarını da iyi bilmelidir. IIA veya diğer meslekî kurum veya kuruluşlardan edinilebilecek bilgiler, denetçinin bilgisinin güncel kalmasını temin edecektir.

## SUİİSTİMAL VE KÖTÜ RİSK DEĞERLENDİRME YÖNETİMİ

Tüm kuruluşlar, insan unsurunun olduğu her süreçte, suiistimale çeşitli derecede maruzdurlar. Kuruluşun maruz kaldığı suiistimal derecesi, bulunduğu işin içinde yer alan suiistimal riskleri ile, suiistimali engellemek ya da teşhis etmek için yapılan etkili iç kontrollerle ve

bu süreçte yer alan kişilerin dürüstlüğü ve bağlılığı ile bağlantılıdır. Suiistimal riski, suiistimalin olma ihtimali ve olduğunda da kuruluşun karşılaşacağı potansiyel zarar ve güçlüklerdir.

Suiistimal ihtimali, genellikle, suiistimal yapmanın kolaylığına, suiistimale götüren saikle ilgili etkenlere ve şirketin suiistimal geçmişine bağlıdır. Suiistimal yönetiminde, malî kayıpların sınırlandırılması veya devre dışı bırakılmasından çok, tüm sonuçların sınırlandırılması veya devre dışı bırakılması vardır. Meselâ, bazı kurumlar için, itibar kaybının, kurumun yetenekli personeli veya ürünleri için müşterileri cezbetme veya mevcutları tutma yeteneğine etkisinin yanı sıra, işin büyümesi ve devamı için gerekli olan ruhsatların ve imkânların edinilmesi üzerinde önemli derecede kötü etkisi vardır.

Suiistimal riskinin değerlendirilmesinde iç denetçiler, varsa, kurumun kurumsal risk yönetim modelini kullanmalıdır. Aksi takdirde, denetçiler aşağıdaki kılavuzları kullanabilirler:

1. Kurumu tehdit edebilecek özel suiistimal yapılarının anlaşılması. Kurumun bu suiistimallere maruziyetini değerlendirmek ve bunları açıklıkla ortaya koymak için, kurumdaki mevcut bütün riskleri içine alan bir risk modelinin kullanılması. Bu risk modeli, tutarlı kategorileri de kullanmalı (diğer bir deyişle, risk alanları birbiriyle kesişmemeli) ve yüksek risk alanlarının teşhis edilip kapsam içine alınması için bir risk değerlendirmesi yapacak kadar ayrıntılı olmalıdır.

COSO'nun (Treadway Komisyonu Sponsor Kurumlar Komitesi'nin) Kurumsal Risk Yönetim Çerçevesi aşağıdaki konuları içeren yararlı bir model sunmaktadır:

- **Olayın Teşhis Edilmesi:** Beyin fırtınaları, mülâkatlar, odak grupları, anketler, sektör araştırması ve olay envanterleri.
- **Risk Değerlendirmeleri:** İhtimal ve sonuçların içerir.
- **Riske Cevap Stratejileri:** Yönetmek, transfer etmek, üstlenmek

veya riski ortadan kaldırmak.

- **Kontrol Faaliyetleri:** Riskleri mevcut suiistimal karşıtı programlarla ve kontrol faaliyetleriyle bağlantılandırmak ve bu program ve faaliyetlerin etkinliğini artırmak.
- **İzleme/Gözleme:** Kötü yönetim sebebiyle herhangi bir tedbir alınmamış (bakiye) suiistimal ve risklerin ele alındığı denetim plan ve programları.

2. Bir kuruluştaki suiistimal risklerini önleme veya azaltma amaçlı kontrolleri değerlendirirken, maliyet ve fayda değerlendirmesi yapılmalıdır. Değerlendirmede suiistimalin tek bir kişi veya bir grup tarafından yapılıp yapılamayacağı da ele alınmalıdır. Uygulamada, suiistimalin %100 engellenmesi ne mümkündür ne de bunun maliyet etkinliği vardır. Değerlendirmelere, çalışanlardan yanlış yere şüphelenmenin veya çalışanlara güven duyulmadığı havasının olumsuz etkisi de katılmalıdır.

## SUİİSTİMALİN ENGELLENMESİ VEYA CAYDIRILMASININ UNSURLARI

Suiistimalin engellenmesi, suiistimali yapacak olan kişileri bundan vazgeçirmeyi ve suiistimal olduğunda suiistimal riskini sınırlamak için alınan tedbirleri içerir. Suiistimalin engellenmesindeki *ana* mekanizma *iç kontroldür*. İç kontrolün tesis edilmesi ve çalıştırılmasındaki baş sorumlu, *yönetimdir*.

Aşağıda, COSO kontrol çerçevesinde bir örnek olarak sunulan bir suiistimal engelleme programının kontrol öğelerinden bazıları bulunmaktadır. Denetçinin hangi kontrol çerçevesini kullandığına bakılmaksızın her öğenin değerlendirmeye alınması gerekmektedir.

**1. Kontrol Ortamı.** Şirketler aşağıdaki noktaları kapsayan uygun bir kontrol ortamı tesis etmelidirler:

- Yönetim kuralları, etik politikası veya yönetimin tarzını ortaya koyacak suiistimal politikası.

- Endişelerin ortaya konduğu etik ve ihbar programları.
- İstihdam ve prim kılavuzları ve uygulamaları.
- Denetim komitesi, yönetim kurulu veya diğer kurulların gözetimi.
- Bildirilen konuların soruşturulması ve teyid edilen aksaklıklara çözüm bulunması.

2. **Suiistimal Risk Değerlendirmesi.** Kuruluşlar, yanlış mali rapor, aktiflerin yanlış değerlendirilmesi, yanlış harcama faturaları veya yönetimin aldığı yanlış malî kararlar dâhil suiistimal ile ilgili tüm riskleri teşhis etmeli ve değerlendirmelidir. Şirketler, ayrıca, görevler ayrılığı ilkesinin uygun şekilde yapılıp yapılmadığını da değerlendirmelidir.

3. **Kontrol Faaliyetleri.** Şirketler, yanlış mali raporlamaların, şirket varlıklarının yanlış kullanılmasının, uygunsuz tahsilat ve harcamaların teşhisi, engellenmesi ve en aza indirilmesi için yönetimin alacağı tedbirler dâhil, etkili kontroller tesis etmeli ve tatbik etmelidir. Ayrıca şirketler, çalışanların kurumsal politikaları okuyup anladığından ve bunlara bağlı olduğundan emin olunmasını sağlayacak bir teyid veya kabul süreci oluşturmalıdır.

4. **Bilgi ve İletişim.** Şirketler, suiistimal ile ilgili etkili bilgi ve iletişim uygulamaları, ahlakî çelişkilerin tartışıldığı ortamlar, iletişim kanalları ve hizmet içi eğitim ortamları oluşturmalıdır. Suiistimalin önlenmesine yönelik sürekli gözetim yazılımları gibi teknolojileri kullanmalıdır. Bu konuda politikalar ve kılavuzlar hazırlanmalı ve personele duyurulmalıdır.

5. **İzleme/Gözleme.** Şirketler, sürekli ve dönemsel performans değerlendirmeleri yapmalı ve suiistimalin engellenmesinde bilgisayar teknolojisi kullanımının etkisini değerlendirmelidir.

**İç Denetçinin Rolü**

İç denetçilerin, kurum içindeki potansiyelin büyüklüğü ile orantılı olarak, iç kontrol sistemlerinin uygunluk ve yeterliğinin test ve

değerlendirmesini yaparak suiistimalin önlenmesinde şirketlere yardımcı olma sorumlulukları vardır. Bu sorumluluklarını yerine getirirken, iç denetçiler şunları dikkate almalıdırlar.

1. **Kontrol ortamı.** Kontrol ortamının özelliklerinin değerlendirilmesi, suiistimal öncesi denetim ve incelemelerin yönetilmesi, suiistimal denetimlerinin sonuçlarının raporlanması, suiistimale çözüm çabalarına destek verilmesi. Bazı durumlarda, iç denetçilerin faal ihbar hattı da olabilir.

2. **Suiistimal risk değerlendirmesi.** Yönetimin suiistimal risk değerlendirmesinin değerlendirilmesi; özellikle teşhis, değerlendirme ve potansiyel suiistimal ve tedarikçilerin, müteahhitlerin ve diğer tarafların da dâhil olduğu yanlış model ve senaryolarının test edilme süreçleri.

3. **Kontrol faaliyetleri.** Suiistimal ile ilgili kontrollerin tasarımı ve işleyiş etkinliğinin değerlendirilmesi; denetim plan ve programlarının, aşırı risk ve birleşik suiistimal denetimlerine hitap etmesinin temin edilmesi; bir suiistimal veya hırsızlığın özelliklerine bakarak tesislerin tasarımının değerlendirilmesi ve kanunlar, düzenlemeler veya sistemler ve bunların kontroller üzerindeki etkilerinin gözden geçirilmesi.

4. **Bilgi ve iletişim.** Bilgi ve iletişim sistemlerinin ve uygulamalarının etkililiğinin değerlendirilmesi ve suiistimal ile ilgili eğitim inisiyatiflerine destek verilmesi.

5. **İzleme/Gözleme.** İzleme/gözleme faaliyetlerinin ve ilgili bilgisayar yazılımlarının değerlendirilmesi; incelemelerin yapılması, denetim komitesinin kontrol ve suiistimal ile ilgili gözetim çalışmasının desteklenmesi ve uygun suiistimal denetimi ve soruşturması tecrübesine sahip çalışanların istihdam edilmesi ve eğitilmesi.

## SUİİSTİMALİN TESBİTİ

Yönetim ve iç denetim biriminin, suiistimalin tesbiti konusunda farklı rolleri vardır. Bu rollerin tanımları şöyledir:

### Suiistimalin Tesbitinde Yönetimin Rolü

Yönetim, makul bir maliyetle etkili bir kontrol sisteminin tesis ve tedarikinden sorumludur. Bunun içinde, diğer kontroller etkili çalışmadığında bazı kontrollerin tasarlanması da vardır. Bu belirtilerin takibi, suiistimali ortaya çıkartabilir.

İzleyici bir kontrole örnek olarak, faal bir ihbar hattının tesis edilmesi ve iletişime sunulmasını veya müşteri veya çalışanların, endişelerini belirlemek ve şikâyette bulunmak için kullanacakları benzer bir sistemi verebiliriz. Diğer izleme ve tesbit kontrollerinde şunlar vardır:

- Kapı ve pencerelere alarm takılması.
- İzleme kameralarının yerleştirilmesi.
- Bilgi sistemleri için kontrollerin tasarlanması.
- Envanter sayımının yapılması.
- Denetim.
- Fatura ve maliyet merkezi giderlerinin gözden geçirilmesi ve onaylanması.
- Hesapların mutabakatı.

### Suiistimalin Tesbitinde İç Denetçinin Rolü

Normal bir denetimde incelenen faaliyetlerde suiistimalin varlığı durumunda, suiistimalin tesbiti için, iç denetçiler 1220 numaralı iç denetim standardında belirtilen azamî meslekî özen ve dikkati gösterme sorumluluğundadır.

Ancak, iç denetçilerin çoğundan, aslî sorumluluğu suiistimalleri tesbit etmek ve soruşturmak olan bir kişinin sahip olduğu bilgiye sahip olmaları beklenmemektedir. Ayrıca, uygulanmalarında gerekli meslekî

özen gösterilse bile, sadece denetim prosedürleri de suiistimalin tesbitini garanti edemezler.

İyi tasarlanmış bir iç kontrol sistemi, suiistimale meydan vermemelidir. Denetçiler tarafından yapılan testler, var olan suiistimal belirtilerinin tesbit edilme ve daha ayrıntılı bir inceleme için dikkate alınma ihtimalini arttırır.

Denetim sırasında, iç denetçinin suiistimalin tesbitiyle ilgili sorumlulukları şunlardır:

- Kontrol tasarımlarının değerlendirilmesindeki suiistimal risklerinin dikkate alınması ve atılacak denetim adımlarının tesbiti. İç denetçilerin suiistimal ve usûlsüzlükleri tesbit etmesi beklenmediği durumlarda, gözlem altındaki süreçteki iş hedefleri için makul güvencenin sağlanması ve maddî kontrol zaafiyetlerinin - basit hatâ veya kasdî çabalar sonucunda da olsa- tesbit edilmesi beklenmektedir.
- Bir suiistimalin yapılmış olabileceğini gösteren bulgu ve belirtileri tesbit etmek için suiistimal hakkında yeterli bilgi sahibi olmak. Bu bilgi, suiistimalin özelliklerini, suiistimal yapmak için kullanılan teknikleri ve incelenen faaliyet ve işlemlerde görülebilen suiistimal türleri hakkındaki bilgileri de kapsar.
- Suiistimale yol açabilecek ve zemin hazırlayabilecek kontrol zaafiyetleri gibi konulara karşı uyanık olmak. Önemli ve ciddî kontrol zaafiyetleri tesbit edildiği takdirde, iç denetçiler tarafından yapılan ek testler başka suiistimal belirtilerinin tesbitine yönelik testleri de içermelidir. Bazı belirti örnekleri: Yetkisiz işlemler, kontrollerin aşılması, açıklanamayan fiyat sapmaları ve olağandışı fazla ürün kayıpları. İç denetçiler, her hangi bir zamanda birden fazla belirtinin bir arada mevcut olmasının, suiistimalin yapılması ihtimalini arttırdığını bilmelidir.
- Suiistimal yapıldığını gösteren belirtileri değerlendirmek ve ek bir tedbire gerek olup olmadığına ya da bir soruşturma açılmasının önerilmesine gerek olup olmadığına karar vermek.

- Bir soruşturma açılmasını önermek için suiistimal hakkında yeterli belirtinin ve bulgunun mevcut olduğu tesbiti yapıldığı takdirde, durumu kurum içinde uygun yetkili kişi ve birimlere bildirmek.

# Uygulama Önerisi 1210.A2-2 Suiistimalin Soruşturulması, Raporlanması, Çözüme Kavuşturulması ve İletişim İle İlgili Denetçinin Sorumlulukları

Uluslararası İç Denetim Standartlarından
Standart 1210.A2'nin yorumu

## İlgili Standart

**1210.A2** İç denetçi, suiistimal belirtilerini tesbit edebilecek yeterli bilgiye sahip olmalıdır, fakat esas görev ve sorumluluğ suiistimalleri tesbit etmek ve soruşturmak olan bir kişinin uzmanlığına sahip olması beklenemez.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, suiistimaller konusunda aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun, gerekli bütün hususları ortaya koymak gibi bir amacı yoktur. Bunun yerine, suiistimal konusunda asgarî bir bilgi seviyesi vermeyi ve yapılabilecek bazı uygulamalar hakkında tavsiyede bulunmayı amaçlamaktadır. Bir denetim bölümü ve bölümdeki bireyler için gerekli olan eğitim ve tecrübe seviyesi, yönetim ve yönetim kurulunun İç Denetim Yöneticisinden beklediği danışmanlık ve meslekî hizmetlerin yanı sıra bölüm yönetmeliğinde kendileri için belirlenmiş rollere göre değişiklik göstermektedir.Bu yüzden, işin içine ne kadar derin girilirse o kadar yeterlik gerekmektedir.*

*Bu öneri uygulaması, 1210.A2-1, "Suiistimal Riskinin Değerlendirilmesi, Önlenmesi ve Tespitinde Denetçinin Sorumlulukları" başlıklı uygulama önerisi ile birlikte okunmalıdır.*

### Suiistimalin Soruşturulması

Uygulama önerisinin bu bölümü, "denetim tarafından, analizler sonucu suiistimal riskinin yüksek olduğu belirlenen süreç veya işlemlerdeki suiistimal belirtilerini önceden tespit etmek için tasarlanan bir denetim"

olarak tanımlanan "suiistimal denetimi" faaliyetine yönelik değildir. Bu kılavuz, kurum içinde kontrol hatâları veya suç işleme şüphesi üzerine endişeler oluştuğunda başlatılan incelemelere yöneliktir. Şüpheler, resmî bir şikâyet sürecinden, gayriresmî duyumlardan veya suiistimali test etmek için tasarlanan bir denetimi de içermek üzere bir denetimden kaynaklanabilir.

Bir suiistimalin soruşturulması, belirli ayrıntılarla ilgili yeterli bilgi toplamak ve suiistimalin olup olmadığının, suiistimalden kaynaklanan kayıp ve risklerin boyutunun, suiistimali kimlerin yaptığının ve suiistimalin yapısının (nasıl gerçekleştiğinin) belirlenmesi için gerekli prosedürleri uygulamak gibi hususları kapsar. Suiistimal soruşturmalarının en önemli sonuçlarından biri, masum kişilerin şüpheli durumdan kurtulmalarıdır.

Soruşturmalar, sadece soruşturmanın başlamasına sebep olan olayı değil, suiistimal faaliyetinin bütün yapısını ve büyüklüğünü ortaya çıkartacak şekilde tasarlanmalıdır. Soruşturma çalışması, sürecin kanunî yollar için gerekli çalışma kâğıtlarının/dosyaların hazırlanmasını da içerir.

İç denetçiler, avukatlar, soruşturmacılar, güvenlik personeli ve kurum içinden veya dışından diğer uzmanlar, genellikle suiistimal soruşturmalarını gerçekleştiren veya buna yardımcı olan taraflardır.

Soruşturmalar ve çözüm için düşünülen yollar, yerel kanunlar göz önüne alınarak dikkatli bir şekilde değerlendirilmelidir. Soruşturmaların nasıl ve nerede yapılacağı, telâfi/tazmin uygulamaları, disiplin uygulamaları, soruşturma ile ilgili iletişimin ne şekilde olacağı hâlen yürürlükteki mevzuat ile belirlenmiş olabilir. Kurumun hukuk danışmanı ile birlikte çalışmak ve ilgili kanunlara âşina olmak, hem meslekî hem de yasal açıdan, denetçinin menfaatinedir. Bu kılavuz, uluslararası içeriktedir ve bu yüzden yapısı itibariyle genel bir anlam taşımaktadır.

**Yönetimin Rolü**

Yönetim, soruşturma süreciyle ilgili kontrolleri geliştirmekten sorumludur. Bu sorumluluk, soruşturmaların etkin şekilde yapılması için gerekli politika ve prosedürlerin hazırlanmasını ve soruşturma sonuçlarının sağlıklı alınması, raporlandırılması ve iletişim için gerekli olan standartların geliştirmesini de ihtiva eder. Bu gibi standartlar genelde bir suiistimal politikasında ayrıntılandırılır ve iç denetim bu politikanın geliştirilmesinde rol alabilir.

Bu gibi politika ve prosedürler, işin içinde yer alan kişilerin haklarını, soruşturmayı yapacak kişilerin özelliklerini ve suiistimalin olduğu veya soruşturulduğu yer ve ülkedeki mevzuat hükümlerini dikkate almak zorundadır. Politikalar, zararları tazmin/telâfi etmek ve kamusal ve cezaî dava süreci için yasal önlemler almak da dahil olmak üzere, yönetimin çalışanları, tedarikçileri veya müşterileri ne şekilde müeyyideye bağlayacağını dikkate almalıdır. Özellikle soruşturmacılar ve hukuk müşaviri arasındaki ilişki olmak üzere, soruşturmada yer alan çeşitli görevlilerin yetki ve sorumluluklarının açık bir şekilde belirtilmesi, yönetim açısından önemlidir. Ayrıca, bilhassa başlangıç aşamasında iken, devam eden soruşturma ile ilgili dahilî yazışmaları asgarîye indirecek prosedürlerin tasarlanması ve buna uyulması yönetim için önemlidir.

Politika, suiistimalin gerçekleştirildiğine dair kararı verecek olan soruşturmacının rolünü belirlemelidir. Yönetim, suiistimal ile ilgili sonuca soruşturmacının veya yönetimin mi varacağına ya da şirketin delilleri bu konuda karar vermek üzere dışarıdan bazı yetkililere mi sunacağına karar vermelidir. Suiistimalin olduğuna dair bir hüküm, bazı ülkelerde sadece yargı makamları tarafından verilebilir. Soruşturma, sadece kurum politikasının ihlâl edildiğine dair bir hüküm ile de sonuçlandırılabilir.

**İç Denetçinin Rolü**

Soruşturmalarda iç denetçinin rolü, suiistimal politikalarının yanı sıra

iç denetim yönetmeliğinde de belirtilmelidir. Meselâ, iç denetim, suiistimalin soruşturulmasında öncelikli sorumluluk sahibi olabilir, soruşturmalar için kaynak vazifesi görebilir veya (soruşturmaların etkililiğinin değerlendirilmesinden sorumlu oldukları için) soruşturmalarda yer almayabilirler. İç denetimin bağımsızlığı üzerindeki tesiri uygun şekilde dikkate alınıp gözetildiği sürece, bu rollerin her biri kabul edilebilir.

Meslekî yeterlilik kıstasını sağlamak için, suiistimal soruşturma ekiplerinin, suiistimalin yapısı, soruşturma teknikleri ve ilgili mevzuat hakkında yeterli bilgi edinme sorumluluğu vardır. Soruşturmacılara ve adlî uzmanlara eğitim hizmeti ve sertifikasyon veren ulusal ve uluslararası programlar vardır.

İç denetim birimi, soruşturmaların yapılmasından sorumlu ise, kendi personelini kullanarak veya dışarıdan gelenlerle ya da her ikisini de birleştirerek soruşturmayı yürütebilir. Bazı durumlarda, iç denetim, yardımcı olması amacıyla, kuruluşun denetim dışındaki çalışanlarından da yararlanabilir.

Soruşturma ekibinin gecikme olmadan bir araya getirilmesi genellikle çok önem arz eder. Eğer kurumda dışarıdan uzmanlara ihtiyaç varsa, iç denetim yöneticisi, dışarıdan hizmet sağlayıcıları önceden tespit etmeli ve böylece dış kaynaklara hızla ulaşılması sağlanmalıdır.

Soruşturma görevindeki öncelikli sorumluluğun iç denetime verilmediği şirketlerde, denetçilerden bilgi toplamaları ve iç kontrolün gelişimi için tavsiyelerde bulunmaları istenebilir.

**Soruşturmacının Rolü (iç denetime veya başka bir yere görevlendirildiğinde)**

Kuruluşun soruşturma prosedür veya protokollerine bağlı kalınarak, her bir soruşturma için bir soruşturma planı geliştirilmelidir. Baş soruşturmacı, soruşturmanın etkili bir şekilde yürütülmesi için gerekli

olan bilgi, beceri ve diğer vasıfları belirlemeli ve ekibe yeterli ve uygun kişileri almalıdır. Bu süreçte, soruşturmaya dâhil olan çalışanlar ile veya kurumun diğer çalışanları ile arasında her hangi bir muhtemel menfaat çatışması olmaması temin edilmelidir.

Plan, aşağıdaki amaçlara cevap verecek yöntemleri kapsamalıdır:

- Gözetim, mülâkat veya yazılı ifade alma gibi yollarla bilgi toplama.
- Delil toplamaya dair mevzuat ve delillerin kullanılma şekli dikkate alınarak, delillerin tevsiki.
- Suiistimalin büyüklüğünün belirlenmesi.
- Suiistimal yapılırken kullanılan tekniklerin belirlenmesi.
- Sebeplerin değerlendirilmesi.
- Faillerin teşhis edilmesi.

Bu süreçteki her hangi bir noktada, soruşturmacılar, şikâyet veya şüphelerin asılsız olduğu sonucuna varıp, süreci bitirebilir.

Faaliyetler, soruşturma süresi boyunca yönetim, hukuk danışmanı ve insan kaynakları, sigorta risk yönetimi gibi diğer uzmanlarla eşgüdümlü bir şekilde yürütülmelidir.

Soruşturmacılar, bilgili olmalı ve soruşturma kapsamındaki kişilerin bireysel haklarının ve kuruluşun kendi itibarının şuurunda olmalıdır.

Kurum içindeki suiistimaldeki suç ortaklığının seviye ve boyutları değerlendirilmelidir. Bu değerlendirme, önemli delillerin yok edilmemesi veya delil olma özelliğine zarar gelmemesi ve işin içinde olan kişilerden yanıltıcı bilgi alınmasının engellenmesi açısından çok önemlidir.

**Suiistimalin Raporlanması**

Suiistimalin raporlanmasında, suiistimal soruşturmasının sonuç ve

durumuyla ilgili, süreç içinde veya sonunda yönetim ve/veya yönetim kuruluyla iletişimi kapsayan sözlü veya yazılı iletişim araçları vardır. Raporlama, soruşturmanın her aşamasında yapılabilir. Yazılı bir rapor, yönetim ve yönetim kuruluna yapılan sözlü bir açıklamadan sonra verilebilir.

*Uluslararası İç Denetim Standartları'ndan Standar*t 2400'de, denetim görevi iletişimleriyle ilgili bilgi verilmektedir. Suiistimal konusunda iç raporlandırma ile ilgili ilâve bilgiler şunlardır:

- Suiistimal ile ilgili sunulan sonuç rapor taslağı, gözden geçirilmesi için hukuk danışmanına verilmelidir. Müşteri önceliğini öne çıkarabilen bir kurumun, böyle bir karar vermesi durumunda, rapor mutlaka hukuk danışmanına verilmelidir.
- Önemli bir suiistimal veya güven sarsılması durumunun belirli bir kesinlik derecesi kazanması hâlinde, üst yönetim ve yönetim kurulu durumdan derhal haberdar edilmelidir.
- Bir suiistimal soruşturmasının sonuçları, suiistimalin kurumun malî durumunda ve hâli hazırda yayınlanmış bir ya da daha fazla yıllık faaliyet sonuçlarında daha önceden tespit edilmemiş ters bir etkiye sebep olduğunu ortaya koyabilir. Böyle bir şeyin ortaya çıkartılması hâlinde üst yönetim ve yönetim kurulu derhal konudan haberdar edilmelidir.
- Soruşturmanın sonunda, yazılı bir rapor veya başka bir resmî belge yayınlanmalıdır. Bu rapor ya da belgede, soruşturmaya başlama sebebi, zaman aralıkları, gözlemler, varılan sonuçlar, getirilen çözümler ve kontrolleri geliştirmek için alınan önlem (veya yapılan tavsiyeler) bulunmalıdır. Soruşturmanın nasıl çözüme kavuşturulduğuna göre, rapor, soruşturma kapsamındaki bazı kişileri gizlilik kapsamına alarak yazılmalıdır. Bu raporun içeriği hassastır ve yasal gereklilikler, kısıtlamalar ve şirket politika ve prosedürleriyle uyum içinde olurken üst yönetim ve yönetim kurulunun ihtiyaçlarına da cevap verebilmelidir.

**Suiistimallerin Çözümü**

Suiistimallerin çözüme kavuşturulmasından iç denetçi ya da soruşturmacı değil, *yönetim sorumludur*. Çözümün kapsamında, bir suiistimal ve fail(ler)i soruşturulduktan ve deliller gözden geçirildikten sonra, kurumun alacağı tedbirler bulunmaktadır.

İç denetçiler, ulaştıkları tesbitleri değerlendirmeli ve suiistimale sebep olan kontrol zaafiyetlerine getirilecek çözümler konusunda yönetime bilgi vermelidir. Denetçiler, mutad denetim programlarına ilâve adımlar eklemeli veya gelecekte benzer suiistimallerin varlığını ortaya çıkarabilmek için "suiistimal denetimi" programları geliştirmelidir.

Yönetimin suiistimal politika ve prosedürlerinde (uygulama önerisinde daha önce bahsedilmiştir), her bir süreçte kimin yetkili ve sorumlu olduğu tanımlanmalıdır. Bu faaliyetlerin iç denetimin bağımsızlığı üzerindeki etkisi kabul edilip buna uygun şekilde davranıldığı sürece, iç denetçiler, aşağıdaki süreçlerde danışman olarak yer alabilirler. Çözüm aşağıdakilerin hepsini veya bir bölümünü kapsayabilir:

- Başta şüphe duyulan ama daha sonra masum olduğu anlaşılan kişiye bilgi verme.
- Bir endişesini ileten kişiye bilgi verme.
- Bir çalışanı, şirket standartlarına, istihdam kurallarına veya çalışanın sözleşmesine göre cezalandırma.
- Çalışandan, müşteriden veya tedarikçiden zararın gönüllü olarak tazmininin istenmesi.
- Tedarikçi ile sözleşmenin sona erdirilmesi.
- Olayın adlî makamlara, emniyet güçlerine veya benzeri kurumlara bildirilmesi ve onların soruşturmasına yardım edilmesi.
- Dava açılması veya benzeri süreçlere başvurulması.
- Sigortaya başvurma.
- Failin meslek birliğine şikâyette bulunma.

Müşterilere tavsiyelerde bulunmanın yanı sıra, iç denetçiler şunlarda yer alabilirler:

- (İç denetimin soruşturma yapma sorumluluğunun olmadığı yerlerde) kurumun ilgili politika, prosedür ve kanun ve düzenlemelere uyduğunu temin etmek için, soruşturma sürecinde bulunmak.
- Zimmete geçirilen veya ilgili varlıkların konumlandırılması ve/veya güvence altına alınması.
- Kuruluşun hukukî, sigorta veya diğer tazmin/telâfi tedbirlerine destek verme.
- Kuruluşun iç ve dış soruşturma-sonrası raporlama ve iletişim planları ve uygulamalarının değerlendirilmesi ve izlenlenmesi.
- Tavsiye edilen kontrol iyileştirmelerinin uygulamasını, zamanlama, etkililik ve verimliliği teminen izleme.

**İletişim Araçları**

Yanlış ve/veya eksik bilginin gayri resmî yollardan yayılma riskini sınırlandırmak için, iç denetçiler, iletişim stratejisi ve planının tasarlanması konusunda soruşturmanın mümkün olan en erken safhasında, yönetime tavsiyede bulunabilirler.

Yukarıda belirtilen suiistimalin raporlandırılmasına ek olarak, soruşturmadan çıkartılacak iki çeşit *iletişim şekli* vardır: Kamu iletişim araçları ve planlı iç iletişim araçları.

Yönetim tarafından basına, adlî makamlara veya diğer dış taraflara verilen her beyanat, hukuk danışmanı ile eşgüdümlü bir şekilde gerçekleştirilmelidir. Beyanatlar, sadece yetkili sözcüler tarafından verilmelidir.

İç iletişim araçları, yönetim tarafından onun kurum içindeki bütünlüğü güçlendirmesi açısından, şirket politikaları ihlâl edildiğinde gerekli

davranışın yapıldığını gösteren ve iç kontrollerin neden önemli olduğunu vurgulayan stratejik bir araçtır. Bu gibi iletişim araçları haber bülteni veya idarî bir açıklama şeklinde olabilir. Bu durum, kurumda iş dürüstlüğü üzerine verilen bir eğitimde örnek olarak da kullanılabilir. Tüm bu iletişim araçları, genellikle durum şirket içinde çözüme kavuşturulduktan sonra kullanılır ve faillerin isimleri ve de soruşturmanın ayrıntıları gibi mesaj için gerekli olmayan veya yasalara aykırı düşen hususlara yer verilmez.

Bir soruşturma ve sonuçları, özellikle suiistimal halk tarafından öğrenildiğinde, kuruluşu zora sokan bazı gerilimlere veya ahlakî sorunlara sebep olabilir. Yönetim, bu durum için herkesin söz aldığı bir toplantı ve/veya bir takım kurma stratejisi planlayabilir.

**Suiistimal İle İlgili İç Kontrol Sistemi Üzerine Bir Düşüncenin Oluşturulması**

Yönetim veya yönetim kurulu, iç denetçiden, suiistimal ile ilgili olarak şirketin iç kontrol sistemi üzerine bir düşünce oluşturmasını isteyebilir. Denetçiler, bir düşünce ortaya koymadan önce ilgili bilgilere yeterince sahip olduklarından emin olmak için, 2410 numaralı standartlar ve "*İç Kontroller Üzerine Bir Fikrin Sunulmasında İç Denetimle İlgili Uygulamalı Hususlar*" gibi diğer IIA uygulama yardımlarına başvurmalıdır.

# Uygulama Önerisi 1220-1: Azamî Meslekî Özen ve Dikkat

Uluslararası İç Denetim Standartlarından
Standart 1220'nin Yorumu

## İlgili Standart

**1220 Azamî Meslekî Özen ve Dikkat**
İç denetçiler, makul sınırlar içinde tedbirli ve ehil bir iç denetçiden beklenen beceriye sahip olmalı, azamî özen ve dikkati göstermelidir. Azamî meslekî özen ve dikkat, hiç hatâ yapılmayacağı anlamına gelmez.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, azamî meslekî özen ve dikkati değerlendirirken aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun bu değerlendirmede gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Azamî meslekî özen ve dikkat, aynı veya benzer durum ve koşullarda, makul sınırlar içinde tedbirli ve ehil bir iç denetçiden beklenen beceri, özen ve dikkatin gösterilmesi anlamına gelir. Bu nedenle, meslekî özen ve dikkat seviyesi, üstlenilen iş ve görevin karmaşıklık düzeyine uygun olmalıdır. Gereken meslekî özen ve dikkati gösterirken, iç denetçiler, kasdî suç, hatâ, ihmal, verimsizlik, yanlış kullanım, etkisizlik, yararsızlık ve çıkar çatışmaları olasılığı konusunda uyanık olmalıdır. İç denetçiler, usulsüzlük olasılığının en yüksek olduğu koşul ve faaliyetler konusunda da tetikte olmalıdır. Ayrıca, iç denetçiler, yetersiz kontrolleri tespit etmeli ve kontrol konusunda kabul edilebilir prosedür ve uygulamalara uymak için geliştirilmesi gereken konularda tavsiyelerde bulunmalıdır.

2. Azamî özen ve dikkat standardı, hiç hatâ yapmamayı ya da

olağanüstü performans göstermeyi değil, sadece makul dikkat ve beceriyi gerektirir. Azamî özen ve dikkat standardı, iç denetçinin inceleme, kontrol ve denetimleri makul sınırlar içinde yapmasını gerektirir, fakat *bütün işlemlerin* ayrıntılı bir şekilde incelenmesini ve kontrol edilmesini gerektirmez. Bundan dolayı, iç denetçiler, hiç bir aykırılığın veya usulsüzlüğün olmayacağı konusunda kesin ve mutlak bir garanti veremez. Bununla birlikte, iç denetçi, bir iç denetim görevini üstlendiğinde, önemli usulsüzlük veya aykırılık olasılıkları dikkate alınmalıdır.

# Uygulama Önerisi 1220-2: Bilgisayar Destekli Denetim Teknikleri (BDDT'ler[1])

Uluslararası İç Denetim Standartlarından
Standart 1220.A2'nin Yorumu

## İlgili Standart

**1220.A2 Azamî Meslekî Özen ve Dikkat**
Azamî meslekî özen ve dikkati gösterirken, iç denetçi, bilgisayar destekli denetim tekniklerini ve diğer veri analiz tekniklerini kullanmayı düşünmelidir.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu-Bilgisayar Destekli Denetim Tekniklerinin Kullanılması, Doküman G3'ten uyarlanmıştır. Bahsi geçen BS Denetim kılavuzu ISACA tarafından Aralık 1998'de yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, Bilgisayar Destekli Denetim Tekniklerini kullanarak iç denetim yaparken aşağıdaki önerileri de dikkate almalıdırlar. Ancak bu kılavuzun Bilgisayar Destekli Denetim Tekniklerinin kullanımı için gereken bütün prosedürleri kapsamak gibi bir amacı yoktur; kılavuz, sadece, ayrıntılı planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumlulukları hakkında bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

## 1. KILAVUZA DUYULAN İHTİYAÇ:

Bilgisayar Destekli Denetim Teknikleri, denetçilerin denetimler sırasında kullandığı önemli araçlardır. BDDT'ler; genelleştirilmiş denetim yazılımı, yardımcı program, test verileri, uygulama

[1] Bilgisayar Destekli Denetim Teknikleri: Computer-assisted Audit Techniques (CAATs)

yazılımı izleme (tracing) ve eşleme (mapping) ve denetim uzman sistemleri gibi pek çok tipte araç ve teknikler içerir. BDDT'ler, aşağıda sayılanlar da dahil çeşitli denetim prosedürlerini uygulamak amacıyla kullanılabilirler:

- İşlem ayrıntıları ve bakiyelerine ilişkin testler
- Analitik inceleme prosedürleri
- Bilişim Sistemleri (BS) genel kontrollerinin uyum testleri
- BS uygulama kontrollerinin uyum testleri
- Sızma (penetration) testi

BDDT'ler, denetimlerde oluşturulan denetim bulgularının ve delillerinin büyük bir kısmını üretebilirler. Bu nedenle denetçi, BDDT'lerin kullanımını dikkatle planlamalı ve kullanım sırasında gereken meslekî özeni göstermelidir.

## 2. PLANLAMA:

**BDDT'lerin Kullanımı İçin Karar Faktörleri:**
Denetimi planlarken, denetçi, manuel tekniklerin ve BDDT'lerin uygun bir kombinasyonunu kullanmayı düşünmelidir. BDDT'lerin kullanılıp kullanılmayacağının belirlenmesinde dikkate alınması gereken faktörler şunları içerir:

- Denetçinin bilgisayar bilgisi, uzmanlığı ve tecrübesi
- Uygun BDDT'lerin ve BS olanaklarının bulunup bulunmadığı
- Manuel tekniklere kıyasla BDDT'leri kullanmanın etkinliği ve verimliliği
- Zaman kısıtı
- Bilişim sistemi ve bilgi teknolojisi ortamının bütünlüğü
- Denetim risklerinin düzeyi

**BDDT Planlama Adımları:**
Denetçinin seçtiği BDDT'lerin uygulanmasına hazırlanırken atması gereken temel adımlar şunlardır:

- BDDT'lerin denetim hedeflerini belirlemek
- Kurumun BS olanakları, programları/sistemi ve verilerinin kullanılabilirliği ve erişilebilirliğini tespit etmek
- Uygulanacak prosedürleri (örneğin istatistiksel örneklem, yeniden hesaplama, teyit/doğrulama, vb.) tanımlamak
- Çıktı ihtiyaçlarını tanımlamak
- Personel, BDDT'ler ve işleme ortamı (kurumun BS olanakları veya denetim BS olanakları) gibi kaynak ihtiyaçlarını tespit etmek
- Kurumun BS imkânları, programları/sistemi ve ilgili dosya tanımları da dahil verilerine erişimin sağlanması
- Kullanılacak BDDT'ler ile ilgili hedefler, üst düzey akış şemaları ve işletim talimatları da dahil dokümanların hazırlanması

**Denetlenen İle Yapılacak Düzenlemeler:**
Ayrıntılı işlem dosyaları gibi veri dosyaları, genellikle, sadece kısa bir süre saklanmaktadır; bundan dolayı, denetçi, ilgili verilerin denetim için gerekli olan süre boyunca saklanması için gerekli düzenlemeleri yapmalıdır. Denetimin kurumun üretim ortamı üzerindeki etkilerini asgari düzeye indirmek için, kurumun BS olanakları, programları/sistemi ve verilerine erişimle ilgili düzenlemeler, erişime ihtiyaç duyulan zamandan çok önce yapılmalıdır. Denetçi, üretim programları/sisteminde oluşan değişikliklerin BDDT'lerin kullanımı üzerinde yapabileceği etkiyi değerlendirmelidir. Bunu yaparken, denetçi, bu değişikliklerin hem BDDT'lerin bütünlüğü ve faydası üzerindeki hem de Denetçinin kullandığı programlar/sistem ve verilerin bütünlüğü üzerindeki etkisini dikkate almalı ve değerlendirmelidir.

**BDDT'lerin Test Edilmesi:**
Denetçi; uygun planlama, tasarım, test etme, işleme ve belge incelemesi yoluyla, BDDT'lerin bütünlüğü, güvenilirliği, faydalılığı ve güvenliği hakkında makul seviyede bir güvence sağlamalıdır. BDDT'lere güvenmeden ve onları dayanak olarak kabul etmeden önce bu güvencenin elde edilmesi gerekir. Bu testin niteliği, zamanlaması ve kapsamı, BDDT'lerin ticari piyasada mevcudiyetine ve istikrarına bağlıdır.

**BDDT'ler ve Verilerin Güvenliği:**
BDDT'lerin veri analizinde kullanılmak üzere bilgi elde etmek için kullanıldığı durumlarda denetçi, verilerin elde edildiği bilişim teknolojileri (BT) ortamının ve bilişim sisteminin bütünlüğünü teyid etmelidir. BDDT'ler, gizli tutulması gereken önemli program/sistem bilgileri ile üretim verilerini elde etmek için de kullanılabilir. Denetçi, bu üretim verilerini ve program/sistem bilgilerini uygun bir gizlilik ve güvenlik düzeyinde tutmalı ve korumalıdır. Bunu yaparken Denetçi, verilerin sahibi olan kurumun istediği ve ilgili mevzuatın öngördüğü gizlilik ve güvenlik düzeyini dikkate almalıdır. Denetçi, BDDT'lerin bütünlüğü, güvenilirliği, faydalılığı ve güvenliğinden sürekli emin olmak için uygun prosedürler uygulamalı ve bu prosedürlerin sonuçlarını kaydetmelidir. Örneğin bu, BDDT'lerde sadece izin verilmiş değişikliklerin yapıldığından emin olmak amacıyla, gömülü denetim yazılımı üzerinde yapılan program bakım ve program değişiklik kontrollerinin gözden geçirilmesini içermelidir. BDDT'ler denetçinin kontrolü altında olmayan bir ortamda bulunuyorsa, BDDT'lerdeki değişiklikleri tespit etmek amacıyla uygun kontroller yapılmalıdır. BDDT'lerde bir değişiklik yapıldığında denetçi, bu BDDT'leri dayanak almadan önce, uygun planlama, tasarım, test etme, işleme ve belge incelemesi yoluyla, BDDT'lerin bütünlüğü, güvenilirliği, faydalılığı ve güvenliği hakkında güvence sağlamalıdır.

## 3. DENETİM ÇALIŞMASININ YAPILMASI:

**Denetim Bulguları ve Delillerinin Toplanması:**
BDDT'lerin ayrıntılı tanımlamalar ve denetim hedeflerini karşıladığı hususunda makul güvence elde edilmesi için, BDDT'lerin kullanımı Denetçi tarafından kontrol edilmelidir. Denetçi:

- uygunsa, kontrol toplamları arasında bir mutabakat çalışması yapmalıdır,
- çıktıların makul olup olmadığını incelemelidir,
- BDDT'lerin mantığını, parametrelerini veya ilgili diğer özelliklerini incelemelidir,
- ilgili kurumun, BDDT'lerin bütünlüğüne katkıda bulunabilecek genel BS kontrollerini (örneğin, program değişiklik kontrolleri ve sisteme, programa ve/veya veri dosyalarına erişim) incelemelidir.

**Genelleştirilmiş Denetim Yazılımı:**
Üretim verilerine erişmek için genelleştirilmiş denetim yazılımını kullanırken denetçi, kurum verilerinin bütünlüğünü korumak için uygun önlemleri almalıdır. Gömülü denetim yazılımında, denetçi de sistemin tasarlanması çalışmasına katılmalı ve gerekli teknikler kurumun uygulama programları/sistemlerinde geliştirilerek muhafaza edilmelidir.

**Yardımcı Program:**
Yardımcı program kullanırken denetçi, işleme sırasında planlanmamış müdahalelerin olmadığından ve yardımcı programın uygun sistem kütüphanesinden alındığından emin olmalıdır. Bu yardımcı programlar sisteme ve dosyalarına kolaylıkla zarar verebileceği için denetçi, kurumun sistemi ve dosyalarının bütünlüğünü korumak için uygun önlemleri de almalıdır.

**Test Verileri:**
Denetçi test verilerini kullanırken, bu verilerin sadece hatâlı işlem potansiyeline işaret ettiğini bilmelidir; bu teknik, fiilî/gerçek üretim verilerini değerlendirmez. Denetçi aynı zamanda, işlem sayısına, test edilen program sayısına ve programların/sistemlerin karmaşıklığına bağlı olarak, test verileri analizinin son derece karmaşık ve zaman alıcı olabileceğini de bilmelidir. Test verilerini kullanmadan önce denetçi, test verilerinin kullanılmakta olan mevcut sistemde daimi ve kalıcı etkiler yapmayacağından emin olmalıdır.

**Uygulama Yazılımı İzleme ve Eşleme:**
Uygulama yazılımı izleme ve eşleme işlevini kullanırken denetçi, halen üretimde kullanılmakta olan hedef programın, değerlendirmeye konu olan kaynak kod tarafından oluşturulduğunu teyid etmelidir. Denetçi, uygulama yazılımı izleme ve eşleme işlevinin sadece hatâlı işlem potansiyeline işaret ettiğini bilmelidir; bu işlev, fiilî/gerçek üretim verilerini değerlendirmez.

**Denetim Uzman Sistemleri:**
Denetim uzman sistemlerini kullanırken denetçi, izlenen karar yollarının mevcut denetim ortamına/durumuna uygun olduğundan emin olmak için, sistemin işleyişi hakkında ayrıntılı bilgi sahibi olmalıdır.

**4. BDDT'lerin DOKÜMANTASYONU:**

**Çalışma Kâğıtları:**
Yeterli denetim bulgusu ve delili sağlamak için, BDDT süreci adım adım ve yeterince kaydedilmelidir. Özellikle, BDDT uygulamasını tanımlamak için denetim çalışma kâğıtları, aşağıdaki bölümlerde verilen ayrıntılar da dahil, yeterli dokümantasyon içermelidir.

**Planlama:**
Dokümantasyon şunları içermelidir:

- BDDT'lerin hedefleri
- Kullanılacak BDDT'ler
- Uygulanacak kontroller
- Personel ve zamanlama

**Uygulama:**
Dokümantasyon şunları içermelidir:

- BDDT hazırlama ve test prosedürleri ve kontrolleri
- BDDT'ler tarafından yapılan testlerin ayrıntıları
- Girdiler (örneğin, kullanılan veriler, dosya düzenleri), işlemler (örneğin, BDDT'lerle ilgili üst düzey akış şemaları, mantık) ve çıktılar (örneğin, günlük dosyaları, raporlar) hakkında ayrıntılar
- İlgili parametreler veya kaynak kodu listesi

**Denetim Bulgu ve Delilleri:**
Dokümantasyon şunları içermelidir:

- Üretilen çıktılar
- Çıktı üzerinde yapılan denetim analiz çalışmalarının tanımı
- Denetim bulguları
- Denetim sonuçları
- Denetim tavsiyeleri

## 5. RAPORLAMA:

**BDDT'lerin Tanımı:**
Raporun hedefler, kapsam ve metodoloji bölümü, kullanılan BDDT'lerin açık bir tanımını içermelidir. Bu tanım aşırı ayrıntılı olmamalı, fakat okuyucu için yeterli bir genel bilgi vermelidir. Kullanılan BDDT'lerin tanımı raporun, BDDT'lerin kullanımıyla ilgili somut bulguların tartışıldığı bölümüne de konulmalıdır. Kullanılan

BDDT'lerin tanımı birden fazla bulgu için geçerli ise ya da aşırı ayrıntılı ise, bu tanım, raporun hedefler, kapsam ve metodoloji bölümünde kısaca açıklanmalı ve okuyucu daha ayrıntılı bir tanım içeren bir eke yönlendirilmelidir.

**EK - TERİMLER:**

**Uygulama Yazılımı İzleme ve Eşleme:** Uygulama yazılımının işleme mantığı aracılığıyla veri akışını analiz etmek ve izlenen mantık, yollar, kontrol koşulları ve işleme sıralarını kaydetmek için kullanılabilecek uzmanlaşmış araçlardır. Hem komut dili veya iş kontrol komutları hem de programlama dili bu yolla analiz edilebilir. Bu teknik, program/sistem; eşleme, izleme, enstantaneler (snapshots), paralel simülasyonlar ve kod karşılaştırmalarını içerir.

**Denetim Uzman Sistemleri:** Uzmanların ilgili alandaki bilgilerini otomatize etmek suretiyle denetçilere karar alma süreçlerinde yardımcı olmak amacıyla kullanılabilen uzman veya karar destek sistemleridir. Bu teknik, otomatik risk analizi, sistem yazılımı ve kontrol hedefleri yazılım paketlerini içerir.

**Bilgisayar Destekli Denetim Teknikleri (BDDT):** Genelleştirilmiş denetim yazılımı, yardımcı programlar, test verileri, uygulama yazılımı izleme ve eşleme ile denetim uzman sistemleri gibi otomatik denetim teknikleridir.

**Genelleştirilmiş Denetim Yazılımı:** Belirli otomatik işlevleri yerine getirmek için tasarlanmış bir bilgisayar programı veya programlar dizisidir. Bu işlevler; bilgisayar dosyalarını okumak, verileri seçmek, verileri işlemek, verileri tasnif etmek, verileri özetlemek, hesaplamalar yapmak, örnekler seçmek ve denetçinin belirlediği biçimde raporlar basmak işlevlerini içerir. Bu teknik, denetim amaçlarıyla edinilen veya yazılan yazılımları ve üretim sistemlerine gömülü yazılımları içerir.

**Test Verileri:** Bilgisayar uygulamalarında programlanmış olan işleyiş mantığı, hesaplamalar ve kontrollerin test edilmesinde kullanılabilen benzeştirilmiş (simüle edilmiş) işlemlerdir. Münferit programlar veya bir sistemin tamamı test edilebilir. Bu teknik; Bütünleşik Test Uygulamaları (Integrated Test Facilities-ITF) ve Temel Vaka Sistem Değerlendirmelerini (Base Case System Evaluations-BCSE) içerir.

**Yardımcı Program:** Bilgisayar donanım üreticileri veya yazılım satıcıları tarafından temin edilen ve sistem işletiminde kullanılan bilgisayar programlarıdır. Bu teknik; işleme faaliyetini, test programlarını, sistem faaliyetlerini ve operasyonel prosedürleri incelemek, veri dosyası faaliyetini değerlendirmek ve iş muhasebesi verilerini analiz etmek için kullanılabilir.

# Uygulama Önerisi 1230-1: Sürekli Meslekî Gelişim

Uluslararası İç Denetim Standartlarından
Standart 1230'un Yorumu

## İlgili Standart

**1230 Sürekli Meslekî Gelişim**
İç denetçiler, mevcut bilgi, beceri ve diğer vasıflarını sürekli meslekî gelişimle artırmalı ve güçlendirmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, sürekli meslekî gelişim konusunda aşağıdaki önerileri de dikkate almalıdır. Ancak bu kılavuzun, bu konuda gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçiler, meslekî yeterliliklerini sürdürmek ve artırmak amacıyla eğitimlerini devam ettirmekten sorumludur. İç denetçiler, iç denetim standartları, prosedürleri ve teknikleriyle ilgili güncel gelişmeleri takip etmelidir. Bu sürekli eğitim; meslek derneklerine üye olmak, konferanslara, seminerlere, üniversite kurslarına, şirket içi eğitim programlarına ve araştırma projelerine katılmak yoluyla alınabilir.

2. İç denetçilerin, meslekî yeterliliklerini, *Uluslararası İç Denetçi*® (CIA) unvanı ve Uluslararası İç Denetçiler Enstitüsü'nün (IIA) verdiği başka unvanlar gibi uygun meslekî sertifikaları alarak göstermeleri beklenir ve istenir.

3. Meslek sertifikası bulunan iç denetçiler, bu sertifikanın gereklerini yerine getirebilmek için yeterli sayıda sürekli meslekî eğitim kursuna katılmalıdır.

4. Hâlen uygun meslek sertifikası bulunmayan iç denetçiler, meslekî sertifika almak için gereken bir eğitim programı ve kursuna katılmalıdır.

# Uygulama Önerisi 1300-1: Kalite Güvence ve Geliştirme Programı

Uluslararası İç Denetim Standartlarından
Standart 1300'ün Yorumu

## İlgili Standart

**1300 Kalite Güvence ve Geliştirme Programı**
İç denetim yöneticisi, iç denetim faaliyetinin tüm yönlerini kapsayan ve etkinliğini sürekli gözleyen bir kalite güvencesi ve geliştirme programı hazırlamalı ve bunu sürdürmelidir. Bu program, dönemsel iç ve dış kalite değerlendirmelerini ve devamlı iç gözlem faaliyetini içermelidir. Programın her parçası, iç denetim faaliyetinin katma değer yaratmasına, kurumun faaliyetlerinin geliştirilmesine yardımcı olmalı ve iç denetim faaliyetinin *Etik Kuralları*na ve *Standartlar*a uyması konusunda güvence sağlamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, kalite programlarını oluşturur ve değerledirirken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun kapsamlı kalite programlarına veya değerlendirilmelerine dair gerekli tüm prosedürleri sunmak gibi bir amacı yoktur; bu kılavuz sadece kalite değerlendirme uygulamalarına ilişkin bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

### 1. Bir Kalite Güvence ve Geliştirme Programının Üzerinden Geçme (KGGP)

İç denetim yöneticisi, çalışma kapsamı *Standartlar*daki ve IIA'nın iç denetim tanımındaki tüm faaliyetleri içine alan bir iç denetim faaliyeti kurmaktan sorumludur. Bunun sağlanması için, Standart 1300 İç Denetim Yöneticisinin bir kalite güvence ve geliştirme programı hazırlamasını gerekli kılar.

**2. KGGP'nin Uygulanması**

İç denetim yöneticisi, iç denetim faaliyetinden yararlanan çeşitli taraflara, iç denetim faaliyetinin, *Standartlar* ve *Etik Kurallar*ıyla uyumlu olması gereken iç denetim yönetmeliğine uygun çalıştığı, etkin ve verimli bir şekilde faaliyet gösterdiği ve hissedarlar ve diğer hak sahiplerinin gözünde katma değer yaratıcı ve kurumun faaliyetlerini iyileştirici olarak görüldüğü konusunda makul bir güvence sağlamak için tasarlanan süreçlerin uygulanmasından sorumlu olmalıdır.

Bu süreçler, gerekli gözetim, dönemsel iç değerlendirmeler, kalite güvencesinin sürekli gözlenmesi ve dönemsel dış değerlendirmeleri içine almalıdır.

**3. KGGP'nin Niteliği ve Kapsamı**

KGGP, Standartlardaki ve mesleğin en iyi uygulamalarındaki gibi, iç denetim faaliyetinin yönetim ve faaliyetlerinin tüm cephelerini kapsamalıdır. KGGP süreçleri, İç Denetim Yöneticisi tarafından veya doğrudan onun gözetimi altında hayata geçirilmelidir. Küçük iç denetim faaliyetleri hariç tutulursa, İç Denetim Yöneticisi, genellikle KGGP sorumluluklarının çoğunu astlarına dağıtır. Büyük ve karmaşık ortamlarda (çok sayıda iş biriminin veya mekânının olması gibi), İç Denetim Yöneticisi denetimden bağımsız ve iç denetim faaliyetinin çeşitli katmanlarıyla danışma hâlinde olan resmî bir KGGP hazırlayabilir. Bu bağımsız fonksiyon, bir denetim yöneticisi tarafından yönetilmelidir. Bu yönetici (ve sınırlı sayıda personel) normalde, KGGP'nin tüm sorumluluklarını yerine getirmez; fakat bu faaliyetleri gözler ve idare eder.

**4. KGGP'nin Kilit Unsurları**

KGGP optimum seviyede meslekî yetkinliği başarmak üzere yapılandırılır ve gözden geçirmeler, mümkün olduğu ölçüde, denetlenen faaliyet ve fonksiyonlardan bağımsız olarak

gerçekleştirilir. İç denetim yöneticisinin emrindeki bir kişi veya birim tarafından çalıştırılan iç denetim faaliyetinin aşağıdaki kilit unsurları, KGGP fonksiyonu açısından dikkate alınmalıdır:

- İç denetim politika ve prosedürlerinin uygulanması ve geliştirilmesini gözetmek; iç denetim faaliyetinin politika ve prosedür kitapçığını sağlamak ve korumak,
- İç denetim yöneticisine ve diğer denetim yöneticilerine iç denetim faaliyetinin mali yönetimi ve bütçelemesiyle yardımcı olmak,
- Denetim riski evrenini etkileyecek yeni bilgileri derleyerek, kullanarak; iç denetim, dış denetim ve diğer değerlendirme ve denetim işlevleri arasında görev dağılımını gözeterek, denetim riski evrenini kapsamlı bir şekilde kollamak ve güncellemek,
- İç denetim yöneticisi ve diğer denetim yönetimine bu alanda yardımın kapsamlı şekilde planlanması ve denetim riskini değerlendirme sisteminin genel işleyişini yönetmek,
- Denetim ve danışmanlık görevlerine dair kapsamlı çizelgelendirme süreçleriyle ve ilgili zaman takip kayıtlarıyla yardımcı olmak,
- İç denetim yönetimine, denetim araçlarının elde edilmesi, bakımı ve çalışmalarda kullanılması konularında ve diğer teknolojilerin kullanımında yardımcı olmak,
- Kurum dışından personel alma ve iç denetim faaliyetinin, kurum içi rotasyona ve yönetim geliştirme programlarına katılmasını yönetmek,
- Personelin kişiler itibariyle, meslekî gelişim düzenlerinin takibi dahil, performans değerlendirme ve kariyer planlamalarının yapılması, girecekleri eğitim programlarının hazırlanması veya seçilmesi gibi personel eğitim ve gelişim faaliyetlerinin izlenmesi,

- İç denetime ait istatistik ve ölçüm elde etme sistemlerini ve denetim sonrası ve diğer araştırma sistemlerini (meselâ, *iç denetim faaliyetinin müşterileri ve diğer hak sahipleriyle ilgili araştırma sistemlerini*) izlemek,
- İç ve dış resmî kalite değerlendirmeleri dahil, kalite güvence ve süreç geliştirme faaliyetlerini yönetmek ve izlemek,
- İç denetim faaliyeti tarafından, üst yönetime ve denetim komitesine sunulmak üzere bilgi toplanması ve dönemsel özet raporlar hazırlanması (*iç ve dış kalite değerlendirme raporları dahil*) çalışmalarını gözetmek ve izlemek,
- İç denetim görevlerinden, dış denetçilerin çalışmalarından ve diğer iç değerlendirme ve soruşturma görevlerinden kaynaklanan eylem planları ve tavsiyeler için kapsamlı bir takip veri tabanı oluşturmak ve yönetmek,
- İç denetim yöneticisinin, denetim yönetiminin ve iç denetim personelinin, iç denetim yönetiminin yönlendirmesi altında, *Standartları*, diğer gelişmeleri, yeni yeni ortaya çıkan en iyi iç denetim uygulamaları, düzenlemeleri ve diğer ortaya çıkan sorun ve fırsatları güncel olarak takip etmelerine yardımcı olmak, "Yardımcı olmak, yönetmek, izlemek, gözlemek ve sürdürmek" kelimeleri, KGGP programında çalışan kişilerin mutlaka bu görevin çoğunu yapmak zorunda olmadığı anlamına gelir. Görev, özel bir amaçla geçici olarak verilebilir veya diğer iç denetim yöneticilerine ve personeline uzun vadeli olarak verilebilir; fakat izlenmesi, idare edilmesi vs, KGGP vasıtasıyla yapılır.

# Uygulama Önerisi 1310-1: Kalite Programı Değerlendirmeleri

Uluslararası İç Denetim Standartlarından
Standart 1310'un Yorumu

## İlgili Standart

**1310 Kalite Programı Değerlendirmeleri**
İç denetim faaliyeti, kalite programının genel etkinliğini gözlemek ve değerlendirmek amacına yönelik bir süreç uygulamalıdır. Bu süreç, hem iç hem de dış değerlendirmeleri içermelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, kalite programlarını geliştirirken veya değerlendirirken bu önerileri dikkate almalıdır. Bu kılavuz kapsamlı kalite programları için gerekli olan hususların tümünü kapsama amacı taşımamakta, sadece kalite değerlendirme uygulamaları konusunda bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

### Kalite Programlarının Gözlenmesi

1- Kalite Programlarının Gözlenmesi, iç denetim faaliyeti tarafından gerçekleştirilen tüm danışmanlık ve denetim faaliyetlerinin dönemsel olarak ve devamlı suretle değerlendirilmesi demektir. Kalite Güvence ve Geliştirme Programı (KGGP) ile sınırlı değildir (*Bkz. 1300-1 sayılı Uygulama Önerisi*). Bu devamlı ve dönemsel değerlendirmeler, (her ikisi de mutat olan) zor ve kapsamlı süreçlerden; danışmanlık ve denetim faaliyetlerinin performansının devamlı izlenmesi ve test edilmesinden ve Standartlara uyumun dönemsel olarak onaylanmasından meydana gelir. Gözlem faaliyeti ayrıca, devamlı ölçümler ve performans ölçümlerinin (yani, denetim planının başarıyla tamamlanması, çevrim süresi, kabul edilen tavsiyeler ve müşteri memnuniyeti gibi) analizini içine almalıdır. Bu değerlendirme sonuçları, iç denetim faaliyetinin iyileştirebileceği

alanlara işaret ediyorsa, iyileştirmeler, İç Denetim Yöneticisi tarafından, KGGP kullanılarak uygulanmalıdır.

**Değerlendirmelerin Tanımlanması ve Zamanlaması**

2- *Devamlı iç değerlendirmeler* ("iç değerlendirmeler" terimi, Uygulama Önerilerindeki başka yerlerde kullanılan "iç gözden geçirme" ve "özdeğerlendirme" terimleriyle eş anlamlıdır) Uygulama Önerisi 1311-1'in ikinci ve üçüncü paragraflarında ifade edildiği gibi, günlük gözetim, gözden geçirme ve iç denetim ölçümlerinin bir parçası olmalıdır.

3- Dönemsel iç değerlendirmeler, 1311-1 sayılı Uygulama Önerisi'nde ortaya koyulduğu gibi tamamlanmalıdır.

4- Dış değerlendirmelerle ilgili iki yaklaşım vardır. Birinci yaklaşımda, bir dış değerlendirme, ehil, bağımsız bir gözden geçirme uzmanı veya ekibi tarafından yapılmalıdır. Bu yaklaşım, tecrübeli ve profesyonel bir proje müdürünün önderliğinde, ehil profesyonellerden oluşan bir dış ekibi içerir (Bu kişilerin özellikleri için bkz. Uygulama Önerisi 1312-1). İkinci yaklaşımda, iç denetim ekibi tarafından tamamlanan iç özdeğerlendirmenin ve raporunun bağımsız bir değerlendirmesi için, gerekli özelliklere sahip, bağımsız bir kişi veya ekip bulunmaktadır. Bu alternatif yaklaşımda, sözü edilen iç denetim faaliyetinin özdeğerlendirmesinin değerlendirmesini yapmak için kalite değerlendirme metodunda deneyimli bağımsız ve gerekli özelliklere sahip kişi veya gözden geçirme ekibi vardır. Bağımsız dış gözden geçirmeyi yapacak olanlar, iç denetim uygulamalarında çok tecrübeli olmalıdırlar.

5- Tam bir iç gözden geçirmenin gerekli olmadığı durumlar olduğunda (bkz. Uygulama Önerisi 1312-2), gerekli özelliklere sahip, bağımsız kişi ve gözden geçirme ekibi tarafından yapılan dış denetim değerlendirmesi, iç denetçi ve pay sahiplerinin güvenirliğine azamî yarar sağlar. İç Denetim Yönetiminde, yaklaşımın temin edilmesi

için üst yönetim ve yönetim kurulu bulunmalıdır.

6- İç değerlendirme faaliyetinin dış değerlendirmeleri, Uygulama Önerileri 1312-1 ve 1312-2'ye göre yapılmalıdır.

**Kalite Programlarının Değerlendirilmesi**

7- Değerlendirmelerle, iç denetim faaliyetinin kalitesine dair bir değerlendirme yapılmalı, bir hükme varılmalı ve daha iyiye gitmesi için tavsiyeler geliştirilmesi mümkün kılınmalıdır. Kalite programları değerlendirilirken şunlar da değerlendirilmelidir:

- Bunlara yönelik önemli aykırılık durumlarının giderilmesi amacıyla zamanında alınacak düzeltici tedbirlere uyum da dâhil olmak üzere, *Standartlar*a ve *Etik Kurallar*ına uyum.
- İç denetim faaliyetinin yönetmeliği, amaçları, hedefleri, politikaları ve prosedürlerinin yeterliliği.
- Kurumun yönetişim, risk yönetimi ve kontrol süreçlerine yapılan katkı.
- Yürürlülükteki kanunlara, yönetmeliklere ve kamusal veya sektörel standartlara uyum.
- Devamlı geliştirme faaliyetlerinin etkinliği ve en iyi uygulamaların benimsenmesi.
- İç denetim faaliyetinin kurumun faaliyetlerine değer katıp katmadığı ve bu faaliyetleri geliştirip geliştirmediği.

**Devamlı Geliştirme**

8- Bütün kalite geliştirme çabaları, gözlem ve değerlendirme faaliyetlerinin sonuçlarına göre, kaynaklar, teknoloji, süreçler ve prosedürlerde gereken değişikliklerin zamanında yapılmasını kapsamalıdır.

**Sonuçların Bildirilmesi**

9- Hesapverebilirlik ve şeffaflığın sağlanması amacıyla, İç Denetim Yöneticisi, kalite programıyla ilgili dış ve gerekirse iç değerlendirme sonuçlarını (üst yönetim, yönetim kurulu ve dış denetçiler gibi) taraflarla paylaşmalıdır. En az yılda bir kez olmak üzere, İç Denetim Yöneticisi, yönetim kuruluna, kalite programı çalışmalarını ve sonuçlarını rapor etmelidir.

# Uygulama Önerisi 1311-1: İç Değerlendirmeler

Uluslararası İç Denetim Standartlarından
Standart 1311'in yorumu

## İlgili Standart

**1311 İç Değerlendirmeler**
İç değerlendirmeler şunları kapsamalıdır:

- İç denetim faaliyetinin performansının devamlı gözden geçirilmesi,
- Özdeğerlendirme yoluyla veya kurum içinde, iç denetim uygulamaları ve *Standartları* bilen kişilerce yapılan dönemsel gözden geçirmeler.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyeti kapsamında iç değerlendirmeler yaparken bu önerileri dikkate almalıdır. Ancak bu kılavuzun, kapsamlı iç değerlendirmeler için gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; sadece iç değerlendirme uygulamaları konusunda bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## Özet

1. İç Denetim Yöneticisi, işin kapsamı Standartlardaki bütün faaliyetleri kapsayacak şekilde, bir iç denetim faaliyeti kurmaktan sorumludur. Bunu sağlamak için, Standart 1300, İç Denetim Yöneticisi'nin bir *Kalite Güvence ve Geliştirme Programı* (KGGP) geliştirmesini ve sürdürmesini gerektirmektedir. KGGP, hem devamlı hem de dönemsel iç değerlendirmeleri içermelidir ("iç değerlendirme" terimi Uygulama Önerilerindeki başka yerlerde kullanılan "*iç gözden geçirme*" ve "*özdeğerlendirme*" kavramları ile eş anlamlıdır). Bu değerlendirmeler, sadece kurumun KGGP'sinin değerlendirilmesi ile sınırlı olmamalı, iç denetim faaliyeti tarafından yapılan tüm denetim ve danışmanlık alanlarını kapsamalıdır. (Bkz. Uygulama Önerisi 1300-1).

**Devamlı İç Değerlendirmeler**

2. Devamlı iç değerlendirmeler çalışmaları, iç denetim faaliyetini yönetmekte kullanılan mutat uygulama ve politikalara birleştirilir ve aşağıdaki *süreç* ve *araçlar* vasıtasıyla gerçekleştirilir:

    - *"Görevin Gözetimi ve Kontrolü"* başlıklı Uygulama Önerisi 2340-1'de tanımlandığı şekliyle görevin gözetimi,
    - İç denetim faaliyetinin kullandığı (mesela, bir denetim ve prosedürler kılavuzundaki) süreçlerin takip edildiğinden emin olmak amacına yönelik kontrol listeleri ve diğer araçlar,
    - Denetlenenlerden ve iç denetim sürecinde yer alan diğer katılımcılardan alınan geri bildirimler,
    - İlgili denetimlerde yer almayan denetim personeli tarafından çalışma kâğıtlarının gözden geçirilmesi,
    - Proje bütçeleri, zaman tutma sistemleri, denetim planı tamamlama kıstasları, maliyeti karşılama kıstasları,
    - (Çevrim süresi ve kabul edilen tavsiyeler gibi) diğer performans ölçümlerinin analizi.

3. Performans kalitesinin devamlı gözden geçirilmesinin sonuçları tespit edilmeli ve gerekli iyileştirmelerin uygulanmasını temin etmek için bir takip çalışması yürütülmelidir.

**Dönemsel İç Değerlendirmeler**

4. Dönemsel iç değerlendirmeler genellikle, rutin dışı, amaca özel gözden geçirmeleri ve uyum testlerini ifade eder. Bunların, (a) iç denetim faaliyeti yönetmeliğine, *Standartlar*a ve IIA'nın *Etik Kuralları*na uyulup uyulmadığını ve (b) iç denetim faaliyetinin iç denetim sürecinde yer alan çeşitli tarafların ihtiyaçlarına cevap verme konusundaki etkinliğini ve verimliliğini değerlendirebilecek şekilde tasarlanmalıdır. IIA'nın Kalite Değerlendirme Kılavuzu, veya bunun muadili kılavuz ve araçlar, dönemsel iç değerlendirmeler için temel teşkil etmelidir.

**5. Dönemsel iç değerlendirmeler:**

- Denetim sürecinde yer alan gruplara yönelik daha ayrıntılı ve derin araştırma ve görüşmeleri içerebilir,
- İç denetim faaliyetinin üyeleri tarafından yapılabilir (öz değerlendirme),
- Hâlen kurum içinde başka konu ve alanlarda görevli olan Uluslararası İç Denetçiler (CIA) tarafından veya diğer ehil denetçiler tarafından yapılabilir,
- Daha sonra kurumun diğer birimlerindeki CIA'lar veya ehil diğer denetçilerin gözden geçirdiği çalışmalarla, özdeğerlendirme çalışmalarını bir araya getirebilir,
- İç denetim faaliyetinin uygulamalarının ve performans ölçümlerinin iç denetim mesleğiyle ilgili en iyi uygulamalarla karşılaştırılıp değerlendirilmesine dayanan kıyaslama (benchmarking) çalışmasını içerebilir.

6. Dış değerlendirmenin hemen öncesinde yapılacak dönemsel bir iç değerlendirme, dış değerlendirmeyi hem kolaylaştırmaya hem de maliyetini azaltmaya yardım edebilecektir. Eğer dönemsel iç değerlendirme, ehil ve bağımsız dışarıdan biri veya bir gözden geçirme ekibi tarafından yapılırsa, değerlendirme sonuçları, dış kalite değerlendirmesinin sonuçlarıyla ilgili bir güvence vermemelidir. Raporda, iç denetim faaliyetlerinin uygulamalarının geliştirilmesi için tavsiye ve öneriler bulunabilir. Eğer dış değerlendirme, "bağımsız onaylı özdeğerlendirme" (Uygulama Önerisi 1312-2) şeklini alırsa, dönemsel iç değerlendirme bu sürecin "özdeğerlendirme" kısmı işlevini görebilir.

7. Performans kalitesi hakkında sonuçlar derlenmeli, tespit edilmeli ve gerekirse, *Standartlar*a uygunluğu sağlamak ve geliştirme çalışmaları yapmak amacıyla uygun tedbirler alınmalıdır.

**Sonuçların Duyurulması**

8. İç Denetim Yöneticisi, iç değerlendirmelerin sonuçlarının rapor edilmesi amacıyla, gerekli güvenilirlik ve nesnelliği sağlayan bir yapı oluşturmalıdır. Genel olarak, devamlı ve dönemsel gözden geçirmeleri yapma sorumluluğunu üstlenen kişiler, gözden geçirme çalışmalarında İç Denetim Yöneticisi'ne bağlı olmalı ve elde ettikleri sonuçları doğrudan doğruya İç Denetim Yöneticisi'ne bildirmelidir.

9. İç Denetim Yöneticisi, yılda en az bir kere, iç değerlendirme çalışmalarının sonuçlarını, gerekli eylem planlarını ve bunların başarılı uygulamalarını yönetim kuruluna raporlamalı ve iç denetim faaliyeti dışındaki uygun kişilerle (üst yönetim ve dış denetçiler gibi) paylaşmalıdır.

# Uygulama Önerisi 1311-2: İç Denetim Faaliyetinin Gözden Geçirilmesinin Desteklenmesi İçin (Nicel Metrikler ve Nitel Değerlendirmeler) Ölçülerin Tesis Edilmesi

Uluslararası İç Denetim Standartlarından
Standart 1210.A2'nin yorumu

Bu Uygulama Önerisi, İç Denetim faaliyetinin ölçümü için tavsiye edilen uygulamaları yansıtmaktadır.

## İlgili Standart

**1311 İç Değerlendirmeler**
İç değerlendirmeler şunları kapsamalıdır:

- İç denetim faaliyetinin performansının devamlı gözden geçirilmesi,
- Özdeğerlendirme yoluyla veya kurum içinde, iç denetim uygulamaları ve *Standartlar*ı bilen kişilerce yapılan dönemsel gözden geçirmeler.

**Bu Uygulama Önerisinin Niteliği:** *Bu uygulama önerisi, Uygulama Önerisi 1311-1'deki konulara dayanmakta ve iç denetim faaliyetlerinin performansının gözden geçirilmesinde ölçülerin tesis edilmesinde yol gösterme amacı taşımaktadır. Bu kılavuzluğun amacı performans ölçüleri kurmak için tek zemin olmak değildir, fakat Uluslararası İç Denetim Standartları (IIA Standartları) ve diğer yaygın ölçüm standartlarıyla birlikte kullanılması önerilmektedir. Bu öneri İDY'ler tarafından önemli görülen özel ölçümlere örnekler verse de, tüm denetim faaliyetlerinde etkili olabilecek tek bir ölçü sistemi yoktur. Hem nicel metrikler hem de nitel değerlendirmeler, denetim faaliyet performansının, önemli hak sahiplerine gösterilmesinde önem taşımaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

**Giriş**

Standard 1310'a göre, iç denetim faaliyetleri, kalite programının genel etkinliğini gözlemek ve değerlendirmek amacına yönelik bir süreç uygulamalıdır. Bu süreç, hem iç hem de dış değerlendirmeleri içermelidir. Uygulama Önerisi 1311-1'de, bu iç gözden geçirmelerin yapılmasında, performans ölçüm analizlerinin bir öğe gibi kullanılması önerilmektedir.

*IIA Standartları*'yla uyumun yanında, denetim faaliyet performans ölçüleri şunları da kapsayabilir: Risk yönetimi ve kontrolü ve yönetim süreçlerinin geliştirmesine katkı seviyesi, ana hedeflere ve belirlenen amaçlara ulaşmak, denetim faaliyet planına göre ilerlemenin değerlendirilmesi, geliştirilmiş personel verimliliği, denetim sürecinin maliyet etkinliğinin artışı, süreç gelişimlerinde artan faaliyet plan sayısı, uygun görev planı ve yönetimi, hak sahiplerinin ihtiyaçlarının karşılanmasındaki etkinlik, kalite güvence gözden geçirmelerinin verimliliği, vb.

**Performans Ölçüm Sürecinin Tesis Edilmesi**

Etkili performans ölçümlerinin tesis edilmesi için İDY şu özelliklere sahip bir süreç kurması gerekir:

- Önemli performans kategorilerinin (örn. iç hak sahiplerinin memnuniyeti) teşhis edilmesi.

Bu öneri aşağıdaki sınıflandırmaların kullanılmasını önermektedir:

- Hak sahiplerinin memnuniyeti
- İç denetim süreçleri
- Yenilik ve yetkinlik

- Performans kategori stratejileri ve ölçülerinin teşhis edilmesi. Stratejiler, hak sahiplerin memnuniyetini sağlamanın yanı sıra *IIA Standartları*'na, diğer mesleki standartlara ve uygulanabilir kanun ve düzenlemelere uygun olmalıdır. Performans ölçülerinin kullanılması, IIA Standartları ile uyumda, iç denetim faaliyetinin

iç değerlendirmesinin bir öğesi olabilir.

- Belli aralıklarla gözlenen, analiz edilen ve rapor edilen performans değerlendirmeleri için bir sürecin sağlanması.

İDY, kullanılan ölçülerin, faaliyetlerinin boyutu, ülke, sanayi dalı, ulusal yasalar ve düzenlemeler ve çevre ile uyum içinde olduğunu temin etmelidir.

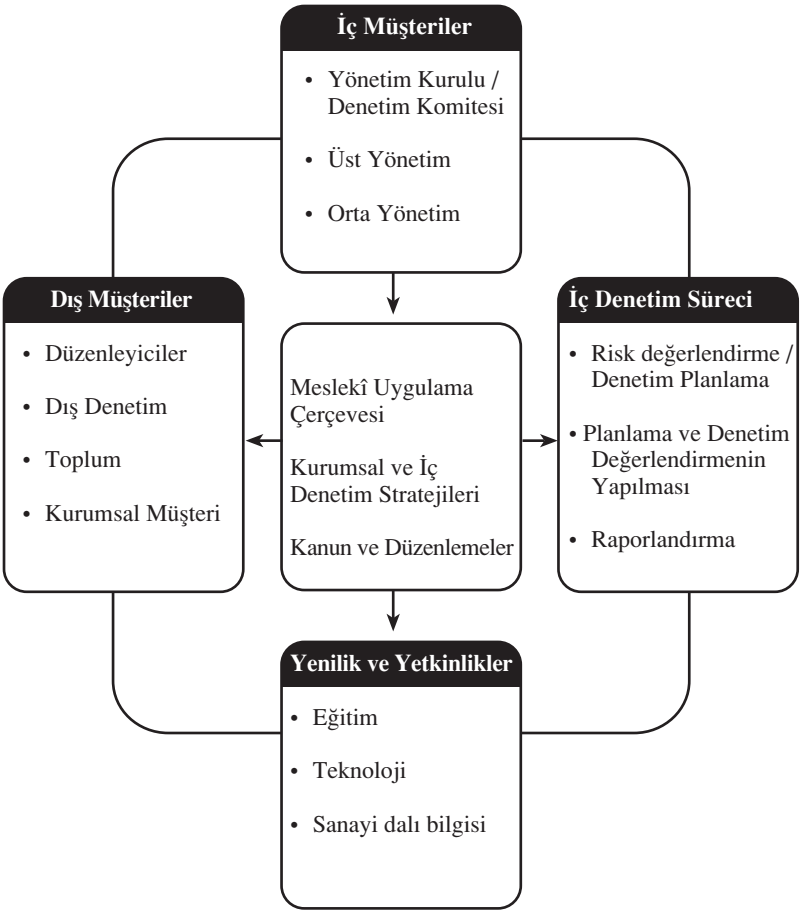
Performans ölçüleri, kuruluşa özel olmalı ve İDY özel denetim faaliyeti ile anlamlı olmayan genel ölçülere güvenme konusunda dikkatli olmalıdır. İDY'ler için önemli olabilecek ölçü örnekleri bu uygulama önerisinin sonundaki Belge A'da liste şeklinde verilmiştir.

**Önemli Performans Kategorilerinin Teşhis Edilmesi**
Yukarıda da belirtildiği gibi İDY, hak sahiplerinin memnuniyeti, denetim süreçleri ve yenilik ve iç denetimin yetkinliği gibi anahtar performans ölçüm kategorilerini teşhis etmelidir.

Hak sahiplerinin kapsamında, denetim komitesi, üst yönetim, dış hükümet kurumları ve düzenleyiciler ve dış denetçiler vardır. Denetim süreçlerinde risk değerlendirmesi, planlama ve denetim metodolojileri vardır. Yenilik ve yetkinliğin kapsamında, teknolojinin, eğitimin ve sanayi dalı bilgisinin etkili kullanımı vardır.

**Performans Kategori Stratejileri ve Ölçümlerin Teşhis Edilmesi**
IIA Standartları, diğer kullanılabilir meslekî standartlar, kurumsal ve iç denetim faaliyeti stratejik planları, kanun ve düzenlemeler, iç denetim yönetmeliği ve görevi, her bir performans kategorisi için en uygun stratejiyi bulmada etkili bir temel oluşturacaktır. Performans kategori stratejileri ve ölçümleri bu temele ve hak sahibinin memnuniyetinin analizine dayanır.

Şekil 1- Performans kategori örneklerinin şekle dönüştürülmüş hali:



**İç ve Dış Hak Sahipleri**

Alışılagelmiş olunduğu gibi, iç denetin faaliyeti için anahtar hak sahipleri (müşteriler) iç ve dış hak sahipleri olarak ikiye ayrılmıştır.

- İç hak sahipleri: Yönetim kurulu/denetim komitesi, üst ve orta yönetimi içerebilir
- Dış hak sahipleri: düzenleyiciler ve dış denetimi içerebilir

İDY, ilgili tüm hak sahiplerini ve her bir hak sahibi için önemli olan, veya olması gereken ürünleri ve hizmetleri teşhis etmelidir. İDY, bunların mevcut memnuniyet seviyelerinin (ve önceliklerinin) ve bunların tespit edilmiş eksikliklerinin değerlendirmesini yapmalıdır. Değerlendirmeler, yüz yüze görüşmeler, planlı oturumlar ve/veya anketlerle yapılabilir. Eksiklikler teşhis edildiğinde, İDY'nin uygun bir faaliyet planı yapması gerekir. Hak sahipleri arasındaki memnuniyet konusunda mutabık kalınmalı ve onaylanmalıdır.

İlgili hak sahiplerini ve bunların memnuniyetlerini tespit ederken dikkat edilmesi gerekenler şunlardır:

- Kurum ve/veya denetim faaliyeti için düzenlemenin kapsamı.
- Anahtar iç ve dış hak sahipleri ile ilişkiler.
- Kurumun yapısı (örn: kamu kuruluşu veya özel sektör).

**İç Denetim Süreçleri**

IIA Performans Standartları, iç denetim süreçlerindeki performans ölçüm kategorilerini teşhis etmede dikkate alınmalıdır. Ayrıca, İç Denetim Yönetmeliği tarafından istenen hususlar da dikkate alınmalıdır. Geri bilgilendirme ve ölçüm mekanizmaları, eğer iç denetim bölüm yönetmeliğinde varsa, [denetimde aynı süreçleri takip etmesi gerekmeyen] yönetim danışmanlık görevleri ve suiistimal araştırma hizmetleri için bilgi toplamak için kurulmalıdır. İç denetim süreç kategorileri ve her kategorinin ölçülmesi için potansiyel alan örnekleri:

**a. Risk Değerlendirme/ Denetim Planlama**

- Anahtar hak sahiplerinden (denetim komitesi, üst yönetim

ve dış denetim) denetim faaliyetinin, risk konularına etkili bir şekilde değinip değinmediği konusunda geri bildirim alındı mı?

- Denetim faaliyeti, risk alanlarını hitap ettiği kapsamı değerlendirmeye alıyor mu?

**b. Denetim Görevinin Planlanması ve Yerine Getirilmesi**

- İçerik, hedef, zamanlama ve kaynakları kapsayan her görev için uygun denetim planları yapıldı mı?
- Denetimler, mevcut denetim metodları ve kullanılan uygulamalara göre yapılıyor mu?

**c. İletişim ve Raporlandırma**

- Anahtar hak sahiplerinden kalite, ayrıntı seviyesi ve denetim iletişim sıklığı ile ilgili geri bildirim alınıyor mu?
- İç denetim faaliyeti, anahtar tavsiyelerin tatbik edildiği seviyeyi ölçüyor mu?

**Yenilik ve Yetkinlik**

IIA Nitelik ve Performans Standartları, iç denetim faaliyetleri yenilik ve yetkinlikle ilgili performans ölçüm kategorilerinin teşhis edilmesinde dikkate alınmalıdır. Yenilik ve yetkinlik kategorileri ve her kategoride ölçülecek potansiyel alan örnekleri şöyledir:

**a. Eğitim**

- Denetim personelinin gerekli eğitimi aldığına dair ölçümler (personel başına eğitim saati, önemli eğitim konularının personel tarafından tamamlanması, vs.) yapıldı mı?
- Denetim personelinin eğitimden memnuniyeti ölçüldü mü?
- Personel sertifika sayısı ölçüldü mü?

**b. Teknolojinin kullanımı**

- Teknolojinin kullanılmasında personel eğitimi için hedefler

belirlendi mi? Bu hedeflere ulaşma amacındaki ölçümlere ulaşıldı mı?

- Teknolojinin denetimin sınanması ve analiz edilmesinde destek olması için hedefler belirlendi mi? Bu hedeflere ulaşma amacındaki ölçümlere ulaşıldı mı?

**c. Sanayi Dalı Bilgisi**

- Personelin sektör, iş konusu, faliyetler ve kilit önemdeki işler (intibak oturumlarının tamamlanması, kilit alanlardaki denetim projeleri, faaliyetlerdeki çalışmalar) hakkında yeterli bilgiye sahip olmalarını temin edecek tedbirler alınmakta mıdır?

**Etkili Bir Performans Ölçümü ve Raporlandırma Sürecinin Uygulanması**

İDY, belirlenmiş denetim faaliyetinin hedef ve amaçlarını destekleyen ve bu hedef ve amaçlarına ulaşmanın uygun değerlendirmesini yapan davranış sergileyen bir ölçüm süreci kurmalıdır. Etkili bir süregelen süreçte şunlar olacaktır:

- IIA Standartları ile aynı paralelde performans ölçüleri, önemli stratejik hedefler ve uygulanabilir kanun ve düzenlemeler. Bu ölçüler, hem nicel hem de nitel olabilir. Ölçü başlıkları net, ölçülebilir, ulaşılabilir, gerçekçi hedef /veya standartlar olmalıdır.
- Ölçüm verilerinin toplanması, özetlenmesi ve analiz edilmesinde ve zamanında geri bildirim verilmesine uygun süreçler.
- Ölçülerin değişen beklenti, şart, öncelik ve hedeflerle uyumlu olmasını sağlayacak süreçler.
- Ölçüm süreç sonuçlarının bölüm yönetimi ve hak sahiplerine rapor edilmesi.
- İç denetim faaliyetinin etkililiği yıllık raporla denetim komitesine sunulması.

Şekil 2 Performans ölçüm sürecinin nasıl uygulanacağını görsel olarak ortaya koymaktadır. Bu örnek, kurumsal strateji ve denetim stratejisi arasındaki bağ dâhil olmak üzere yenilik ve yetkinlik kategorisi için performans ölçümlerini göstermektedir.

İlave kılavuz, kaynak ve örnek için lütfen aşağıdaki IIA Standartları, Uygulama Önerileri ve diğer kaynaklar listesine bakınız.

**İlgili Uygulama Önerisi ve Diğer Kaynaklar**
Uygulama Önerisi 2100-3: İç Denetimin Risk Yönetim Sürecindeki Rolü

Uygulama Önerisi 2140-4: Risk Yönetim Süreci Olmayan Kurumlarda İç Denetimin Rolü

Uygulama Önerisi 1300-1: Kalite Güvence ve Geliştirme Programı

Uygulama Önerisi 1310-1: Kalite Programı Değerlendirmeleri

Uygulama Önerisi 1311-1: İç Değerlendirmeler

Uygulama Önerisi 1312-1: Dış Değerlendirmeler

Uygulama Önerisi 1312-2: Dış Değerlendirmeler - Bağımsız Onaylı Özdeğerlendirme

Uygulama Önerisi 1320-1: Kalite Programı Hakkında Raporlama

Uygulama Önerisi 1330-1: "*Standartlar*a Uygun Yapılmıştır" İbaresinin Kullanılması

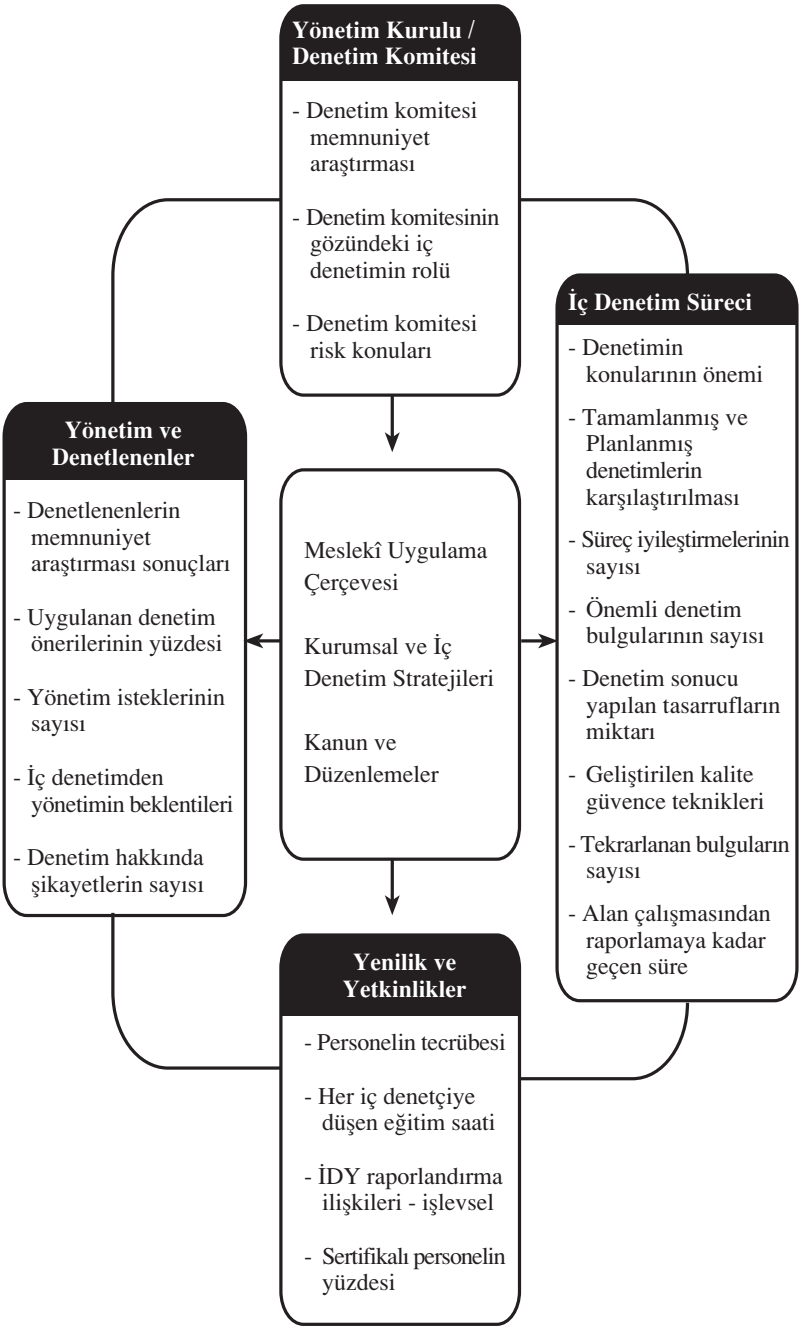
**Diğer Kaynaklar:**

- IIA tarafından yayınlanan *The Quality Assessment Manual* (Kalite Değerlendirme Kılavuzu)
- COSO Girişim Risk Yönetimi - Birleşik Çerçeve
- John Fraser ve Hugh Lindsay tarafından kaleme alınan *20 Questions Directors Should Ask About Internal Audit* (İç Denetim Hakkında Yöneticilerin Sorması Gereken 20 Soru). Bu kitap IIA'nın internet sitesinde bulunabilir ve IIA Araştırma Vakfı, Kanadalı İmtiyazlı Muhasebeleri Enstitüsü ve Kurumsal Yöneticiler Enstitüsü'nün desteğiyle yayınlanmıştır.

- Kurumların kendi denetim bölümlerinin büyüklük, deneyim, uzmanlık ve diğer metrikler konusunda, kendi alanlarındaki benzer büyüklükteki kurumlarla kıyaslamasına imkan veren GAIN adlı IIA'nın Küresel Denetim Bilgi Ağı.
- Prof. Mark L. Frigo, (CPA, CMA) tarafından kaleme alınan A *Balanced Scorecard Framework for Internal Auditing Departments* (İç Denetim Bölümleri İçin Denk Puan Tablosu Çerçevesi) IIA Araştırma Vakfı'nın desteğiyle yayınlanmıştır.

Belge A, İç Denetim Bölümleri İçin Denk Puan Tablosu Çerçevesi adlı kitaptan alınmış ve uyarlanmıştır. Bu tablo, sınırlı sayıdaki İDY tarafından önemli görülen performans değerlendirmelerinin anında yapılmasını sağlamaktadır.

İç denetim faaliyetinin özel ihtiyaçları için, özel performans ölçüleri seçilmelidir.


Yönetim Kurulu / Denetim Komitesi
- Denetim komitesi memnuniyet araştırması
- Denetim komitesinin gözündeki iç denetimin rolü
- Denetim komitesi risk konuları
İç Denetim Süreci
- Denetimin konularının önemi
- Tamamlanmış ve Planlanmış denetimlerin karşılaştırılması
- Süreç iyileştirmelerinin sayısı
- Önemli denetim bulgularının sayısı
- Denetim sonucu yapılan tasarrufların miktarı
- Geliştirilen kalite güvence teknikleri
- Tekrarlanan bulguların sayısı
- Alan çalışmasından raporlamaya kadar geçen süre
Yönetim ve Denetlenenler
- Denetlenenlerin memnuniyet araştırması sonuçları
- Uygulanan denetim önerilerinin yüzdesi
- Yönetim isteklerinin sayısı
- İç denetimden yönetimin beklentileri
- Denetim hakkında şikayetlerin sayısı
Meslekî Uygulama Çerçevesi
Kurumsal ve İç Denetim Stratejileri
Kanun ve Düzenlemeler
Yenilik ve Yetkinlikler
- Personelin tecrübesi
- Her iç denetçiye düşen eğitim saati
- İDY raporlandırma ilişkileri - işlevsel
- Sertifikalı personelin yüzdesi

# Uygulama Önerisi 1312-1: Dış Değerlendirmeler

Uluslararası İç Denetim Standartlarından
Standart 1312'nin Yorumu

## İlgili Standart

**1312 Dış Değerlendirmeler**

Dış değerlendirmeler, kurum dışından vasıflı ve bağımsız bir gözden geçirme uzmanı veya ekibi tarafından en azından beş yılda bir yapılmalıdır. Dış değerlendirme sıklığının arttırılmasına yönelik potansiyel ihtiyaç, dış gözden geçirme uzmanı veya ekibinin sahip olması gereken vasıflar ve bunların bağımsızlığı meseleleri, menfaat çatışması ihtimali de dikkate alınarak, İç Denetim Yöneticisi ile Yönetim Kurulu ve Denetim Kurulu arasında tartışılmalıdır. Bu tartışmalarda, gözden geçirme görevlisi veya ekibinin tecrübesi değerlendirilirken, kurumun büyüklüğü, karmaşıklığı ve sektörü dikkate alınmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyeti kapsamında iç değerlendirmeler yaparken bu önerileri dikkate almalıdır. Ancak bu kılavuzun, kapsamlı iç değerlendirmeler için gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; sadece iç değerlendirme uygulamaları konusunda bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## Özet

1. İç Denetim Yöneticisi, işin kapsamı Standartlardaki bütün faaliyetleri kapsayacak şekilde bir iç denetim faaliyetini kurmaktan sorumludur. Bunu sağlamak için, Standart 1300, İç Denetim Yöneticisi'nin bir *Kalite Güvence ve Geliştirme Programı* geliştirmesini ve sürdürmesini gerektirmektedir. KGGP, ehil ve bağımsız bir gözden geçirme uzmanı veya bir gözden geçirme ekibi tarafından *en az beş yılda* bir dönemsel dış değerlendirmeyi içermelidir. Dış değerlendirmeler, bağımsız bir değerlendirme ile kapsamlı bir özdeğerlendirme

şeklini alabilir (Uygulama Önerisi 1312-2). Dış değerlendirmeler ayrıca, iç denetim faaliyeti tarafındanyürütülen denetim ve danışmanlık görevini de kapsamalı ve KGGP'sini değerlendirmekle sınırlı olmamalıdır (bkz. Uygulama Önerisi 1300-1). Dış değerlendirmeden en iyi verimi almak için, işin kapsamında, iç denetim faaliyetinin daha etkili ve/veya verimli olmasını sağlayabilecek başlıca uygulamaların kıyaslaması, teşhisi ve raporlandırılması da bulunmalıdır. Bu, ya ehil ve bağımsız bir gözden geçirme uzmanı veya bir gözden geçirme ekibi tarafından bir bağımsız gözden geçirme ile ya da bağımsız değerlendirme yapılmış bir özdeğerlendirme ile başarılabilir. Ancak, İç Denetim Yöneticisi, kapsamın, her durumda dış değerlendirmeden beklenen teslim edilebilirleri ortaya koymasını sağlamalıdır.

**Genel Hususlar**

2. Bir iç denetim faaliyetine yönelik dış değerlendirmelerde, iç denetim faaliyetinin Standartlara uygunluğu değerlendirilmeli (ve bu konuda bir görüş beyan edilebilir) ve, gerekirse, gelişme amacına yönelik tavsiyeler verilmelidir. Bu gözden geçirmeler, İç Denetim Yöneticisi ve iç denetim faaliyetinin diğer üyeleri için, özellikle kıyaslama ve en iyi uygulamalar paylaşıldığında, çok faydalı olabilir. Sadece ehil ve bağımsız gözden geçirme uzmanları bu gözden geçirmeleri yapmalıdırlar (bkz. 7 numaralı paragraf).

3. Gözden geçirme çalışması tamamlandıktan sonra yönetim kuruluna (*Standartlar*'ın Sözlük bölümünde tanımlandığı şekliyle) ve üst yönetime resmî bir raporlandırma yapılmalıdır.

**Dış Gözden Geçirme Uzmanlarının Genel Özellikleri**

4. Özdeğerlendirmelere onay verenler de dâhil (Uygulama Önerisi 1312-2), dış değerlendirme uzmanları, kurumdan ve iç denetim faaliyetinden bağımsız olmalıdır. Gözden geçirme ekibi, iç denetim uygulamaları ve dış denetim süreci konusunda uzman kişilerden oluşmalıdır.

**Bağımsızlık**

5. Değerlendirmeyi yapan kişi veya kurumun, değerlendirme ekibinin ve dış değerlendirmeye katılan diğer kişilerin, iç denetim faaliyeti değerlendirme ve incelemeye tâbi olan kuruma veya kurumun personeline karşı her hangi bir yükümlülüğü - veya onlardan her hangi bir çıkarı - olmamalıdır. Ehil ve bağımsız dış değerlendirme uzmanını veya dış değerlendirme ekibini seçerken, İç Denetim Yöneticisi tarafından - yönetim kuruluna da danışarak - bunların bağımsızlığına dair dikkate alınması gereken özel hususlar şunları içerir:

   - Aşağıdakileri sağlayacak, şirketin her hangi gerçekte ve görünürdeki çıkar çatışmaları:
     - Malî beyanların denetimi.
     - Yönetişim, risk yönetimi, malî raporlandırma, iç kontrol ve diğer ilgili alanlardaki önemli danışmalık hizmetleri.
     - İç denetim faaliyetine yardım. Profesyonel hizmet sağlayıcısı tarafından yürütülen işin önem ve büyüklüğü görüşmelerde dikkate alınmalıdır.
   - Değerlendirmeyi yapacak olanların şirket eski çalışanları olması halinde bunların gerçekte ve görünürdeki çıkar çatışmaları. Kişinin kurumdan ayrılmasının üzerinden ne kadar geçmiş olduğu dikkate alınmalıdır.
   - Değerlendirmeyi yapacak olan kişiler, iç denetim faaliyeti değerlendirmeye alınan kurumdan bağımsız olmalı ve ne gerçekte ne de görünürde bir çıkar çatışması olmamalıdır. "Kurumdan bağımsız olmak", iç denetim faaliyetinin bağlı olduğu kurumun bir parçası olmamak veya onun kontrolü altında olmamak anlamına gelir. Ehil ve bağımsız bir dış gözden geçirme uzmanı veya ekibinin seçiminde, onun iç kalite değerlendirmesine katılımını da içerecek şekilde, uzmanın kurumla veya onun iç denetim faaliyetiyle olan

mevcut veya geçmiş ilişkilerinden dolayı gerçek veya görünür bir çıkar çatışması bulunup bulunmadığına özellikle dikkat edilmelidir.

- İç denetim biriminden örgütsel olarak bağımsız olsa bile, o kurumun başka bir bölümünde veya ilişkili bir kurumunda çalışan kişiler, bir dış değerlendirme çalışması açısından, bağımsız sayılmazlar. "İlişkili bir kurum", ana kurum, aynı şirketler grubuna bağlı bir ortaklık veya dış değerlendirmeye konu olan iç denetim faaliyetinin bağlı olduğu kuruma karşı gözetim, izleme veya kalite güvence sorumlulukları olan bir kurum olabilir.
- Karşılıklı gözden geçirme çalışmalarının da olduğu gerçek veya görünürdeki çatışmalar. Üç veya daha fazla kurum (aynı sektörde veya diğer yakın bir grupta, bölgesel derneklerde veya diğer kurum gruplarında - önceki paragrafta yer alan "ilişkili kurum" tanımı haricinde) arasındaki karşılıklı denk gözden geçirme çalışmaları, bağımsızlık endişelerini azaltacak bir tarzda yapılandırılabilir, ama bağımsızlık hususunda endişe yaratmamaya azami özen gösterilmelidir. İki kurum arasında karşılıklı denk gözden geçirme çalışması bağımsızlık testini geçmemelidir.
- Bu bölümde belirtilen örneklerde olduğu gibi bağımsızlığa, görünürde veya gerçekte zarar verebilme endişelerini gidermek amacıyla, bir veya daha fazla bağımsız kişi, bu ekibin çalışmalarını bağımsız bir şekilde onaylamak üzere, dış değerlendirme ekibine katılabilir veya daha sonra ekibe katılması planlanabilir.

**Dürüstlük ve Objektiflik (Nesnellik)**

6. *Dürüstlük*, gözden geçirme uzman(lar)ının gizlilik sınırları içinde güvenilir ve tarafsız olmasını gerektirir. Kişisel kazanç ve çıkarlar için, hizmet ve kamu güveni ve inancı fedâ edilmemelidir.

*Objektiflik*, gözden geçirme uzman(lar)ının hizmetlerine değer katan bir nitelik ve zihnî bir durumdur. Objektiflik ilkesi, tarafsızlık, fikir haysiyeti ve her türlü çıkar çatışmasından uzak olma yükümlülüklerini getirir.

**Yetkinlik (Ehliyet)**

7. Bir dış değerlendirme çalışması yapılırken ve sonuçları raporlanırken meslekî muhakemenin kullanılması gerekir. Bu sebeple, bir dış değerlendirme uzmanı olarak görev yapan bir kişinin:

    - Standartlar hakkında güncel ve derin bilgi sahibi olan, ehil ve yetkili bir denetçi - ki bu onun kalite değerlendirmesi yapmasını sağlar - olması,
    - Mesleğin en iyi uygulamaları konusunda bilgili ve deneyimli olması,
    - İç denetim uygulamalarında veya ilgili danışmanlıkta en az üç yıllık yöneticilik tecrübesine sahip olması gerekir.

Bağımsız gözden geçirme ekiplerinin başları veya özdeğerlendirmenin sonuçlarını bağımsız olarak onaylayan dış gözden geçirme uzmanları (Uygulama Önerisi 1312-2), daha önce dış kalite değerlendirmesinde çalışmış bir takım üyesi olmaktan, IIA'nın kalite değerlendirme eğitimlerini veya benzeri bir eğitimi başarıyla tamamlamaktan, ve iç denetim yöneticiliğinden veya benzeri bir üst seviye iç denetim yöneticiliği deneyiminden kazanılmış daha öte bir yetkinlik ve tecrübe birikimine sahip olmalıdırlar.

8. Gözden geçirme uzman(lar)ı, bilgi teknolojilerinde uzmanlığı ve ilgili sektörde deneyime sahip olmalıdırlar. Başka uzmanlık alanlarında uzmanlığı bulunan kişiler ekibe yardımcı olabilirler. Örneğin, şirket risk yönetimi, istatistiksel örnekleme, operasyonlar izleme sistemleri veya kontrol özdeğerlendirme uzmanları gözden geçirme çalışmasının belirli bölümlerine katılabilirler.

**Üst Yönetim ve Yönetim Kurulu**

9. İç Denetim Yöneticisi, dış kalite değerlendirme sağlayıcısı seçimine ve seçim sürecine, üst yönetimi ve yönetim kurulunu dâhil etmelidir.

**Dış Değerlendirme Kapsamı**

10. Dış değerlendirme çalışması, iç denetim faaliyetinin aşağıdaki unsurlarını içeren geniş bir kapsamda yapılmalıdır:

    - *Standartlar*a, *Etik Kuralları*na, iç denetim faaliyetinin yönetmelik, plan, politika, prosedür ve uygulamalarına ve yürürlülükteki mevzuat ve düzenlemelere uyum,
    - Yönetim kurulu, icra kurulu ve işletme müdürlerinin iç denetim faaliyetinden beklentileri,
    - Yönetişim sürecine katılan kilit gruplar arasındaki bağlantılı ilişkiler dâhil, iç denetim faaliyetinin, kurumun yönetişim süreciyle bütünleştirilmesi,
    - İç denetim faaliyetinde kullanılan araç ve teknikler,
    - Personelin sürecin geliştirilmesine odaklanması dâhil, personelin bilgi, tecrübe ve uzmanlık alanlarının karışımı,
    - İç denetim faaliyetinin kurumun faaliyetlerine katma değer ve iyileştirme sağlayıp sağlamadığın tespit edilmesi.

**Sonuçların Duyurulması**

11. Gözden geçirme çalışmasının ilk sonuçları, değerlendirme süreci sırasında ve sonucunda, İç Denetim Yöneticisi ile tartışılmalıdır. Kesin sonuçlar, İç Denetim Yöneticisi'ne ya da kurum içinde incelemeye yetkisi olan bir yetkiliye, tercihen üst yönetimden uygun kişilere ve yönetim kuruluna doğrudan iletilen raporlarla bildirilmelidir.

12. Raporlamanın kapsamı aşağıdakilerden oluşabilir:

    - Planlanış bir derecelendirme sürecine dayanarak, iç denetim

faaliyetinin *Standartlar*a uyumu hakkında bir görüş: Burada kullanılan "uyum" terimi, iç denetim faaliyetinin uygulamalarının, bir bütün olarak ele alındığında, *Standartlar*ın gereklerine uygun olduğu anlamına gelir. Benzer şekilde "aykırılık" terimi de, iç denetim faaliyetinin uygulamalarında tespit edilen eksikliklerin etkisinin, faaliyetin görev ve sorumluluklarını yerine getirmesini engelleyecek kadar yüksek olması anlamına gelir. *Standartlar*a "kısmî uyum" derecesi, raporun genel kanaatiyle ilgiliyse, bağımsız değerlendirme raporunda da açıklanmalıdır. Dış değerlendirme sonuçları hakkında görüş beyan etmek, güçlü bir meslekî muhakeme, dürüstlük, azamî özen ve dikkatin bir araya getirilmesini gerektirir.

- Hem değerlendirme sırasında gözlemlenen hem de faaliyete uygulanabilecek olan en iyi uygulamalar yönteminin kullanımı hakkında bir değerlendirme ve tespit,

- Gerekirse, geliştirme amacına yönelik tavsiyeler,

- İç Denetim Yöneticisi'nin bir eylem planını ve uygulama tarihlerini de içeren cevapları.

13. Hesap verebilirlik ve şeffaflığın sağlanması için İç Denetim Yöneticisi, - önemli konular için planlanmış düzeltici tedbirlerin ayrıntılarını ve söz konusu planlanmış tedbirlerin başarıya ulaşıp ulaşmadığına dair müteakip bilgiyi de içerecek şekilde -, dış kalite değerlendirmelerinin sonuçlarını, üst yönetim, yönetim kurulu ve dış denetçiler gibi faaliyetten fayda sağlayan ilgili taraflarla paylaşmalıdır.

# Uygulama Önerisi 1312-2: Dış Değerlendirmeler: Bağımsız Onaylı Özdeğerlendirme

Uluslararası İç Denetim Standartlarından
Standart 1312'nin Yorumu

## İlgili Standart

**1312 Dış Değerlendirmeler**

Dış değerlendirmeler, kurum dışından vasıflı ve bağımsız bir gözden geçirme uzmanı veya ekibi tarafından en azından beş yılda bir yapılmalıdır. Dış değerlendirme sıklığının arttırılmasına yönelik potansiyel ihtiyaç, dış gözden geçirme uzmanı veya ekibinin sahip olması gereken vasıflar ve bunların bağımsızlığı meseleleri, menfaat çatışması ihtimali de dikkate alınarak, İç Denetim Yöneticisi ile Yönetim Kurulu ve Denetim Kurulu arasında tartışılmalıdır. Bu tartışmalarda, gözden geçirme görevlisi veya ekibinin tecrübesi değerlendirilirken, kurumun büyüklüğü, karmaşıklığı ve sektörü dikkate alınmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyeti kapsamında dış değerlendirmeler yaparken bu önerileri dikkate almalıdır. Ancak bu kılavuzun, kapsamlı dış değerlendirmeler için gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; sadece dış değerlendirme uygulamaları konusunda bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## Özet

1. İç Denetim Yöneticisi, iş kapsamı *Standartlar*da sayılan bütün faaliyetleri kapsayacak şekilde, iç denetim faaliyetini kurmaktan sorumludur. Bunu sağlamak, *Standart 1300*, İç Denetim Yöneticisinin bir *Kalite Güvence ve Geliştirme Programı* (KGGP) geliştirmesini ve sürdürmesini gerektirmektedir. KGGP'ye nitelikli ve bağımsız bir gözden geçirmesi veya gözden geçirme ekibi

tarafından her beş yılda bir dönemsel dış değerlendirme yapılması dâhil edilmelidir. Dış değerlendirme, bağımsız değerlendirme ile kapsamlı bir özdeğerlendirme şeklini alabilir. Bu dış değerlendirmeler, sadece kurumun KGGP'si ile sınırlı olmamalı, iç denetim faaliyeti tarafından yapılan tüm denetim ve danışmanlık alanlarını kapsamalıdır (bkz. Uygulama Önerisi 1300-1).

**Bağımsız Onaylı Özdeğerlendirme**

2. IIA, bağımsız bir gözden geçirme uzmanı veya ekibi tarafından yapılacak bir dış değerlendirmenin küçük çaplı iç denetim faaliyetleri için sorun çıkarabileceğine veya diğer kurumlarda tam bir dış değerlendirmenin uygun veya gerekli olmayacağına dair endişeleri dikkate almıştır. Örneğin, iç denetim faaliyeti

   (a) aşırı düzenleme ve/veya gözetimin olduğu bir sektörde olabilir

   (b) yönetişim ve iç kontrol ile ilgili yoğun bir dış gözetim ve yönlendirmenin olduğu bir alanda olabilir

   (c) en iyi uygulamalarla yoğun kıyaslamaların dış değerlendirme veya danışmanlık hizmetleri tarafından henüz yapılmış olduğu bir ortamda olabilir veya

   (d) İç Denetim Yöneticisi'nin, iç KGGP gücünün ve çalışanların gelişiminin özdeğerlendirmesinin dışarıdan bir ekip tarafından yapılan kalite değerlendirmesinin faydalarından fazla olduğuna kanaat getirdiği durumlar olabilir.

   IIA, alternatif olarak, aşağıdaki unsurlara sahip bir "bağımsız (dış) onaylı özdeğerlendirme" süreci geliştirmiştir:

   - En azından *Standartlar*a uyumun değerlendirilmesi konusunda, dış değerlendirme sürecinden daha etkili olacak şekilde kapsamlı ve bütünüyle kayıtlı hâle getirilmiş özdeğerlendirme süreci,
   - Vasıflı bir gözden geçirme uzmanı tarafından yerinde gerçekleştirilen bağımsız onay çalışması,

- Ekonomik zaman ve kaynak ihtiyaçları - yani, *Standartlar*a uyumun öncelikli odak konusu olması-.
- Kıyaslama, en iyi uygulamalar yönteminin kullanılmasıyla ilgili danışmanlık ve gözden geçirme çalışması gibi diğer konulara verilen dikkat ve üst ve faaliyet yönetimi ile yapılan görüşmeler azaltılabilir. Ancak bu bilgiler, bir dış değerlendirme için en yararlı bilgilerden biridir.
- Aksi takdirde, Uygulama Önerisi 1312-1'de belirtildiği gibi, aynı şart ve kıstaslar şunlara da uygulanabilir:
  - Genel hususlar.
  - Dış gözden geçirme uzmanı veya ekibinin vasıfları.
  - Bağımsızlık, dürüstlük, tarafsızlık, yetkinlik, yönetim ve yönetim kurulunun onayı, kapsam (araçların, tekniklerin, diğer *en iyi uygulamaların* kullanılması, kariyer gelişimi ve katma değer yaratıcı faaliyetler hariç).
  - Sonuçların raporlandırılması (iyileştirici tedbirlerin belirlenmesi ve uygulaması dâhil).

**Üst Yönetim ve Yönetim Kurulu**

3. İç Denetim Yöneticisi, yaklaşımı tespit etme ve özdeğerlendirme sonuçlarını bağımsız olarak onaylayacak bağımsız gözden geçirme uzmanı veya ekibinin seçme konusunda üst yönetimi ve yönetim kurulunu işe dâhil etmelidir.

**Onaylama Süreci**

4. İç Denetim Yöneticisinin talimatla doğrultusunda çalışan bir ekip, özdeğerlendirme sürecinin tamamına yürütmeli ve belgelendirmelidir. IIA'nın *Kalite Değerlendirme Kılavuzu'nda*, özdeğerlendirme kılavuzu ve araçları dâhil, sürecin tamamı bulunmaktadır. Dış değerlendirmeninkine benzer bir taslak rapor, İç Denetim Yöneticisi'nin *Standartlar*a uygun bir şekilde verdiği kararlarını kapsayacak şekilde hazırlanmalıdır.

5. Vasıflı ve bağımsız bir gözden geçirme uzmanı veya ekibi, sınırlı bir özdeğerlendirme testi uygulamalı ve faaliyetin *Standarlara* uygunluk seviyesi gösterilmesi ve sonuçlar onaylanmalıdır. Bağımsız onay çalışması, IIA'nın *Kalite Değerlendirme Kılavuzu'*nda belirtilen süreçteki veya benzer kapsamlı başka bir süreçteki aşamaları izlemelidir.

6. Özdeğerlendirme ekibinin *Standartlar* ve *Etik Kuralları*na uyuma ilişin değerlendirmelerinin dikkatli bir şekilde gözden geçirilmesini de içeren bağımsız onay sürecinin tamamlanması üzerine:

   - Ehil ve bağımsız dış gözden geçirme uzmanı yukarıda paragraf 4'de belirtilen taslak raporu gözden geçirmeli ve (varsa) çözüme kavuşmamış hususlar konusunda uzlaşma sağlamaya çalışmalıdır.
   - Eğer *Standartlar*a ve *Etik Kuralları*na uygunluk konusundaki değerlendirmelerle mutabıksa, vasıflı bağımsız gözden geçirme uzman(lar)ı bu konuyu (gerekirse) raporun; özdeğerlendirme süreci ve fikri ile mutabık kalarak ve - uygun gördüğü ölçüde - rapordaki tespitler, sonuçlar ve öneriler kısmına eklemelidir.
   - Eğer değerlendirmeler ile mutabık değilse, vasıflı, bağımsız dış gözden geçirme uzman(lar)ı, rapora mutabık olmadığı noktaları, uygun gördüğü ölçüde de önemli tespitler, sonuçlar ve önerileri ile ilgili katılmadığı noktaları belirten bir kısım eklemelidir.
   - Alternatif olarak, vasıflı, bağımsız dış gözden geçirme uzman(lar)ı, özdeğerlendirme *raporuna ek olarak*, yukarıda belirtilen kapsamdaki mutabakat veya mutabakatsızları belirten ayrı bir bağımsız onay raporu hazırlayabilir.
   - Bağımsız onayı haiz nihaî özdeğerlendirme raporu (veya raporları) özdeğerlendirme ekibi ve vasıflı, bağımsız dış gözden geçirme uzman(lar)ı tarafından imzalanmalı ve İç Denetim Yöneticisi tarafından üst yönetime ve yönetim kuruluna sunulmalıdır.

**Sonuçların Rapor Edilmesi**

7. Güvenilirlik ve şeffaflığın sağlanması için İç Denetim Yöneticisi, önemli konular için alınmış planlı düzeltici faaliyetlerin özelliklerini ve bu planlı düzeltici faaliyetlerin gerçekleştirilmesine dair takip eden bilgileri içerecek şekilde, dış kalite değerlendirmelerinin sonuçlarını, üst yönetim, yönetim kurulu ve dış denetçiler gibi değişik taraflarla paylaşmalıdır.

# Uygulama Önerisi 1320-1: Kalite Programı Hakkında Raporlama

Uluslararası İç Denetim Standartlarından
Standart 1320'nin Yorumu

## İlgili Standart

**1320 Kalite Programı Hakkında Raporlama**
İç Denetim Yöneticisi, dış değerlendirme sonuçlarını denetim komitesi ve yönetim kuruluna raporlandırmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyeti kapsamında dış değerlendirmeler yaparken bu önerileri dikkate almalıdır. Ancak bu kılavuzun, kapsamlı dış değerlendirmeler için gerekli olabilecek hususların tümünü kapsamak gibi bir amacı yoktur; sadece dış değerlendirme uygulamaları konusunda bir tavsiyeler demeti sunmaktadır.*

1. Dış değerlendirme çalışması bittiğinde, gözden geçirme ekibi iç denetim faaliyetinin Uluslararası İç Denetim Standartları'na (Standartlar; Uygulama Önerisi 1312-1) uyumluluk derecesi hakkında görüş içeren resmî bir rapor düzenlemelidir. Raporda iç denetim faaliyet yönetmeliği ve diğer standartlara uygunluk ile mevcut durumu geliştirme amacına yönelik tavsiyeler de yer almalıdır. Rapor, değerlendirme çalışmasını talep eden kişiye veya kuruma hitaben düzenlenmelidir. İç Denetim Yöneticisi, dış değerlendirme raporunda açıklanan önemli yorum ve tavsiyelere *cevaben* yazılı bir eylem planı hazırlamalıdır. Bu eylem planının uygun bir şekilde takibi de İç Denetim Yöneticisi'nin sorumluluğundadır.

2. *Standartlara* uyum hakkındaki değerlendirme, dış değerlendirme çalışmasının hayatî bir unsurudur. Gözden geçirme ekibinin, iç

denetim faaliyetinin *Standartlar*a uyumu hakkında değerlendirme yapabilmesi ve fikir beyan edebilmesi için *Standartlar*ı iyi bilmesi gerekir. Ancak, Uygulama Önerisi 1310-1'de belirtildiği gibi, iç denetim faaliyetinin performans değerlendirmesinde dikkate alınması gereken başka kıstaslar da vardır.

# Uygulama Önerisi 1330-1: "Standartlara Uygun Yapılmıştır" İbaresinin Kullanılması

Uluslararası İç Denetim Standartlarından
Standart 1330'un Yorumu

## İlgili Standart

**1330 "Standartlara Uygun Yapılmıştır" İbaresinin Kullanılması**
İç denetçilerin, faaliyetlerinin "Uluslararası İç Denetim Meslekî Uygulama Standartlarına uygun yapıldığını" belirtmeleri teşvik edilir. Ancak iç denetçilerin bu ibareyi kullanabilmesi için, kurumun kalite geliştirme programı hakkındaki değerlendirmelerin, iç denetim faaliyetinin *Standartlar*a uyduğunu göstermesi gerekir.

**Bu Uygulama Önerisinin Niteliği:** *İç Denetçiler, "Uluslararası İç Denetim Standartlarına uygun yapılmıştır" ibaresini kullanırken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun her şeyi kapsamak gibi bir amacı yoktur; bu kılavuz sadece Standartları tamamlayıcı mahiyettedir.*

1. Genel Hususlar: İç denetim faaliyeti hakkında dış ve iç değerlendirmeler, faaliyetin Uluslararası İç Denetim Standartlarına *(Standartlar) ve Etik Kuralları*na uygunluğunu değerlendirecek ve bu konuda bir fikir beyan edecek şekilde yapılmalı ve gerekirse, faaliyeti geliştirme amacına yönelik tavsiyeleri de içermelidir.

2. İç denetim faaliyeti için *beş yılda bir,* bir dış değerlendirme çalışması yapılması esastır. Dış değerlendirme çalışması öngören ve gerektiren yeni standardın daha erken benimsenmesi tavsiye edilir. Dış değerlendirme yaptırmış bulunan kurumların, bir sonraki dış değerlendirme çalışmasını son değerlendirmeden itibaren beş yıl içinde yaptırmaları önerilir.

3. **Uygunluk İbaresinin Kullanılması -** Uygunluk ibaresi, *"Standartlara uygundur"* veya *"Standartlarla uyumludur"* veya *"Standartlara göredir"* şeklinde olabilir. Uygunluk ibaresinin kullanılabilmesi için dönemsel iç değerlendirmelerle birlikte, her beş yılda en az bir dış değerlendirmenin yapılması ve bunun sonucunda iç denetim faaliyetinin *Standartlara ve Etik Kuralları*na uygun olduğu kanaatine ulaşılması gerekir. Uygunluk ibaresinin daha önceden kullanılması, önceki beş yıl içinde yapılmış dış değerlendirme, iç denetim faaliyetinin *Standartlara ve Etik Kuralları*na uyumunu teyid edene kadar uygun değildir. İç denetim faaliyetinin genel kapsam ve faaliyetlerini etkileyebilecek "aykırılık sebepleri" (1 Ocak 2007 itibariyle dış değerlendirme yaptıramama sebepleri dahil) üst yönetime ve yönetim kuruluna açıklanmalıdır.

4. İç denetim faaliyeti tarafından uygunluk ibaresi kullanılmadan önce, bir kalite değerlendirmesi (iç veya dış) sonucu ortaya çıkan ve iç denetim faaliyetinin sorumluklarını yerine getirmesini etkileyen *aykırılıklar*:

   - Tatmin edici bir şekilde giderilmelidir,
   - Aykırılığı giderici tedbirler tevsik edilmeli ve ilgili değerlendirmecilere, aykırılığın tatmin edici şekilde giderildiğine dair mutabakatlarını sağlamak üzere raporlanmalıdır,
   - Aykırılığı giderici tedbirler ve aykırılığı tespit eden ilgili değerlendirmeci(ler) ile olan mutabakat, üst yönetime ve yönetim kuruluna raporlamalıdır.

# Uygulama Önerisi 2000-1: İç Denetim Faaliyetinin Yönetimi

Uluslararası İç Denetim Standartlarından
Standart 2000'in Yorumu

## İlgili Standart

**2000 İç Denetim Faaliyetinin Yönetimi**
İç Denetim Yöneticisi, iç denetim faaliyetini, faaliyetin kuruma değer katmasını sağlayacak etkili bir tarzda yönetmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyetinin yönetilmesi konusunda aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama önerilerine uymak, isteğe bağlıdır.***

1. İç Denetim Yöneticisi, iç denetim faaliyetini,
   - denetim çalışmasının, denetim komitesi ve yönetim kurulunun (gerektiğinde üst yönetimin) onayladığı yönetmelikte tanımlanan genel amaç ve sorumlulukları yerine getirmesini,
   - iç denetim faaliyetinin kaynaklarının verimli ve etkin bir şekilde kullanılmasını,
   - denetim çalışmasının *Uluslararası İç Denetim Standartları*na uygun yapılmasını

   sağlayacak şekilde yönetmekten sorumludur.

# Uygulama Önerisi 2010-1: Planlama

Uluslararası İç Denetim Standartlarından
Standart 2010'un Yorumu

## İlgili Standart

**2010 Planlama**
İç Denetim Yöneticisi, kurumun hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen risk esaslı planlar yapmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyetini planlarken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetim faaliyetinin planlaması, iç denetim faaliyetinin yönetmeliğiyle ve kurumun amaçlarıyla tutarlı olmalıdır. Bu planlama süreci,

   - Hedeflerin,
   - Göreve ait iş çizelgelerinin,
   - Personel kadrosu planlarının ve mali bütçelerin,
   - Faaliyet raporlarının

   belirlenmesini ve hazırlanmasını kapsar.

2. İç denetim faaliyetinin hedefleri, belirli faaliyet plan ve bütçeleri kapsamında *ulaşılabilir*, *gerçekçi* ve mümkün olduğu kadar da *ölçülebilir* olmalıdır. Ayrıca, ölçme kıstasları ve hedeflenen bitiş tarihleri de açıklanmalıdır.

3. Göreve ait iş çizelgeleri aşağıdaki bilgi ve unsurları içermelidir:

- Yapılacak faaliyetler,
- Faaliyetlerin ne zaman yapılacağı,
- Planlanan görevlendirme işinin ve başkalarının sorumluluğundaki bağlantılı işlerin nitelik ve kapsamı dikkate alınarak hesaplanan tahminî iş tamamlama süresi.

4. Görevlendirme iş çizelgesi önceliklerinin belirlenmesinde dikkate alınması gereken hususlar şunlardır:
   - Son görevlendirme tarihleri ve sonuçları,
   - Güncellenmiş risk değerlendirmeleri, risk yönetim ve kontrol süreçlerinin etkinliği,
   - Denetim komitesinin, yönetim kurulunun ve diğer üst yönetimin talepleri,
   - Kurumsal yönetişimle ilgili mevcut sorunlar,
   - Kurumun işleri, faaliyetleri, programları, sistemleri ve kontrollerinde önemli değişiklikler,
   - Faaliyetlerden elde edilebilecek faydaları arttırma fırsatları,
   - Denetim personelinin yetenekleri ve kadro değişiklikleri. İş çizelgeleri, iç denetim faaliyetindeki beklenmedik talepleri karşılayacak şekilde esnek olmalıdır.

# Uygulama Önerisi 2010-2: Denetim Planıyla Risk ve Risk Maruziyeti Arasında Bağlantı Kurulması

Uluslararası İç Denetim Standartlarından
Standart 2010'un Yorumu

## İlgili Standart

**2010 Planlama**
İç Denetim Yöneticisi, kurumun hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen risk esaslı planlar yapmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *Kurumun risk stratejisi de, iç denetim faaliyeti planına yansıtılmalıdır. Kurumun risk yönetimi ile iç denetim süreçleri arasında sinerji yaratmak ve uygulamak amacıyla eşgüdümlü bir yaklaşım izlenmelidir. Bu Uygulama Önerisinde verilenlerin dışında ek hususlar da gerekli olabilir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Her kurum, kendisini olumlu veya olumsuz etkileyebilecek risk ve belirsizliklerle karşı karşıyadır. Risk çeşitli şekillerde yönetilebilir: *Üstlenilerek, kaçınılarak, başkasına transfer edilerek* veya *kontrol* edilerek. Kurum içi kontroller, risk ve belirsizliğin muhtemel olumsuz tesirlerinin azaltılması için kullanılan yaygın yöntemlerdir.

2. İç denetim faaliyetinin denetim planı, kurumu etkileyen ve etkileyebilecek risk ve risk maruziyetleri hakkında yapılan bir değerlendirmeye dayanmalıdır. Risk yönetiminin etkinliğinin değerlendirilmesi yanında, denetimin nihaî hedefi, yönetime, kurumun amaçlarına ulaşmasıyla ilgili olumsuz sonuçları ve etkileri azaltmak için gereken bilgileri vermektir. Riske maruziyetin önemi ve derecesi, çeşitli kontrollerle azaltılabilen bir risk olarak görülebilir.

3. *Denetim evreni*, kurumun stratejik planından unsurlar içerebilir. Bu hâliyle denetim evreni, kurumun genel iş hedeflerini de hesaba katmakta ve yansıtmaktadır. Stratejik planlar, muhtemelen, kurumun risk karşısındaki davranışı ve planlanan hedeflere ulaşma zorluğu hakkında da fikir verir. Denetim evreni, normal şartlar altında, *risk yönetim sürecinin* sonuçlarından da etkilenir. Kurumun *stratejik planı*, kurumun içinde faaliyet gösterdiği ortam dikkate alınarak hazırlanmalıdır. Bu çevre etkenleri, denetim evrenini ve göreli risk değerlendirmesini muhtemelen etkileyecektir.

4. Denetim planı ve evrenindeki güncellemelerde, yönetimin yönelimlerindeki, amaçlarındaki, önceliklerindeki ve odaklandığı hususlardaki değişmeler, göz önünde bulundurulmalıdır. Denetim evreninin kurumun en yeni ve güncel stratejilerini ve yönelimlerini yansıtmasını sağlamak amacıyla, *en azından yılda bir defa* gözden geçirilmesi tavsiye edilir. Bazı şartlar altında, kurumun idarî faaliyetlerinin cereyan ettiği ortamda meydana gelen değişmeler, denetim planlarının daha sık (meselâ, 3 ayda bir) güncellenmesini gerekli kılabilir.

5. Görev iş çizelgeleri, diğer etkenlerin yanı sıra, risk öncelikleri ve risk maruziyetine ilişkin değerlendirmeye de dayanmalıdır. Risk ve riske maruziyetin önemine bağlı olarak, mevcut kaynakların, ne şekilde tahsis edileceğine karar verebilmek için *önceliklerin belirlenmesi* gerekir. Muhtemel denetim alanları arasında İç Denetim Yöneticisinin söz konusu öncelikleri tespit etmesine yardımcı olabilecek çeşitli *risk modelleri* mevcuttur. Risk modellerinin çoğunda, öncelik tespiti için aşağıdakiler gibi risk etkenleri kullanılmaktadır: Mali etkiler, varlıkların likiditesi, yönetimin yetkinliği (ehil olması), iç kontrollerin kalitesi, değişim veya istikrar derecesi, son denetim görevinin tarihi, karmaşıklık düzeyi, personel ve kamuyla ilişkiler, vs. Denetim yaparken, risk maruziyetinin onay ve sınanması için kullanılan yöntem ve teknikler, riskin önem seviyesi ve gerçekleşme ihtimalini dikkate almalıdır.

6. Yönetime yönelik rapor ve bildirimlerde, risk yönetimi sonucu varılan kanaatler açıklanmalı ve riske maruziyeti azaltmaya yönelik tavsiyelerde bulunulmalıdır. Yönetimin riske maruziyet derecesini tam anlayabilmesi için, denetim raporunun, amaçlara ulaşılmasına engel olabilecek risk maruziyetinin sonucunu ve taşıdığı hayatiyeti açıklıkla belirtiyor olması çok önem taşır.

# Uygulama Önerisi 2020-1: Bildirim ve Onay

Uluslararası İç Denetim Standartlarından
Standart 2020'nin Yorumu

## İlgili Standart

**2020 Bildirim ve Onay**
İç Denetim Yöneticisi, önemli ara değişiklikler de dahil, iç denetim faaliyetinin planlarını ve kaynak ihtiyaçlarını, gözden geçirme ve onay için üst yönetime, denetim komitesine ve yönetim kuruluna bildirmelidir. İç Denetim Yöneticisi, kaynak sınırlamalarının etkilerini de bildirmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyetinin planlarını ve kaynaklarını bildirir ve bu konuda onay talep ederken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç Denetim Yöneticisi, iç denetim faaliyetinin iş programı, personel kadro planı ve mali bütçesinin bir özetini yılda bir kere onay için denetim komitesine ve yönetim kuruluna (gerekirse üst yönetime) sunmalıdır. İç Denetim Yöneticisi, bütün önemli ara değişiklikleri de onay ve bilgi için sunmalıdır. Görevlendirme iş programları, personel kadro planları ve mali bütçeler; üst yönetimi, denetim komitesini ve yönetim kurulunu, iç denetim çalışmasının kapsamı ve bu kapsam üzerindeki sınırlamalar hakkında bilgilendirmelidir.

2. Onaylanmış görev iş programları, personel kadro planı, mali bütçe ve bunlardaki bütün önemli ara değişiklikler; denetim komitesinin, yönetim kurulunun, iç denetim faaliyetinin amaç ve planlarının kurumun, denetim komitesinin ve yönetim kurulunun amaç ve planlarını destekleyip desteklemediğini belirlemesine yetecek kadar bilgi içermelidir.

# Uygulama Önerisi 2030-1: Kaynak Yönetimi

Uluslararası İç Denetim Standartlarından
Standart 2030'un Yorumu

## İlgili Standart

**2030 Kaynak Yönetimi**
İç denetim yöneticisi, onaylı planın uygulanabilmesi için, iç denetim kaynaklarının uygun ve yeterli olmasını ve etkin bir şekilde kullanılmasını sağlamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç Denetçiler, "Uluslararası İç Denetim Meslekî Uygulama Standartlarına uygun yapılmıştır" ibaresini kullanırken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun değerlendirmede gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.*

1. İç Denetim Yöneticisi, öncelikle, iç denetim yönetmeliğinde ayrıntılarıyla anlatılan iç denetimin sorumluluklarının yerine getirilmesini sağlayan iç denetim kaynaklarının yönetiminden ve verimliliğinden sorumludur. Bu sorumluluk, kaynak ihtiyacının ve konumunun üst yönetim ve yönetim kuruluna etkili bir şekilde bildirilmesi ve rapor edilmesini de içerir. İç denetim kaynakları içinde, çalışanlar, dış kaynaklar ya da bunların bir birleşimi olabilir. İç denetim kaynaklarının yeterliğinin güvencesi tamamen *yönetim kurulu* ve *üst yönetimin* sorumluluğundadır. İç Denetim Yöneticisi, bu sorumluluğun yerine getirilmesinde onlara yardım etmelidir.

2. İç denetim kaynaklarının becerileri, kabiliyetleri ve teknik bilgileri, planlanan faaliyetlere uygun olmalıdır. İç Denetim Yöneticisi, iç denetim faaliyetlerini gerçekleştirmek için gerekli olan özel becerileri belirlemek üzere dönemsel beceri değerlendirmeleri ve envanter çalışmaları yapmalıdır. Beceri değerlendirmesi, risk

değerlendirme ve denetim planında tanımlanan değişik ihtiyaçları dikkate almalı ve bunlar üzerine kurulmalıdır. İç Denetim Yöneticisi, beceri değerlendirmesinde tanımlanan beceri, bilgi ve özel envanter çalışmaları yapmalıdır. Beceri değerlendirmesi, risk değerlendirme ve denetim planında tanımlanan değişik ihtiyaçları dikkate almalı ve bunlar üzerine kurulmalıdır. İç Denetim Yöneticisi, beceri değerlendirmesinde tanımlanan beceri, bilgi ve özelliklere sahip kaynakları belirlemeli ve tahsis etmelidir. Bu değerlendirme, teknik becerilerin, dil becerilerinin, iş bilgisinin, suiistimalin araştırma ve engelleme becerisinin, muhasebe ve denetim uzmanlığının değerlendirilmesini içerebilir. İç Denetim Yöneticisi, beceri değerlendirmesinin, denetim kapsamının ihtiyaçlarına göre yapıldığını ve bu kapsamın, esas olarak iç denetim kurumunda mevcut kabiliyetlere göre önceden belirlenmemiş olduğunu temin etmelidir.

Riskin dinamik yapısı göz önüne alınarak, İç Denetim Yöneticisi, dönemsel olarak beceri değerlendirmesini güncellemelidir. Bu güncellemelere dayanarak, İç Denetim Yöneticisi, mevcut personelin beceri, kabiliyet ve bilgisinin arttırılma ihtiyacını da dikkate almalıdır. Beceri değerlendirmesinin boyutu ve yapısı, iç denetim işlevinin büyüklüğü ve yapısına uygun olmalıdır.

3. Hem personel hem de muhasebe açısından, iç denetim kaynakları, denetim faaliyetlerini denetim komitesi ve yönetim tarafından beklenen hem derinlik hem de zamanlama konusunda yerine getirmek için yeterli olmalıdır. Kaynak planlamaları, aşağıdaki gibi denetim kapsamı ve unsurlarını dikkatli bir şekilde göz önüne alınmalıdır:

   a. Dönem içinde kapsanan denetim evreninin miktarı.

   b. Plandaki daha yüksek risk alanlarının kapsamı.

   c. Coğrafî kapsam.

d. Planlanmayan projeler, yönetimin istekleri veya diğer denetim-dışı olaylar içi gerekli olan kapasite.

e. Yapılacak işin yapısı ve büyüklüğü.

4. İç Denetim Yöneticisi ayrıca kaynakların verimli kullanımını da güvence altına almalıdır. Bunun içinde, özel görevler için yeterli ve ehil denetçilerin görevlendirilmesi de vardır. Ayrıca, işin yapısı, karmaşıklığı ve kurumun coğrafî yayılımına uygun kaynak yaklaşımı ve kurumsal yapı geliştirmek de bunun içindedir.

5. Kaynak seviyelerinin yeterliliğini göz önüne alırken, maliyet veya diğer sebeplerle karşılıklı geçişler (trade-offs) düşünülüyorsa, İç Denetim Yöneticisi, iç denetim planının kapsam ve zamanlaması üzerindeki etkilere dair açık ifadelerin karar süresinde gözden kaçmamasını temin etmelidir. İç Denetim Yöneticisi, kaynak seviyelerinin, iç denetim yönetmeliğini yerine getirmek için yetersiz olduğuna kanaat getirirse, bu düşünce, nihaî kararı vermeleri için yönetim kurulu ve üst yönetime açık bir şekilde rapor edilmelidir.

6. Genel bir kaynak yönetimi açısından, İç Denetim Yöneticisi, planlama aşamaları, personel değerlendirmesi ve gelişim programları ve diğer insan kaynakları disiplinleri gibi konuları da dikkate almalıdır. İç Denetim Yöneticisi ayrıca, bu beceriler iç denetim faaliyetinin kendisinde olsun olmasın, iç denetimin *kaynak ihtiyaçlarının* doğru tespit edildiğini temin etmelidir. Bunun yanında İç Denetim Yöneticisi, dış kaynak düzenlemeleri, diğer şirket çalışanları veya uzman danışmalar dâhil olmak üzere, kaynak ihtiyaçlarının tespit edilmesinde diğer yaklaşımları dikkate almalıdır.

7. Kaynakların yapısının hassas olması sebebiyle, İç Denetim Yöneticisi, iç denetim faaliyeti için gerekli olan kaynakların yeterliği konusunda üst yönetim ve yönetim kurulu ile *devamlı*

*iletişim* ve *diyalog hâlinde* olmalıdır. İç Denetim Yöneticisi, en az yılda bir kez, yönetim kuruluna kaynakların yeterliği ve durumu hakkında ayrıntılı bir durum raporu sunmalıdır. İç Denetim Yöneticisi, yönetim kuruluna, kaynakların yeterliğini göstermek üzere, ilişkili, güvenilir ve doğru bilgi verildiğini güvence altına almalıdır. Bunun için, İç Denetim Yöneticisi, kaynakların genel yeterliğini gözlemlemekte kullanılabilecek uygun ölçümler, amaçlar ve hedefler geliştirmelidir. Bunların içinde, denetim planı ile kaynakların kıyaslanması, geçici boşluk veya eksikliklerin etkisi, eğitim faaliyetleri, kurumun iş veya risk profilinde ve üçüncü parti düzenlemelerindeki değişiklikler nedeniyle özel beceri ihtiyaçları ve gerekliliklerdeki değişiklikler de vardır.

# Uygulama Önerisi 2040-1: Politika ve Prosedürler

Uluslararası İç Denetim Standartlarından
Standart 2040'ın Yorumu

## İlgili Standart

**2040 Politika ve Prosedürler**
İç Denetim Yöneticisi, iç denetim faaliyetini yönlendirmek amacına yönelik politika ve prosedürleri belirlemelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, politika ve prosedürleri tespit ederken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun bu değerlendirmede gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

Yazılı politika ve prosedürlerin biçim ve içeriği, iç denetim faaliyetlerinin *yapısına, büyüklüğüne* ve işin *karmaşıklık düzeyine* uygun olmalıdır. Bütün iç denetim kurumlarının yazılı idarî ve teknik *denetim el kitaplarına* ihtiyacı olmayabilir. Küçük çaplı iç denetim faaliyetleri, yazılı ve resmî olmayan yollarla yönetilebilir. Küçük bir iç denetim faaliyetinin personeli, günlük yakın kontrol ve gözetimle ve yazılı not ve tutanaklarla yönlendirilebilir ve kontrol edilebilir. Ancak büyük iç denetim faaliyetlerinde, denetim personelinin iç denetim faaliyetlerine ilişkin uygulama standartlarına sürekli uymasını sağlamak ve onları bu yönde yönlendirmek için, daha kapsamlı, resmî ve yazılı politika ve prosedürlere sahip olmak şarttır.

# Uygulama Önerisi 2050-1: Eşgüdüm

Uluslararası İç Denetim Standartlarından
Standart 2050'nin Yorumu

## İlgili Standart

**2050 Eşgüdüm**

İç Denetim Yöneticisi; aynı çalışmaların gereksiz yere tekrarlanmasını asgarîye indirmek ve işin kapsamını en uygun şekilde belirlemek amacıyla, ilgili güvence ve danışmanlık hizmetlerini yerine getiren diğer iç ve dış sağlayıcılarla, mevcut bilgileri paylaşmalı ve faaliyetleri bunlarla eşgüdüm içinde sürdürmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, ilgili güvence ve danışmanlık hizmetlerini yerine getiren diğer sağlayıcılarla çalışmaların eşgüdümünü sağlarken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun bu konuda gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Aynı çalışmaların gereksiz yere tekrarlanmasının asgarîye indirilmesi ve işin kapsamının en uygun şekilde belirlenmesi amacıyla, iç ve dış denetim işlerinin eşgüdümünün sağlanması gerekir. İç denetim işlerinin kapsamı, risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve iyileştirmek amacına yönelik, sistemli ve disiplinli bir yaklaşımı içerir. İç denetim işlerinin kapsamı, *2100 numaralı standartlarda* açıklanmaktadır. Öte yandan, dış denetçilerin olağan inceleme çalışmaları, yıllık mali tabloların genel olarak âdil olup olmadığı ve gerçeği yansıtıp yansıtmadığı hakkındaki görüşü desteklemek için yeterli delilin elde edilmesini sağlayacak şekilde tasarlanır. Dış denetim işinin kapsamı, ilgili meslekî standartlara göre belirlenir ve dış denetçiler, yıllık mali tablolar hakkında görüş beyan etmek amacıyla uyguladıkları prosedürlerin ve elde ettikleri delillerin

yeterliliğine karar vermekten sorumludur.

2. İç denetim faaliyetiyle eşgüdüm de dahil, dış denetçilerin çalışmalarının gözetimi, denetim komitesinin, *yönetim kurulunun* tam sorumluluğundadır. Fiilî eşgüdümü sağlamaktan İç Denetim Yöneticisi sorumlu olmalıdır. *İç Denetim Yöneticisi*, denetim işlerinin etkin eşgüdümünü sağlamak için denetim komitesi ve yönetim kurulundan destek talep edecektir.

3. İç denetçilerin işleriyle dış denetçilerin işleri arasında eşgüdümün sağlanması için, İç Denetim Yöneticisi, iç denetçilerin *2100 numaralı standartlardaki* kurallara göre yapacakları işlerin, iç denetimin kapsamı açısından güvenilir nitelikte olan dış denetim işlerinin bir tekrarı olmamasını sağlamalıdır. Meslekî ve örgütsel raporlama sorumlulukları ve görevlerinin izin verdiği sınırlar içinde, iç denetçiler, görevlerini, azamî denetim eşgüdümü, etkinliği ve verimliliğini sağlayacak bir tarzda yapmalı ve yürütmelidir.

4. İç Denetim Yöneticisi, dış denetçilerin yıllık mali tabloların denetlenmesiyle ilgili iş ve görevlerini yapmayı kabul edebilir. İç denetçilerin, dış denetçilere görevlerini ve sorumluluklarını yerine getirmelerinde yardımcı olmak amacıyla yapacakları işler, Uluslararası İç Denetim Standartlarının ilgili bütün hükümlerine tâbidir.

5. İç Denetim Yöneticisi, iç ve dış denetçiler arasındaki eşgüdüm konusunda düzenli değerlendirmeler yapmalıdır. Bu değerlendirmeler, toplam denetim maliyeti de dahil, iç ve dış denetim işlevlerinin genel etkinliği ve verimliliğiyle ilgili değerlendirmeleri de içerebilir.

6. Denetim komitesi ve yönetim kurulu, genel kontrol ve izleme görevini yerine getirirken, İç Denetim Yöneticisinden, dış denetçilerin performansını değerlendirmesini isteyebilir. Bu değerlendirmeler, normal olarak, İç Denetim Yöneticisinin iç ve

dış denetim çalışma ve faaliyetlerinin eşgüdümünü sağlama görevinin bir parçası olarak yapılmalı ve başka performans konularını, ancak denetim komitesi ve yönetim kurulunun veya üst yönetimin özel talebi hâlinde kapsamalıdır. Dış denetçilerin performansı hakkındaki değerlendirmeler, varılan sonuçları destekleyen yeterli veri ve bilgilere dayandırılmalıdır. İç ve dış denetim faaliyetlerinin eşgüdümü konusunda dış denetçilerin performans değerlendirmeleri, bu uygulama önerisinde açıklanan kıstaslara dayanmalı ve bunları yansıtmalıdır.

7. İç denetçilerin çalışmalarıyla eşgüdüme ilişkin konuların dışında, dış denetçilerin performansı hakkındaki değerlendirmeler, aşağıdakiler gibi bazı *ek etkenler*i de kapsayabilir:
   - Meslekî bilgi ve deneyim,
   - Kurumun faaliyet gösterdiği sektör hakkında bilgi,
   - Bağımsızlık,
   - Özel uzmanlık hizmetlerinin mevcudiyeti,
   - Kurumun ihtiyaçlarının önceden tahmin edilmesi ve bu ihtiyaçlara cevap verilmesi,
   - Kilit nitelikteki görev personelinin devamlılığının makul ölçüler içinde sağlanması,
   - Gerekli iş ilişkilerinin sürdürülmesi,
   - Sözleşmeden kaynaklanan taahhütlerin yerine getirilmesi,
   - Kuruma genel değer kazandırılması.
8. İç Denetim Yöneticisi, iç ve dış denetçiler arasındaki eşgüdüm hakkında yaptığı değerlendirmelerin sonuçlarını, gerektiğinde, dış denetçilerin performansına ilişkin görüşleriyle birlikte, üst yönetime, denetim komitesine ve yönetim kuruluna rapor etmelidir.

9. Meslekî standartlar uyarınca, dış denetçilerin belirli konuları

denetim komitesi ve yönetim kuruluna rapor etmeleri gerekebilir. İç Denetim Yöneticisi, sorunlar hakkında bir anlayış birliğine varmak amacıyla, bu konularda dış denetçilerle iletişim kurmalı ve bilgi alışverişi yapmalıdır. Bu konular şunları da içerebilir:

- Dış denetçilerin bağımsızlığını etkileyebilecek konu ve sorunlar,
- Önemli kontrol zayıflıkları,
- Hatâlar ve usulsüzlükler,
- Yasa dışı fiil ve işlemler,
- Yönetim kararları ve muhasebe tahminleri,
- Önemli denetim ayarlamaları,
- Yönetimle olan anlaşmazlıklar ve
- Denetimin yapılmasında karşılaşılan güçlükler.

10. Denetim çalışmalarının eşgüdümü; karşılıklı çıkarları ilgilendiren konuları tartışmak amacına yönelik dönemsel toplantıları da kapsar:

- **Denetim kapsamı:** Denetim kapsamı konusunda eşgüdümü sağlamak ve aynı çalışmaların gereksiz yere tekrarlanmasını asgarîye indirmek için, iç ve dış denetçilerin planladığı denetim faaliyetleri tartışılmalı ve görüşülmelidir. Denetim süreci sırasında, denetim çalışmalarının eşgüdümünü ve denetim faaliyetlerinin etkinliğini ve zamanında tamamlanmasını sağlamak ve o güne kadar yapılan işlerle ilgili gözlem ve tavsiyelerin planlanan işlerin kapsamında bir ayarlama yapılmasını gerektirip gerektirmediğine karar vermek amacıyla, yeterli sayıda toplantı düzenlemelidir.
- **Birbirlerinin denetim programlarına ve çalışma kâğıtlarına erişim:** İç denetçilerin dış denetim çalışmasının sonuçlarını iç denetim amaçlarıyla kullanmanın kabul edilebilirliği konusunda tatmin olabilmeleri için, dış

denetçilerin programlarına ve çalışma kâğıtlarına erişmeleri önemli olabilir. Bu erişim yetkisi, iç denetçilerin bu programların ve çalışma kâğıtlarının gizliliğini koruma sorumluluğuna da beraberinde getirir. Aynı şekilde, dış denetçilerin iç denetim çalışmasının sonuçlarını dış denetim amacıyla kullanmanın uygun olduğunu konusunda tatmin olabilmesi için, iç denetçilerin programlarına ve çalışma kâğıtlarına erişmeleri de önemli olabilir.

- **Denetim raporları ve idarî yazışmaların değişimi:** İç denetimin nihaî rapor ve yazıları, yönetimin bu rapor ve yazılara verdiği yanıtlar ve daha sonraki iç denetim faaliyet takibi incelemeleri, dış denetçilere de açık olmalıdır. Bu rapor ve yazılar, dış denetçilerin denetim işlerinin kapsamını tespit etmesine ve gerekli ayarlamaları yapmasına yardımcı olur. Ayrıca, iç denetçilerin de dış denetçilerle ilgili idarî yazışmalara erişebilmesi gerekir. İdarî yazışmalarda ele alınan ve tartışılan sorun ve konular, iç denetçilerin gelecek iç denetim çalışmasında vurgulanması gereken alan ve konuları planlamasına yardımcı olur. İdarî yazışmaların incelenmesinden ve ilgili yöneticilerin, denetim komitesinin ve yönetim kurulunun gereken düzeltici tedbirleri başlatmasından sonra, İç Denetim Yöneticisi, gerekli takip ve düzeltme çalışmasının yapılmasını sağlamalıdır.

- **Denetim teknikleri, yöntemleri ve terminoloji konusunda anlayış birliği:** İlk olarak, İç Denetim Yöneticisi, dış denetçilerin planladığı işlerin kapsamını tam olarak anlamalı ve dış denetçilerin planladığı işlerin planlanan iç denetim işleriyle birlikte *2100 numaralı standartlardaki* gereklere uygun olduğu konusunda tatmin olmalıdır. İç Denetim Yöneticisinin, bu konuda tatmin olması için, dış denetçilerin planlamada kullandığı önem düzeylerini ve dış denetçilerin planladığı prosedür ve çalışmaların niteliği ve kapsamını anlaması gerekir.

İkinci olarak, İç Denetim Yöneticisi, (1) iç ve dış denetim işleri ve çalışmalarını eşgüdümünü sağlamak; (2) dış denetçilerin işlerini güvenilirlik açısından incelemek ve değerlendirmek ve (3) *dış* denetçilerin hedeflerine ulaşmaları için gereken bazı işleri yapacak olan iç denetçilerin dış denetçilerle etkin iletişim kurmasını sağlamak için, dış denetçilerin teknikleri, yöntemleri ve terminolojisinin iç denetçiler tarafından da yeterince anlaşıldığından emin olmalıdır.

Son olarak, İç Denetim Yöneticisi, dış denetçilerin bu teknikler, yöntemler ve terminoloji kullanılarak yapılan işlere güvenebilmelerini sağlamak için, dış denetçilerin iç denetçilerin teknikleri, yöntemleri ve terminolojisini anlamasını sağlamak amacıyla yeterli bilgiyi dış denetçilere vermelidir. İç ve dış denetçilerin işlerinin etkin ve verimli bir şekilde eşgüdümünü sağlamak ve birbirlerinin çalışmalarına güvenebilmek için *benzer* teknikler, yöntemler ve terminoloji kullanmaları daha etkin ve verimli olabilir.

# Uygulama Önerisi 2050-2: Dış Denetim Hizmetlerinin Satın Alınması

Uluslararası İç Denetim Standartlarından
Standart 2050'nin Yorumu

## İlgili Standart

**2050 Eşgüdüm**

İç Denetim Yöneticisi; aynı çalışmaların gereksiz yere tekrarlanmasını asgarîye indirmek ve işin kapsamını en uygun şekilde belirlemek amacıyla, ilgili güvence ve danışmanlık hizmetlerini yerine getiren diğer iç ve dış sağlayıcılarla, mevcut bilgileri paylaşmalı ve faaliyetleri bunlarla eşgüdüm içinde sürdürmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç Denetim Yöneticisi, dış denetim hizmetleri satın almaları istendiği takdirde veya bu konuda görevlendirildikleri takdirde aşağıdaki önerileri dikkate almalıdır. Bu öneriler; dış denetim hizmetlerini temin etmekle görevlendirildikleri takdirde denetim komitesi ve finans yönetimine de faydalı olabilir. Ancak bu kılavuzun her durumda ve her koşulda dikkate alınması gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur. İç Denetim Yöneticileri, bu kılavuzdaki önerileri, özel koşullara ve durumlara uyarlamak için gereken değişiklikleri yapmalıdır. Bu uygulama önerisi, özellikle, mali tabloların denetimi için dış denetim hizmetlerinin satın alınmasında uygun olabilir, fakat başka görev türleri için dış denetim hizmetlerinin temin edilmesinde de faydalı olabilir. İç ve dış denetim çalışmaları ve faaliyetlerinin "eşgüdümü"yle ilgili öneriler için "Eşgüdüm" standartıyla ilgi PA 2050-1 sayılı Uygulama Önerisine bakınız.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçilerin kurum için dış denetçilerin seçilmesi, seçeneklerin değerlendirilmesi veya dış denetçilerin tutulması sürecine katılımı ve katkısı; bu süreçte hiçbir rolü olmamaktan, yönetime veya denetim komitesine tavsiyelerde bulunmaya ve sürece, sürecin yönetimine veya sürecin denetimine katılmaya veya yardıma kadar

farklılık gösterebilir. *IIA Standartları* iç denetçilerin "ilgili güvence ve danışmanlık hizmetlerinin diğer iç ve dış sağlayıcılarıyla mevcut bilgileri paylaşmalarını ve faaliyetlerin eşgüdümünü" gerektirdiği için, iç denetçilerin dış denetçilerin seçilmesi veya tutulmasında ve iş kapsamlarının belirlenmesinde belirli bir rol oynaması veya katkıda bulunması uygun olabilir.

2. Denetim komitesinin ve yönetim kurulunun onayladığı bir politika; mevcut hizmet sağlayıcılarının bir teklif isteme kararını ilgili kurumun mevcut hizmetlerden memnun olmadığının bir işareti veya göstergesi olarak algılamaması için, dönemsel dış denetim hizmeti taleplerini kolaylaştırabilir ve bu talepleri normal iş faaliyetlerinin bir parçası yapabilir. Bu konuda belirli somut bir politika yoksa, iç denetçi bu hizmetlerin, kurumun başka mevcut hizmet tedarik politikalarına tâbi olup olmadığını belirlemelidir. Uygun politikaların bulunmaması hâlinde, iç denetçi, bu konuda uygun kural ve politikaların belirlenmesini *sağlamayı düşünmelidir*.

3. Dış denetim hizmetlerinin seçilmesi veya dış denetçilerin tutulmasıyla ilgili uygun politikalar, aşağıda sayılan konuları kapsamalıdır:

    - Politikanın yönetim kurulu veya denetim kurulu tarafından onaylanması,
    - Politika kapsamındaki hizmetlerin niteliği ve türü,
    - Sözleşmenin süresi, resmî hizmet taleplerinin sıklığı ve/veya mevcut hizmet sağlayıcılarıyla çalışmaya devam etme kararı,
    - Dış denetçi seçim ve değerlendirme ekibinin üyeleri veya katılımcıları,
    - Değerlendirmede dikkate alınması gereken kritik veya temel kıstaslar,
    - Hizmet ücretleriyle ilgili sınırlamalar ve politika istisnaları onay prosedürleri,

- Belirli sektörler veya ülkelere özgü idarî veya hukukî koşullar veya benzeri kurallar.

4. Denetim veya yönetim kurulunun onayladığı bir politika, sadece mali tabloların denetlenmesi dışında, dış denetim firmalarının sunduğu başka hizmetlerin alınması konusunu da kapsayabilir. Bu politika şu konuları içerebilir:
   - Vergi hizmetleri,
   - Danışmanlık hizmetleri ve diğer denetim-dışı hizmetler
   - İç denetim için dış kaynak kullanımı ve/veya müşterek kaynak kullanımı hizmetleri,
   - Dış kaynak kullanımı veya müşterek kaynak kullanımı yoluyla temin edilen diğer hizmetler,
   - Kararlaştırılan hizmet görevlendirmeleri gibi özel hizmetler,
   - Değerleme, kıymet takdiri ve aktüerya hizmetleri,
   - Personel alımı, defter tutma ve teknoloji hizmetleri gibi geçici hizmetler,
   - Dış denetim firmalarının verdiği hukukî hizmetler.

5. Mevcut hizmet sağlayıcılarının göreve devam etmesine ve başka potansiyel hizmet sağlayıcılarından teklif istenmemesine veya teklif isteminin ertelenmesine ilişkin dönemsel ve resmî kararları destekleyen uygun belge ve kayıtlar saklanmalıdır.

6. Seçim kurulunun katılımcılarını, sürecin her safhası için temel sonuç materyalleri ve hedef tarihlerini, teklif istenecek adayları, talep edilecek hizmetlerin niteliği ve kapsamını ve bilgilerin potansiyel adaylara nasıl verileceğini açıklayan bir seçme süreci planı yapılmalı ve hazırlanmalıdır. Seçme sürecinin başlangıcında, bir kurum, sıklıkla, bütün potansiyel adayların katıldığı kapsamlı bir toplantı düzenleyebilir. Bu toplantıda, yönetim, hizmet talebiyle

ilgili bilgileri içeren bir sunum yapar ve adaylara, talep edilen hizmetleri tanımlayan ve açıklayan bir bilgi paketi veya rapor verir ve dağıtır. Bu genel toplantıdan sonra, her adayla ayrı saha toplantıları yapılabilir ve bu toplantılara ilgili yönetim temsilcileri katılabilir. Özel durumlarda, başka toplantı ve bilgilendirme paketleri kombinasyonları da pratik veya uygun olabilir.

7. Potansiyel hizmet sağlayıcılarının sayısını azaltarak, makul sayıda nihaî aday tespit etmek amacına yönelik bir eleme sürecini kolaylaştırmak için *iki aşamalı* bir hizmet talebi sistemi uygulanabilir. *İlk olarak,* bilgi talepleri, potansiyel adaylar hakkında temel bilgiler ve başka genel bilgiler de dahil, adayların *vasıfları* hakkında gerekli bilgilerin temin edilmesine odaklanmalıdır. İlgili firmanın tarihçesi, firmanın büyüklüğü, mevcut kaynak ve imkânları, kurum felsefesi ve denetim yaklaşımı, özel uzmanlık alanı, görevi üstlenecek olan yerel veya hizmet ofisi, ilgili sektördeki uzmanlığı ve göreve tahsis edilecek olan temel ekip üyelerinin biyografileri gibi bilgiler toplanmalıdır.

8. *İlk eleme sürecinden sonra,* bir sonraki safhaya geçmek için seçilen adaylara, talep edilen hizmetler hakkında daha ayrıntılı ve özel bilgiler almak için ikinci bir talep gönderilmelidir. Beklenen hizmetleri ve temel hedef tarihleri gösteren ayrıntılı bir *hizmet talep formu* hazırlanmalıdır. Adaylardan, hizmetlerin ücretleri de dahil, belirli özel ayrıntıları bildirmeleri istenmelidir. Sürecin kalan kısmı için, talep edilen ek bilgilerin teslim tarihlerini, adayların *seçim kuruluna* yapacağı sunumları içeren toplantıların tarihlerini ve son seçim tarihini gösteren bir zaman çizelgesi hazırlanabilir ve adaylara verilebilir. Ayrıntılı hizmet talep formu, talep edilen hizmetlerin her birini tanımlamalı ve hizmetlerin bir hizmet sağlayıcısından tek bir paket olarak mı alınacağını, yoksa birden fazla hizmet sağlayıcısı arasında bölüştürüleceğini mi açıklamalıdır.

9. Adayların vasıflarını bazı temel kıstaslara göre karşılaştırmak ve özetlemek ve bunu, bütün hizmet sağlayıcılarının tutarlı ve objektif bir şekilde değerlendirilmesine imkân veren bir formatta yapmak uygun olabilir. Düşünme süreçlerini teşvik eden ve temel kıstaslara göre değerlendirmeye odaklanan sorular yöneltilebilir. Bir *değerlendirme formu*, seçim kurulunun her üyesinin adayların her biri hakkında yaptığı analizlerin ve vardığı sonuçların toplanmasını kolaylaştırabilir. Kurumun çeşitli adaylarla geçmiş ilişkileri, daha önce alınan hizmetlerin tipleri ve geçmişte uygulanan ücretler gibi temel bilgiler, seçim kuruluna, değerlendirmeye başlamak için uygun bir bakış açısı verebilir.

10. Dış denetim görevleriyle ilgili hizmet düzenlemeleri, yazılı bir anlaşmaya geçirilmeli ve hem ilgili hizmet sağlayıcısı hem de denetlenen tarafından imzalanmalıdır.

11. Seçme süreci sonucunda hizmet sağlayıcısının değiştirilmesi hâlinde, düzgün ve düzenli bir değişiklik için uygun geçiş dönemi planları yapılmalıdır. Gerekirse, resmî kurum ve yetkililer de dahil ilgili taraflara gönderilmesi gereken bildirim ve açıklamalar da zamanında iletilmelidir.

12. İç denetçiler, kurumun dış denetçilerin devam eden hizmet faaliyetleri ve çalışmalarını nasıl izlediğini ve takip ettiğini belirlemelidir. Hizmet sözleşmelerinin ve diğer anlaşmaların koşullarına uyulup uyulmadığı dönemsel olarak incelenmelidir. Dış denetçilerin bağımsız olup olmadığı değerlendirmesine iç denetçiler de katılmalı ve bu değerlendirme *en azından yılda bir kere* yapılmalı ve sonuçları denetim komitesine bildirilmelidir.

# Uygulama Önerisi 2060-1: Denetim Komitesi, Yönetim Kurulu ve Üst Yönetime Raporlama

Uluslararası İç Denetim Standartlarından
Standart 2060'ın Yorumu

## İlgili Standart

**2060 Yönetim Kurulu, Denetim Komitesi ve Üst Yönetime Raporlamalar**

İç Denetim Yöneticisi, iç denetim faaliyetinin amacı, yetkileri, görev ve sorumlulukları ve plana kıyasla performansı konularında, denetim komitesi, yönetim kurulu ve üst yönetime dönemsel raporlar sunmalıdır. Bu raporlar, önemli riskleri, kontrol sorunlarını, kurumsal yönetişim sorunlarını ve denetim komitesi, yönetim kurulu ve üst yönetimin ihtiyaç duyabileceği veya talep edebileceği başka konuları da içermelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, denetim komitesi, yönetim kurulu ve üst yönetime raporlama yaparken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun bu konuda gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç Denetim Yöneticisi, üst yönetime, denetim komitesine ve yönetim kuruluna *yıl boyunca dönemsel olarak* faaliyet raporları sunmalıdır. Bu faaliyet raporları, görevle ilgili önemli tespit ve tavsiyeleri içermeli ve onaylanmış görev iş programları, personel (kadro) planları ve mali bütçelerden önemli sapmaları ve bunların sebeplerini üst yönetime, denetim komitesine ve yönetim kuruluna bildirmelidir.

2. Görevle ilgili önemli tespitler, İç Denetim Yöneticisinin görüş ve kanaatine göre, kurumu olumsuz etkileyebilecek durumlardır.

Görevle ilgili önemli tespitler; usulsüzlük ve yolsuzluklar, yasa dışı fiil ve işlemler, hatâlar, verimsizlik, israf, etkisizlik, çıkar çatışmaları ve kontrol zayıflıkları gibi durumları kapsayabilir. Bu durumları üst yönetimle birlikte inceledikten sonra, İç Denetim Yöneticisi, bu sorunlar tatmin edici bir şekilde çözümlenmiş olsun ya da olmasın, önemli tespit ve tavsiyeleri denetim komitesi ve yönetim kuruluna da bildirmelidir.

3. Yönetimin görevi ve sorumluluğu, görevle ilgili önemli tespit ve tavsiyeler dikkate alınarak alınması gereken tedbirler hakkında kararlar almaktır. Üst yönetim, maliyetinden veya başka hususlardan dolayı, rapor edilen bir sorunu düzeltmeme ve çözmeme riskini üstlenmeye karar verebilir. Üst yönetimin önemli tespit ve tavsiyelere ilişkin bütün kararları, denetim komitesi ve yönetim kuruluna bildirilmelidir.

4. Üst yönetimin, denetim komitesinin ve yönetim kurulunun rapor edilen sorunu düzeltmeme ve çözmeme riskini üstlendiği durumlarda, İç Denetim Yöneticisi, görevle ilgili olarak daha önce rapor edilen önemli tespit ve tavsiyeler hakkında denetim komitesi ve yönetim kuruluna bilgi vermenin uygunluğunu değerlendirmelidir. Bu, özellikle kurumda, denetim komitesi, yönetim kurulu veya üst yönetimde meydana gelen değişikliklerde -veya benzeri başka değişikliklerin olduğu durumlarda- gerekli olabilir.

5. Faaliyet raporları, yukarıda bahsi geçen konulara ek olarak,

   (a) fiilî performansı iç denetim faaliyetinin hedefleri ve görev iş programlarıyla ve (b) harcamaları mali bütçelerle karşılaştırmalıdır. Bu raporlar, önemli sapmaların sebebini açıklamalı ve alınan veya alınması gereken tedbirleri göstermelidir.

# Uygulama Önerisi 2060-2: Denetim Komitesiyle İlişkiler

Uluslararası İç Denetim Standartlarından
Standart 2060'ın Yorumu

## İlgili Standart

**2060 Yönetim Kurulu, Denetim Komitesi ve Üst Yönetime Raporlamalar**

İç Denetim Yöneticisi, iç denetim faaliyetinin amacı, yetkileri, görev ve sorumlulukları ve plana kıyasla performansı konularında, denetim komitesi, yönetim kurulu ve üst yönetime dönemsel raporlar sunmalıdır. Bu raporlar, önemli riskleri, kontrol sorunlarını, kurumsal yönetişim sorunlarını ve denetim komitesi, yönetim kurulu ve üst yönetimin ihtiyaç duyabileceği veya talep edebileceği başka konuları da içermelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyeti ile denetim komitesi arasındaki ilişkiler konusunda aşağıda verilen önerileri dikkate almalıdır. Ancak bu ilkeler, dikkate alınması gereken bütün hususları kapsamak gibi bir amaç gütmemekte, sadece denetim komiteleri ile iç denetim arasında uygun ilişkilerin kurulması için gerekli temel bilgileri özetlemektedir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Bu metinde kullanılan "*denetim komitesi*" terimiyle, kurumun denetim ve kontrol işlevlerinin gözetim ve denetiminden sorumlu yönetim kademesine atıfta bulunulmaktadır. Bu güvene dayanan görevler genellikle bir denetim komitesine verilmesine rağmen, bu uygulama önerisinde verilen bilgiler, yeddieminler, politika ve strateji tayin eden birimler, bir şahıs şirketinin sahipleri, iç kontrol komiteleri veya yönetim kurulları gibi denk yetki ve sorumluluklara sahip başka gözetim ve denetim grupları için de geçerlidir ve onlara da uygulanabilir.

2. *Uluslararası İç Denetçiler Enstitüsü* (IIA), denetim komiteleri ve iç denetçilerin amaçlarının birbirine bağlı olduğunu kabul eder. Bunların her birinin üst yönetim, yönetim kurulu, hissedarlar ve kurum dışı taraflara karşı sorumluluklarını yerine getirebilmesi için, denetim komitesiyle güçlü bir iş ilişkisinin kurulması şarttır. Bu Uygulama Önerisi, denetim komitesi ile iç denetim faaliyeti arasında uygun bir ilişkinin özellik ve nitelikleri hakkında IIA'nın görüşlerini özetlemektedir. IIA, denetim komitesinin sorumluluklarının bu Uygulama Önerisinin kapsamı dışındaki faaliyetleri de kapsadığını bilir; dolayısıyla bu Uygulama Önerisi, denetim komitesinin sorumluluklarının kapsamlı ve tam bir tanımını vermek iddiasıyla hazırlanmamıştır.

3. Denetim komitesi ile iç denetim faaliyeti arasında, esas olarak İç Denetim Yöneticisi aracılığıyla, etkin bir ilişki kurmak için önem taşıyan üç faaliyet alanı vardır:

   - Denetim komitesine, sorumluluklarını yerine getirebilmesi için, yönetmelik, faaliyet ve süreçlerinin uygun olmasını sağlamaya yardımcı olmak,
   - İç denetimin yönetmeliği, rolü ve faaliyetlerinin net ve açık bir şekilde anlaşılmasını ve bunların denetim komitesinin ve yönetim kurulunun ihtiyaçlarına cevap verecek şekilde olmasını sağlamak,
   - Denetim komitesi ve başkanıyla açık ve etkin bir iletişim sürdürmek.

**Denetim Komitesinin Sorumlulukları:**

4. İç Denetim Yöneticisi, denetim komitesi yönetmeliği, rolü ve faaliyetlerinin onun sorumluluklarını yerine getirmesi için uygun olmasını sağlamak konusunda kurula yardımcı olmalıdır. İç Denetim Yöneticisi, faaliyetlerinin dönemsel gözden geçirilmesi ve bu konuda iyileştirme tedbirleri tavsiye edilmesi konularında kurula yardımcı olarak önemli bir rol oynayabilir. Bu yolla, İç

Denetim Yöneticisi, denetim komitesi çalışmaları ve düzenleyici uygulamalar konusunda denetim komitesi için değerli bir *danışman* olabilir. İç Denetim Yöneticisinin yapabileceği faaliyet ve işlerin örnekleri şunlardır:

- Denetim komitesinin yönetmeliğini *en az yılda bir* gözden geçirmek ve bu yönetmeliğin, yönetim kurulunun verdiği emir veya işaretler ışığında, denetim komitesinin üstlendiği bütün sorumluluklara temas edip etmediği konusunda denetim komitesine bilgi vermek,
- Denetim komitesinin toplantıları için, gereken tüm faaliyetlerin ayıntılarını içeren ve bunların tamamlanıp tamamlanmadığını açıklayan ve kendisine verilen bütün görevleri yerine getirdiğini yönetim kuruluna *yılda bir* rapor etmesinde denetim komitesine yardımcı olan bir *planlama gündemi* hazırlamak,
- Denetim komitesinin toplantı gündemini hazırlamak ve kurul başkanının incelemesine sunmak; toplantı malzemelerinin denetim komitesinin bütün üyelerine dağıtımını sağlamak ve denetim komitesi toplantı tutanaklarını yazmak,
- Denetim komitesini, faaliyet ve uygulamalarının genel kabul gören uygulamalara uygun ve tutarlı olmasını sağlamak amacıyla, kurulun faaliyet ve uygulamalarının mevcut *en iyi uygulamalarla* karşılaştırıldığı dönemsel gözden geçirmeler yapmaya teşvik etmek,
- Denetim komitesi üyelerine verilen malzemelerin ve bilgilerin onların ihtiyaçlarını karşılayıp karşılamadığını değerlendirmek için kurul başkanıyla dönemsel toplantılar yapmak,
- Yeni kurul üyelerinin risk ve kontroller konusunda eğitilmesi gibi, eğitim veya bilgilendirme kursları veya sunumlarının yararlı olup olmayacağının denetim komitesine sorulması,
- Kurula ayırdığı zamanın ve görüşme sıklığının yeterli olup olmadığının denetim komitesine sorulması.

**İç Denetim Faaliyetinin Rolü:**

5. İç Denetim Yöneticisinin denetim komitesiyle ilişkisi, denetim komitesinin iç denetim işlevini anlamasını ve desteklemesini ve iç denetim faaliyetinden gereken her konuda yardım almasını sağlamak konusunda İç Denetim Yöneticisinin üstlendiği temel rol etrafında şekillenmelidir. IIA, sağlam bir yönetişimin, etkin kurumsal yönetişim sistemlerinin *dört temel unsuru* arasında yaratılan sinerjiye bağlı olduğuna inanır ve bu tezi destekler: *Yönetim kurulu, yönetim, iç denetçiler ve dış denetçiler*. Bu yapı içinde, iç denetçiler ve denetim komitesi birbirlerini karşılıklı olarak destekler. Denetim komitesinin bir kurumun faaliyetlerini tam olarak anlayabilmesi için, iç denetçilerin işlerinin değerlendirilmesi şarttır. İç Denetim Yöneticisinin kurula karşı üstlendiği rolün aslî bir unsuru da, bu hedefe ulaşılmasını ve kurulun İç Denetim Yöneticisini güvenilir bir danışmanı olarak görmesini temin etmektir. İç Denetim Yöneticisi, bu rolün gereğini yerine getirmek için çeşitli faaliyetler yapabilir:

   - Denetim komitesinin iç denetim yönetmeliğini *yılda bir kere* gözden geçirmesini ve onaylamasını talep etmek. *(Bir iç denetim yönetmeliği örneği, IIA'nın internet sitesinde bulunabilir. http://www.theiia.org/ecm/guide-ia.cfm?doc_id=383 ).*

   - Mevcut örgütlenme yapısının iç denetçilere uygun ve yeterli bağımsızlık verdiğinden emin olmak amacıyla, iç denetimin işlevsel ve idarî hiyerarşik ilişkilerini denetim komitesiyle birlikte incelemek ve gözden geçirmek *(Uygulama Önerisi 1110-2 "İç Denetim Yöneticisi - Hiyerarşik İlişkiler),*

   - İç Denetim Yöneticisinin tayini, ücreti, performans değerlendirmesi, görevde kalması ve görevden azledilmesi de dahil olmak üzere İç Denetim Yöneticisi ile ilgili istihdam kararlarının denetim komitesi tarafından incelenmesini öngören bir hükmü denetim komitesi yönetmeliğine koymak,

   - İç denetim hizmetlerinin *dışarıdan alınmasına* ilişkin tekliflerin

denetim komitesi tarafından incelenmesi ve onaylanmasını öngören bir hükmü denetim komitesi yönetmeliğine koymak,

- İç denetim faaliyetinin sorumluluklarını yerine getirmesine engel olan bütçe veya kapsam sınırlamaları bulunmamasını temin etmek amacıyla, personelin ve bütçenin yeterliliği ve iç denetim faaliyetlerinin kapsamı ve sonuçları konularının değerlendirilmesinde denetim komitesine yardımcı olmak,
- Diğer kontrol ve gözlem işlevlerinin (örneğin, risk yönetimi, mevzuata uyum, güvenlik, iş devamlılığı, hukuk, etik, çevre ve dış denetim) *gözetimi ve eşgüdümü* hakkında bilgi vermek,
- Kurumun ve bağlı şirketlerinin faaliyetlerinin kontrolü süreçleriyle ilgili önemli sorunları ve bu süreçlerde iyileştirme ve geliştirme yapmaya yönelik önerileri rapor etmek ve bu konularda bir karar alınana kadar gerekli tüm bilgileri vermek,
- Yıllık *denetim planının* durumu ve sonuçları hakkında ve birim kaynaklarının yeterliliği konusunda üst yönetim ve denetim komitesine bilgi vermek,
- Yönetimin belirlediği risk veya kontrol endişeleri de dahil, risk esaslı uygun bir yöntem uygulayarak esnek bir yıllık denetim planı hazırlamak ve dönemsel güncellemeler yanında, bu planı gözden geçirme ve onaylaması için denetim komitesine sunmak,
- Gerektiğinde yönetimin ve denetim komitesinin talep ettiği özel görev veya projeler de dahil, onaylanmış yıllık denetim planının uygulamaları hakkında rapor sunmak,
- Şirketin iç kontrollerinde önemli görevleri bulunan çalışanların veya yönetimin dahil olduğu suiistimal şüphelerinin denetim komitesine zamanında bildirilmesi konusunda, iç denetim biriminin sorumluluğunu iç denetim yönetmeliğine koymak. Kurum içinde önem arz eden şüpheli suiistimal fiilleri hakkında araştırma yapılmasına yardımcı olmak ve sonuçları yönetime ve denetim komitesine bildirmek,

- Denetim komiteleri, iç denetim faaliyetinin IIA'nın "*Uluslararası İç Denetim Standartları'na" (Standartlar)* uyduğunu ilân edebilmesi için iç denetim faaliyetinin *her beş yılda bir* kalite değerlendirmesine tâbi tutulması gerektiğini bilmelidir. Düzenli kalite değerlendirmeleri, iç denetim faaliyetlerinin bu Standartlara uygun olduğu konusunda denetim komitesine ve yönetime yeterli güvence verecektir,

**Denetim Komitesiyle İletişim:**

6. Yukarıda sayılan faaliyetler saklı kalmak kaydıyla, İç Denetim Yöneticisi ile denetim komitesi arasındaki ilişkinin genel etkinliği, büyük ölçüde, taraflar arasındaki iletişime bağlıdır. Günümüzde denetim komiteleri açık ve samimî iletişim konusunda yüksek bir seviye beklentisi içindedir. İç Denetim Yöneticisinin denetim komitesi tarafından güvenilir bir *danışman* olarak görülebilmesi için, iletişim temel unsurdur. İç denetim, tanımı gereği, denetim faaliyetlerine sistemli ve disiplinli bir yaklaşım getirerek denetim komitesine hedeflerine ulaşması konusunda yardımcı olabilir; fakat uygun bir iletişim kurulamazsa, denetim komitesinin bunu gerçekleştirmesi mümkün değildir. İç Denetim Yöneticisi, aşağıdaki konularda *denetim komitesiyle iletişim kurmayı* düşünmelidir:

   - Denetim komiteleri, hassas konuları tartışmak için İç Denetim Yöneticisi ile düzenli olarak özel toplantılar yapmalıdır,
   - Denetim işinin tanımlanan görevi ve kapsamına göre denetim faaliyetlerinin sonuçları hakkında bir yıllık özet rapor veya değerlendirme sunmak,
   - Denetim komitesine ve yönetime, denetim çalışmalarının sonuçlarını özetleyen dönemsel raporlar sunmak,
   - İç denetim konusunda en son eğilimler ve başarılı uygulamalar hakkında denetim komitesini sürekli bilgilendirmek,
   - Denetim komitesini bilgilendirme ihtiyaçlarının karşılanıp karşılanmadığını dış denetçilerle tartışmak,

- Denetim komitesine verilen bilgilerin tamlığını ve doğruluğunu gözden geçirmek,

- İç ve dış denetçiler arasında etkin ve verimli bir faaliyet eşgüdümü olup olmadığını teyid etmek. İç ve dış denetçilerin işleri arasında tekrarlama olup olmadığını tespit etmek ve bunun sebeplerini açıklamak.

# Uygulama Önerisi 2100-1: İşin Niteliği

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyetinin çalışmalarının niteliğini değerlendirirken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun bu değerlendirmede gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetim çalışması, risk yönetimi, kontrol ve yönetişim süreçlerinin *yeterliliğinin ve etkinliğinin* ve verilen görevlerin yerine getirilmesinde gösterilen performans kalitesinin değerlendirilmesi ve iyileştirilmesi amacına yönelik sistemli ve disiplinli bir yaklaşımı içine alır. Kurumun mevcut risk yönetimi, kontrol ve yönetişim süreçlerinin yeterliliğini değerlendirmenin gayesi; (1) bu süreçlerin niyetlenildiği gibi çalıştığından ve kurumun hedef ve amaçlarına ulaşmasını sağlayacağından emin olmak ve (2) kurumun faaliyetlerinin performans etkinliği ve verimliliği açısından geliştirilmesine yönelik tavsiyelerde bulunmaktır. Üst yönetim, denetim komitesi ve yönetim kurulu, denetlenecek faaliyetler ve denetim işinin kapsamı hakkında genel talimatlar verebilir.

2. Kurum yönetimi, risk yönetimi, kontrol ve yönetişim süreçlerini,

kurumun hedef ve amaçlarının verimli ve ekonomik bir şekilde gerçekleştirilmesi için makul bir güvence sağlayacak şekilde, planladığı ve tasarladığı takdirde, bu risk yönetimi, kontrol ve yönetişim süreçleri uygun ve yeterli sayılır. *Verimli performans,* hedef ve amaçların doğru, zamanlı ve ekonomik şekilde gerçekleştirilmesi anlamına gelir. *Ekonomik performans*, hedef ve amaçların mevcut risk maruziyetine uygun asgarî kaynak kullanımıyla (yani, asgarî maliyetle) gerçekleştirilmesi anlamına gelir. Riskleri azaltmak ve beklenen sapmaları kabul edilebilir bir düzeyde sınırlandırmak için tasarım ve uygulama safhalarında maliyet açısından en etkin önlemler alındığı takdirde, makul güvence sağlanmış kabul edilir. Böylece, *tasarım süreci*, hedef ve amaçların belirlenmesiyle başlar. Bu safhanın ardından; ilgili kavram, bölüm, faaliyet ve insanların, belirlenen hedef ve amaçlara ulaşmak için birlikte çalışabilecek bir şekilde örgütlenmesi veya toplanması aşaması gelir.

3. Yönetim, ilgili süreçleri kurumun hedef ve amaçlarına ulaşılması için makul güvence sağlayacak bir şekilde yönlendirdiği takdirde, bu risk yönetimi, kontrol ve yönetişim süreçleri etkin sayılır. Hedeflere ulaşılması ve planlanan faaliyetlerin yürütülmesine ek olarak, kurum yönetimi, ilgili işlem ve faaliyetler için yetki vererek, performans sonuçlarını izleyerek ve kurumun belirlediği süreçlerin tasarlandığı gibi devam edip etmediğini kontrol ederek *yönlendirme* yapar.

4. Genel olarak, tüm kurumun sürdürülebilir olmasından ve kurumun çalışmaları, davranışları ve performansından dolayı hissedarlara, diğer menfaat sahiplerine, resmî yetkililere ve genel kamuya karşı kurum yönetimi sorumludur. Özel olarak, genel yönetim sürecinin temel ve aslî hedefleri:

    - ilgili, güvenilir ve inanılır finans ve işletme bilgilerine ulaşmak,
    - kurum kaynaklarının etkin ve verimli kullanılmasını sağlamak,

- kurumun varlıklarını korumak,
- kanunlara, mevzuata, etik ve iş standartlarına ve sözleşmelere uyulmasını sağlamak,
- risk maruziyetlerini belirlemek ve tanımlamak ve bunları kontrol altına almak için etkin stratejiler uygulamak,
- faaliyetler veya programlar için hedef ve amaçlar koymak.

5. Kurum yönetimi, hedef ve amaçlara ulaşılması konusunda makul güvence sağlamak için yeterli tedbirlerin alınması ve uygulanmasını planlar, örgütler ve yönlendirir. Yönetim, hedef ve amaçlarını dönemsel olarak gözden geçirir ve süreçlerini iç ve dış koşullardaki değişikliklere göre uyarlar. Yönetim, riskleri anlamasını ve etkin risk stratejileriyle yönetmesini mümkün kılacak etik iklimini de içine alan bir kurum kültürü oluşturur ve uygular.

6. *Kontrol*, yönetimin belirlenen hedef ve amaçlara ulaşma ihtimalini artırmak amacıyla aldığı tedbirlerdir. Kontrol, *önleyici* (istenmeyen olayları caydırıcı), *tespit edici* (meydana gelen istenmeyen olayları tespit edici ve düzeltici) ya da *yönlendirici* (istenen olayları teşvik edici veya bunların olmasını sağlayıcı) nitelikte olabilir. *Kontrol sistemi* kavramı, bir kurumun hedef ve amaçlarına varmak için kullandığı kontrol unsurları ve faaliyetlerinin bütünlüklü bir toplamını kapsar.

7. İç denetçiler, hedef ve amaçlara ulaşılacağı konusunda makul güvencenin bulunup bulunmadığını tespit etmek amacıyla, planlama, örgütleme ve yönlendirmeden oluşan *yönetim sürecinin* tamamını değerlendirir. İç denetçiler, ileriye yönelik bir bakış açısıyla güvence sağlama kabiliyetini etkileyen iç veya dış koşullardaki fiilî veya potansiyel değişiklikler konusunda uyanık olmalıdır. Bu durumlarda, iç denetçiler, performansın düşmesi riskine dikkat etmelidir.

8. Bu iç denetim değerlendirmeleri, bir bütün olarak, genel yönetim sürecinin değerlendirilmesi için gereken veri ve bilgileri verir. Kurum içindeki bütün iş sistemleri, süreçler, operasyonlar, bölümler ve faaliyetler iç denetçilerin bu değerlendirmelerine tâbidir. İç denetim işinin genel kapsamı;
    - yönetimin uyguladığı risk yönetimi sisteminin etkin olduğu,
    - yönetimin iç kontrol sisteminin yeterli, etkin ve verimli olduğu,
    - yönetişim sürecinin gerekli değerleri belirlemek ve korumak, hedefleri tespit etmek, faaliyetleri ve iş performansını izlemek ve sorumluluklarla ilgili tedbirleri tanımlamak açısından etkin olduğu konusunda makul güvence sağlamalıdır.

# Uygulama Önerisi 2100-2: Bilgi Güvenliği

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bir kurumun bilgi güvenliğiyle ilgili yönetişim faaliyetlerini inceler ve değerlendirirken aşağıdaki önerileri dikkate almalıdır. Ancak bu kılavuzun bilgi güvenliğine ilişkin kapsamlı bir güvence veya danışmanlık görevi için gerekli olabilecek her şeyi kapsamak gibi bir amacı yoktur; kılavuz, sadece, denetim komitesi, yönetim kurulu ve üst yönetimle ilgili görevlerini tamamlayıcı nitelikte üst düzey denetçi sorumlulukları hakkında bir tavsiyeler demeti sunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçiler, üst yönetimin, denetim komitesinin ve yönetim kurulunun bilgi güvenliğinin idarî bir sorumluluk olduğu konusunda açık bir anlayışa sahip olup olmadıklarını belirlemelidir. Bu sorumluluk, bilgilerin hangi ortamda saklandığına bakılmaksızın kurum için hayatî öneme sahip *bütün* veri ve bilgileri kapsar.

2. İç Denetim Yöneticisi, iç denetim faaliyetinin bilgi güvenliğini ve bağlantılı risk ve risk maruziyetlerini değerlendirmek için yeterli ve uygun denetim kaynaklarına veya bu kaynaklara erişim olanağına sahip olup olmadığını tespit etmelidir. Bu, kurumun dış kurumlarla ilişkilerinden kaynaklananlar dahil hem iç hem dış risk ve risk maruziyetlerini kapsar.

3. İç denetçiler, bilgi güvenliği *ihlâllerinin* ve kurum açısından

tehlike oluşturabilecek durumların iç denetim faaliyetlerini yürüten kişilere derhal bildirileceği konusunda, denetim komitesinin ve yönetim kurulunun diğer yönetim birimlerinden güvence alıp almadığını da tespit etmelidir.

4. İç denetçiler, gerektiğinde, geçmiş ve gelecekteki muhtemel saldırılara veya saldırı girişimlerine karşı, önleyici, tespit edici ve azaltıcı tedbirlerin etkinliğini değerlendirmelidir. İç denetçiler; denetim komitesinin ve yönetim kurulunun, mevcut tehditler, olaylar, karşılaşılan zayıflıklar ve uygulanan düzeltici tedbirler hakkında yeterince bilgilendirildiğini teyid etmelidir.

5. İç denetçiler, kurumun bilgi güvenliği uygulamalarını dönemsel olarak değerlendirmeli; mevcut koruma ve kontrol iyileştirmeleri ya da yeni koruma ve kontrol uygulamaları (hangisi uygunsa) tavsiye etmelidir. Bu değerlendirmeden sonra, denetim komitesi ve yönetim kuruluna, bir *güvence raporu* sunulmalıdır. Bu değerlendirmeler, bağımsız ve ayrı görevler olarak ya da onaylanmış denetim planının bir parçası olan başka denetim veya görevlerle bütünlük arz edecek şekilde yapılabilir.

# Uygulama Önerisi 2100-3: İç Denetimin Risk Yönetim Sürecindeki Rolü

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İligili Standart

**2100 İşin Niteliği**

İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetimin tanımı şöyledir: "... risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek ve iyileştirmek amacına yönelik disiplinli bir yaklaşımdır." İç denetçiler, iç denetimi Standartlara uygun bir şekilde gerçekleştirmek için, kurumun risk yönetimi sürecinde önemli ve temel bir rol oynar. Bu uygulama önerisi, iç denetçilere, bir kurumun risk yönetim sürecindeki rollerinin tespit edilmesi için ve Standartlara uymaları için bir kılavuz görevini yapmaktadır. Bu uygulama önerisinde ele alınan konuların dışında başka konuların da ele alınması gerekebilir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Risk yönetimi, kurum yönetiminin temel sorumluluklarından biridir. İş hedeflerine ulaşabilmek için, yönetimin, kurum içinde sağlam risk yönetimi süreçlerinin bulunmasını ve kullanılmasını sağlaması gerekir. Denetim komitesi ve yönetim kurulu, uygun risk yönetimi süreçlerinin bulunup bulunmadığını ve bu süreçlerin yeterli ve etkin olup olmadığını tespit etmek konusunda denetleyici bir rol oynar. İç denetçiler, yönetimin uyguladığı risk süreçlerinin yeterliliği ve etkinliğini inceleyerek, değerlendirerek, rapor ederek ve bu konuda iyileştirici önlemler önererek hem yönetime hem de denetim komitesine yardımcı olmalıdır. Kurumun risk yönetimi

ve kontrol süreçlerinden kurum yönetimi, denetim komitesi ve yönetim kurulu *sorumludur*. Ancak, *danışmanlık* rolünü üstlenen iç denetçiler de, bu risklerin tanımlanması, değerlendirilmesi, risk yönetimi yöntemlerinin uygulanması ve bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında yardımcı olabilir.

2. Kurumun risk yönetimi süreçleri hakkında değerlendirme ve incelemeler yapmak ve raporlar yazmak, normal olarak, *yüksek denetim önceliğine* sahip bir görevdir. Yönetimin uyguladığı risk süreçlerini değerlendirme görevi; denetçilerin denetim çalışmalarını planlamak için risk analizlerini kullanması gereğinden *farklıdır*. Bununla birlikte, üst yönetimin, denetim komitesi ve yönetim kurulunun endişe duyduğu konuların tespiti de dahil, kapsamlı bir risk yönetim sürecinden elde edilen bilgiler, iç denetçilerin denetim faaliyetlerini planlamasına yardımcı olabilir.

3. İç Denetim Yöneticisi, kurumun risk yönetimi sürecinde, üst yönetimin, yönetim kurulunun ve denetim komitesinin iç denetim faaliyetinden *beklentilerini* öğrenmeli ve kavramalıdır. Bu bilgiler, iç denetim faaliyetinin ve denetim kurulunun *yönetmeliklerine* de yazılmalıdır.

4. Kurumun risk yönetimi sürecinde rol oynayan bütün kişi ve gruplar arasında faaliyetlerin ve sorumlulukların *eşgüdümü* gerekir. Bu sorumluluk ve faaliyetler, kurumun stratejik planlarında, denetim komitesi ve yönetim kurulunun politikalarında, yönetmeliklerde, genelgelerde, faaliyet prosedürlerinde ve başka idarî belgelerde de açıkça ifade edilmelidir. Kayıtlara geçirilmesi gereken faaliyet ve sorumluluklara örnek olarak şunları gösterebiliriz:

   - Stratejik yönün tayini görevi denetim komitesine, yönetim kuruluna veya bir başka komiteye verilebilir,
   - Risklerin sorumluluğu üst yönetim kademelerine verilebilir,

- Ek risklerin kabulü sorumluluğu icra kurulu düzeyinde olabilir,
- Kesintisiz risk tespit, tanımlama, değerlendirme, azaltma ve izleme faaliyetleri, faaliyetler düzeyinde yürütülebilir,
- Dönemsel değerlendirme ve güvence sağlama görevleri, iç denetim faaliyetine verilmelidir.

5. İç denetçilerin işlerinin olağan akışı içinde önemli risk ve risk maruziyetlerini tespit etmeleri ve değerlendirmeleri beklenir.

6. İç denetim faaliyetinin bir kurumun risk yönetim sürecinde oynadığı rol, zamanla değişebilir ve
   - hiç rolü olmamaktan,
   - iç denetim planının bir parçası olarak risk yönetimi sürecini denetlemeye,
   - izleme komitelerine, izleme faaliyetlerine ve durum raporlama çalışmalarına katılmak gibi, risk yönetim sürecinde faal ve kesintisiz destek ve katılıma,
   - risk yönetim sürecinin yönetimi ve eşgüdümünekadar uzanan bir aralıkta olabilir.

7. Son olarak, iç denetimin risk yönetimi sürecindeki rolünü tespit etmek, üst yönetimin ve denetim komitesinin görevidir. Yönetimin iç denetimin rolü konusundaki görüşü de, muhtemelen, kurumsal kültür, iç denetim personelinin kabiliyeti, ülkenin mahallî koşulları ve gelenekleri gibi etkenler dikkate alınarak belirlenir.

8. Bu konuda, aşağıda sayılan uygulama önerilerinde ek öneri ve tavsiyeler bulunabilir:
   - PA 2100-4 Risk Yönetim Süreci Bulunmayan Kurumlarda İç Denetimin Rolü

- PA 1130.A1-2 İç Denetimin Diğer (Denetim-Dışı) Görev ve Fonksiyonlarla İlgili Sorumlulukları
- PA 2110-1 Risk Yönetim Süreçlerinin Yeterliliğinin Değerlendirilmesi
- PA 2010-2 Denetim Planıyla Risk ve Risk Maruziyeti Arasında Bağlantı Kurmak

# Uygulama Önerisi 2100-4: Risk Yönetim Süreci Bulunmayan Kurumlarda İç Denetimin Rolü

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**

İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetimin tanımı şöyledir: "... risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek ve iyileştirmek amacına yönelik disiplinli bir yaklaşımdır." İç denetçiler, iç denetimi Standartlara uygun bir şekilde gerçekleştirmek için, kurumun risk yönetimi sürecinde önemli ve temel bir rol oynar. Ancak bazı kurumlarda yerleşik bir risk yönetimi süreci bulunmayabilir. Bu uygulama önerisi, iç denetçilere, yerleşik bir risk yönetimi süreci bulunmayan bir kurumdaki rollerinin tespit edilmesi için bir kılavuz görevini yapmaktadır. Bu uygulama önerisinde ele alınan konuların dışında başka konuların da ele alınması gerekebilir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Risk yönetimi, yönetimin temel sorumluluklarından biridir. İş hedeflerine ulaşabilmek için, yönetimin, kurum içinde sağlam risk yönetimi süreçlerinin bulunmasını ve kullanılmasını sağlaması gerekir. Denetim komitesi ve yönetim kurulu, uygun risk yönetimi süreçlerinin bulunup bulunmadığını ve bu süreçlerin yeterli ve etkin olup olmadığını tespit etmek konusunda *denetleyici* bir rol oynar. İç denetçiler, yönetimin uyguladığı risk süreçlerinin yeterliliği ve etkinliğini inceleyerek, değerlendirerek, rapor ederek ve bu konuda iyileştirici önlemler önererek hem yönetime hem de

denetim komitesine yardımcı olmalıdır. Kurumun *risk yönetimi ve kontrol süreçlerinden yönetim, denetim komitesi ve yönetim kurulu sorumludur.* Ancak, *danışmanlık* rolünü üstlenen iç denetçiler de, bu risklerin tanımlanması, değerlendirilmesi ve risk yönetimi metodolojilerinin uygulanması ve bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında yardımcı olabilir.

2. Kurumun risk yönetimi süreçleri hakkında değerlendirme ve incelemeler yapmak ve raporlar yazmak, normal olarak, *yüksek denetim önceliğine* sahip bir görevdir. Yönetimin uyguladığı risk süreçlerini değerlendirme görevi, denetçilerin denetim çalışmalarını planlamak için risk analizlerini kullanması gereğinden farklıdır. Bununla birlikte, yönetimin, denetim komitesi ve yönetim kurulunun kaygı duyduğu konuların tespiti de dahil, kapsamlı bir risk yönetim sürecinden elde edilen bilgiler, iç denetçilerin denetim faaliyetlerini planlamasına yardımcı olabilir.

3. İç Denetim Yöneticisi, kurumun risk yönetimi sürecinde, üst yönetim, denetim komitesi ve yönetim kurulunun iç denetim faaliyetinden *beklentilerini* öğrenmeli ve kavramalıdır. Bu bilgiler, iç denetim faaliyetinin ve denetim kurulunun yönetmeliklerine de yazılmalıdır.

4. Bir kurum bir risk yönetimi süreci oluşturmamışsa, iç denetçi, böyle bir sürecin oluşturulmasına ilişkin tavsiyeleriyle birlikte bu konuyu yönetimin dikkatine sunmalıdır. İç denetçi, denetim faaliyetinin risk yönetimi sürecindeki rolü konusunda yönetimin, denetim komitesi, yönetim ve yönetim kurulunın görüş ve talimatlarını almalıdır. İç denetim faaliyetinin ve denetim kurulunun yönetmelikleri, her birinin risk yönetimi sürecindeki rolünü açıklamalı ve göstermelidir.

5. Talep hâlinde, iç denetçiler, kurumun risk yönetim sürecinin ilk

kuruluşuna yardımcı olacak faal bir rol oynayabilir. Daha faal bir rol ise, geleneksel güvence faaliyetlerine ek olarak, temel süreçlerin geliştirilmesinde *danışmanlık* görevinin üstlenilmesini kapsar. Bu yardımın kapsamı iç denetçilerin normal güvence ve danışmanlık faaliyetlerinin kapsamını aştığı takdirde, iç denetçilerin bağımsızlığı bozulabilir. Bu durumlarda, iç denetçiler, *Standartların* açıklama ve raporlamayla ilgili gereklerine uymalıdır. Bu konuda, *İç Denetimin Diğer (Denetim-Dışı) Görev ve Fonksiyonlarla İlgili Sorumluluğu başlıklı Uygulama Önerisi 1130.A1-2'*de ek bilgiler bulunabilir.

6. Bir risk yönetim sürecinin geliştirilmesi ve yönetiminde faal bir rol oynamak "risklerin sorumluluğunu üstlenmek" rolüyle aynı değildir. "Risklerin sorumluluğunu üstlenmek" rolünden kaçınmak için, iç denetçiler, mevcut risklerin tespit edilmesi, tanımlanması, azaltılması, izlenmesi ve "sorumluluğun üstlenilmesi" konularındaki rolleri konusunda yönetimden teyit istemelidir.

7. Özet olarak, iç denetçiler, risk yönetimi süreçlerini oluşturabilir veya kolaylaştırabilir; fakat tespit edilen ve tanımlanan risklerin yönetimini "*üstlenmemeli*" veya bu konuda sorumluluk almamalıdır.

# Uygulama Önerisi 2100-5: Mevzuata Uyum Programlarının Değerlendirilmesinde Hukukî Mülâhazalar

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler bir kurumun mevzuata uyum programlarını değerlendirirken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun, mevzuata uyumla ilgili kapsamlı bir güvence veya danışmanlık görevi için gerekli olabilecek bütün prosedürleri temsil etmek veya kapsamak gibi bir amacı yoktur.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

**Dikkat:** *İç denetçilerin hukukî sorunlarla ilgili tüm konularda hukuk danışmanına başvurması tavsiye edilir, çünkü farklı ülkelerdeki kanunlar arasında çok büyük farklar olabilir. Bu uygulama önerisindeki öneriler esas olarak Amerika Birleşik Devletleri hukuk sistemine dayanmaktadır.*

1. Mevzuata uyum programları, kurumlara, personelin kastî olmayan kanun ihlâllerini önlemek, yasa dışı faaliyet ve işlemleri tespit etmek ve personelin kastî kanun ihlâllerini caydırmak konusunda yardımcı olur. Bu mevzuata uyum programları, sigorta tazminat taleplerinin kanıtlanmasında, yönetici ve memurların sorumluluğunun tespit edilmesinde, kurumsal kimliğin yaratılması

veya geliştirilmesinde ve kasıt sebebiyle artırılmış cezaî tazminatların uygunluğuna karar verilmesinde de yardımcı olabilir. İç denetçiler, bir kurumun mevzuata uyum programlarını, etkin ve verimli programlar için aşağıda önerilen sistem ışığında değerlendirmelidir.

2. Kurum, hem kendi çalışanları hem de temsilci ve acentelerinin uyması gereken ve suç teşkil eden eylemleri azaltabilecek nitelikte olan mevzuata uyum standartları ve usulleri tespit etmeli ve uygulamalıdır.

   - Kurum, yasaklanmış işlem ve faaliyetleri açıkça gösteren ve tanımlayan bir yazılı iş davranış kuralları politikası belirlemelidir. Bu politika, bütün çalışanların kolaylıkla anlayabileceği bir dilde kaleme alınmalı ve hukuk dilini kullanmaktan kaçınmalıdır.
   - İyi hazırlanmış bir politika, çalışanlara ilgili tüm konularda kılavuzluk eder. Kontrol listeleri, soru yanıt bölümü ve daha fazla bilgi için ek kaynaklara referanslar, politikanın kullanıcılar için uygun ve kullanışlı olmasına yardımcı olur.
   - Kurum, mevzuata uyum programlarının uygulanmasından sorumlu olan yönetim kurulu üyeleri, üst seviye memurlar, üst düzey mevzuata uyum görevlisi ve birim personelini tanımlayan bir örgütlenme şeması yapmalıdır.
   - Çalışanların çok hukukî ve "tek taraflı" gördüğü iş davranış kuralları politikaları, çalışanların etik veya yasalara aykırı davranışlara girme riskini artırır. Açık, basit ve âdil görülen iş davranış kuralları politikaları ise, çalışanların bu tür işlem ve davranışlara girme riskini azaltır.
   - Etiğe veya yasalara açıkça aykırı olan davranışlara da mali teşvikler getiren ödüllendirme sistemleri uygulayan şirketlerde, mevzuata uyum sorunları doğması beklenebilir.

- Uluslararası faaliyetleri olan şirketlerin, sadece belirli seçilmiş coğrafî bölgeler için değil, evrensel anlamda hazırlanmış bir mevzuata uyum programı yapması gerekir. Bu programlar, ilgili mahallî koşulları, kanunları ve düzenlemeleri yansıtmalıdır.

3. Standartlara ve prosedürlere uyumu denetleme konusundaki genel sorumluluğun, kurumun üst düzey personelinden seçilmiş belirli kişi veya kişilere verilmesi gerekir.
   - Kurumun üst düzey personeli terimi, *kurum üzerinde önemli kontrole sahip* olan veya kurum içinde *politika belirleme* ve *yapma* konusunda *önemli rol oynayan* kişiler anlamına gelir.
   - Kurumun üst düzey personeli terimi şu kişileri kapsar: Yönetim kurulu üyeleri; icraî görevleri olan yöneticiler; satış, idare veya finans gibi, kurumun önemli bir iş veya fonksiyon biriminden sorumlu olan kişiler ve kurumda önemli bir sermaye payına sahip kişiler.
   - Programın gerçekten etkili olabilmesi için, icraî anlamda kurumun en üst seviye yöneticisinin (Yönetim Kurulu Başkanı, Genel Müdür, İcra Kurulu Başkanı ve diğer üst düzey yöneticilerin de programa katılması ve katkıda bulunması gerekir.
   - Bazı kurumlarda, *mevzuata uyumla* ilgili aslî sorumlulukların şirketin genel hukuk danışmanına verilmesi, çalışanların, yönetimin programa çok bağlı olmadığını ve programın bir bütün olarak firma için değil, sadece hukuk birimi için önemli olduğunu düşünmelerine yol açabilir. Başka kurumlarda ise, bunun tam tersi de doğru olabilir.
   - Birden fazla iş biriminden oluşan büyük bir şirkette, mevzuata uyum sorumluluklarının her birimdeki üst düzey personele verilmesi gerekir.
   - Şirketin mevzuata uyum birimi kurması ve mevzuata uyum biriminin diğer personelini seçmesi yeterli değildir. Şirket,

seçilen bu personele uygun yetkilerin verilmesini ve bu personelin görevlerini yapabilmek için ihtiyaç duydukları kaynaklarla donatılmasını da sağlamalıdır. Mevzuata uyum personeli, üst yönetime ulaşma imkânına sahip olmalıdır. Mevzuata uyum biriminin yöneticisi, doğrudan CEO'ya bağlı olmalıdır.

4. Kurumun, yasa dışı faaliyet ve işlemlere girme eğilimi olduğunu bildiği ya da bilmesi gerektiği kişilere önemli takdir ve karar yetkileri vermemeye dikkat etmelidir.

   Şirketler, her düzey ve kademede iş için müracaat eden kişilerin geçmişte suç işleyip işlemediğini ve yasa dışı bir hareketi olup olmadığını, özellikle de şirketin faaliyet gösterdiği sektör içinde bir yasa dışı hareketi olup olmadığını araştırmalıdır.

   İş için yapılan müracaatlarda, kişinin sabıka kaydı da araştırılmalıdır. Meslek sahibi kişilerin geçmişte herhangi bir disiplin suçu işleyip işlemedikleri, ilgili ruhsatlandırma komitelerinden araştırılmalıdır.

   Şirketin, çalışanların ve iş için müracaat edenlerin özel hayatın gizliliğine ilişkin cari kanunlardan doğan haklarına tecavüz etmemesine dikkat edilmelidir. Pek çok ülkede, bir şirketin çalışanlarının geçmişi hakkında araştırmaları sırasında alabileceği bilgileri sınırlandıran kanunlar vardır.

5. Kurum, belirlediği standart ve prosedürleri bütün çalışanlarına, temsilcilerine ve acentelerine etkin ve eksiksiz duyurmak amacına yönelik tedbirler almalıdır; bu amaçla, söz konusu kişilerin eğitim programlarına katılmasını isteyebilir ya da gerekenleri kolay anlaşılır bir tarzda açıklayan yayınlar çıkartabilir.

   - Bir mevzuata uyum programının etkinliği, bu programın çalışanlara duyurulduğu ve bildirildiği yollara bağlıdır. Genel olarak, etkileşimli bir bilgilendirme formatı bir konferans veya seminerden daha çok işe yarar. Şahsen duyurulan

programlar, sadece ve tamamen video veya oyun formatlarında duyurulan programlardan daha iyi iletilir. Dönemsel olarak tekrarlanan programlar bir sefer sunulanlardan daha etkili iletilir.

- En iyi programlar, çalışanların yeni tekniklerin pratiğini yapmasına ve yeni bilgileri kullanmasına imkân veren personel eğitimlerini de içerir. Bu tür faaliyetler, özellikle yönetim eğitiminde gereklidir, fakat bütün düzeyde çalışanların eğitimi açısından da etkilidir.
- Bir kurumun iş davranış kuralları politikasında ve personel el kitabında kullandığı dil, kolay anlaşılır olmalıdır. Politikanın ve personel el kitabının temel eğitim açısından eksiği olan çalışanlara duyurulması için alternatif yöntemler bulunmalı ve uygulanmalıdır.
- Haber bültenleri, posterler, e-posta, soru formları ve sunumlar gibi çeşitli araç ve ortamlar aracılığıyla, personele, mevzuata uyum hakkında uyarılar, açıklamalar ve notlar iletilmelidir.
- Kurumlar, bu programı farklı personel gruplarına farklı şekillerde ve ortamlarda sunmalı ve her personel grubu veya birim için önem taşıyan konularla ilgili tüm bilgilerin o grup veya birime özellikle verilmesini hedeflemelidir. Bilgilerin ilgili grubun işle ilgili ihtiyaçlarına uyarlanması gerekir. Örneğin, çevre mevzuatına uyumla ilgili bilgilerin, bu kanunları ve yönetmelikleri ihlâl etme veya bu kanunların ve yönetmeliklerin ihlâlini tespit etme olasılığı daha fazla olan imalat veya emlak yönetimi gibi birimlere iletilmesi ve verilmesi gerekir. Öte yandan, bu eğitimin bu konuda hiçbir sorumluluğu bulunmayan bir birime verilmesi zararlı bile olabilir, çünkü çalışanlarda ilgisizliğe yol açabilir ya da programın iyi oluşturulmadığı inancının doğmasına neden olabilir.

- *Yeni işe alınanlar*, intibak (oryantasyon) eğitiminin bir parçası olarak mevzuata uyum konusunda da temel eğitime tâbi tutulmalıdır. Daha sonra, bu kişiler de kendi birimleri içinde devam eden mevzuata uyum çaba ve çalışmalarına dahil edilebilir.
- Kurumun *acentelerinin* de, özellikle onlara yönelik olarak hazırlanmış bir sunum toplantısına katılmaları istenmelidir. Kurumun temel değerlerini acentelerine de bildirmesi ve acentelerin şirkete atfedilebilecek olan eylem ve davranışlarının mevzuata uyum programına uygun olarak izleneceğini açıklaması önemlidir. Kurum, kurumun mevzuata uyum standartlarına uymayan acenteler ile iş ilişkisini kesmekte kararlı olmalıdır.
- Kurum, çalışanlarından, şirketin iş davranış kuralları politikasını okuduklarını, anladıklarını ve bu politikanın gereklerine uyduklarını dönemsel olarak teyid ve tasdik etmelerini istemelidir. Bu bilgiler üst yönetime ve yönetim kuruluna *yıllık dönemler hâlinde* sunulmalıdır.
- İş etiğiyle ilgili bütün belgeler (iş davranış kuralları, insan kaynakları politikaları/kitapçıkları, vb.) *bütün* çalışanların kullanımına açık olmalıdır. Kurumun intraneti gibi kesintisiz erişim olanağı sağlayan araçların kullanılması da tavsiye edilir.

6. Kurum, çalışanlarının, temsilci ve acentelerinin cezayı gerektiren eylemlerini tespit amacıyla tasarlanmış makul izleme ve denetim sistemleri kullanarak ve söz konusu kişilerin kurum içinden başka kişilerin suç eylemlerini ceza korkusu olmadan ihbar edebileceği bir *ihbar* sistemi kurarak ve bunu herkese duyurarak, standartlarına uyumu sağlamak amacıyla *makul tedbirler* almalıdır.
    - Kurum, iç denetim planına, şirketin büyüklüğüne ve denetim görevinin güçlüğüne göre uygun miktarda kaynak tahsis etmelidir. Denetim planı, kurumun faaliyet sahalarının her

birindeki faaliyetleri üzerinde odaklanmalı ve yoğunlaşmalıdır.

- *Denetim planı*, yazılı malzemelerin etkin ve verimli olup olmadığını, çalışanların duyuru ve bildirimleri alıp almadığını, tespit edilen ihlâller için gereken işlemlerin yapılıp yapılmadığını, disiplinin âdil ve tarafsız uygulanıp uygulanmadığını, ihbarcılara karşı misilleme yapılıp yapılmadığını ve mevzuata uyum biriminin sorumluluklarını yerine getirip getirmediğini tespit etmek amacına yönelik incelemeler de dahil, kurumun mevzuata uyum programı ve prosedürlerinin incelenmesi ve gözden geçirilmesini de içermelidir. Denetçiler, mevzuata uyum programının geliştirilip geliştirilemeyeceğini tespit etmek amacıyla programı incelemeli ve bu konuda çalışanların görüş ve önerilerini almalıdır.
- Her programın, çalışanların etiğe aykırı, yasa dışı ya da şirketin iş davranış kurallarına aykırı olduğuna inandıkları işlem ve faaliyetleri bildirebileceği bir "*telefon hattı*" ya da başka bir ihbar sistemi mevcut olmalıdır. Çalışanlar, bu tür davranışları misilleme veya ceza korkusu olmadan ihbar etmekte serbest olmalıdır.
- Telefon hattını yöneten bir avukat, avukat-müvekkil ve iş-ürün gizliliği imtiyazlarını daha iyi koruyabilir. Ancak yapılan bir araştırmada, çalışanların hukuk birimi tarafından veya şirket dışından bir birim tarafından cevaplanan telefon hatlarına daha az güven duyduğu sonucuna varılmıştır. Aynı araştırmada, çalışanların yazılı raporlara veya dışarıdan bir ombudsmana duyduğu güvenin daha da az olduğu ve misilleme yapılmayacağı güvencesini veren bir politikayla desteklenen ve şirket içinden bir temsilci tarafından yanıtlanan telefon hatlarına duyulan güvenin daha çok olduğu sonucuna da varılmıştır.
- *Ombudsman*'ın doğrudan doğruya mevzuata uyum müdürüne veya yönetim kuruluna bağlı olması, ihbarcıların isimlerini

gizli tutabilmesi, ihbarcılara yol göstermesi, misilleme yapılmamasını sağlamak amacıyla izleme ve takip görevlerini üstlenmesi durumunda şirket içinden bir ombudsmanın kullanılması daha etkili olmaktadır. Ayrıca, bazı ülkelerde, ombudsmanın ihbarcılardan aldığı gizli bilgi ve ihbarları açıklamama yetkisiyle donatıldığı sınırlı bir *ombudsman gizliliği* kabul edilmiş ve benimsenmiştir.

- Etik veya yasalara aykırı işlem ve faaliyetleri açığa çıkartmanın etkili bir aracı da, *iş etiği soru formları*dır. Kurumun her personeline, personelin rüşvet, yasa dışı ödemeler veya başka suç eylemlerinden haberdar olup olmadığı sorusunu yönelten bir soru formu verilmelidir. Gizliliği korumak için, bu soru formu kurumun *hukuk danışmanı* tarafından gönderilmeli; soru formunun *gizlilik koruması* altında olduğunu belirten bir açıklama içermeli; personelin soru formunu doldurmasını, imzalamasını ve iade etmesini ve kopyasını almamasını istemeli ve kurumun bu yolla aldığı ve topladığı bilgileri resmî makamlara veya ilgili davalarda mahkemelere açıklama hakkını saklı tuttuğunu belirten bir açıklama içermelidir. Soru formu dışarıdan kişilere açıklandığı ve verildiği takdirde, gizliliğin kaybolacağı açıktır.

7. *Standartlar*, bir suç eylemini tespit edememekten dolayı sorumlu tutulan kişilere uygulanacak disiplin kuralları da dahil, uygun disiplin mekanizmalarıyla *istikrarlı ve tutarlı* bir şekilde uygulanmalıdır. Bir suçtan sorumlu tutulan kişilerin yeterli ve uygun disiplin cezalarıyla cezalandırılması, standartların uygulanmasının gerekli bir unsurudur; ancak uygun ve yeterli disiplin cezası her durumun kendine özgü şartlarına göre tespit edilecektir.

   - *Mevzuata uyum programı,* kurumun iş davranış kurallarını ihlâl edenlerin suça bağlı ve orantılı olarak uyarı, ücret kaybı, geçici uzaklaştırma, nakil veya iş akdinin feshi gibi cezalarla

cezalandırıldığı bir *disiplin sistemini* içermelidir. Fakat bir çalışanın yasa dışı bir eylemde bulunması hâlinde, kurumun "yasa dışı faaliyet ve işlemlere girme eğilimi olduğunu bildiği ya da bilmesi gerektiği kişilere önemli takdir ve karar yetkileri vermeme" yükümlülüğünün bir parçası olarak o çalışanı işten çıkartması ve onun hizmet akdini feshetmesi gerekebilir.

- *Program* kapsamında uygulanan disiplinin âdil olması gerekir. Özellikle kurumun üst yönetiminin veya önemli elemanlarının faaliyetleri bağlamında etik veya yasalara aykırı işlem ve eylemler cezalandırılmazsa, programın başarı şansı çok az olur. Bu tür kişilerin haksız eylemlerinin cezalandırılmaması, diğer çalışan ve işçilerde de bu tür davranışları özendirir.
- Çalışanların hizmet akdinin feshedilmesi veya başka disiplin cezaları; ihbarlara ilişkin kanunlarla, zorla çalıştırmama doktrininin istisnalarıyla, çalışanların hizmet sözleşmeleriyle veya sendikalarla imzalanan sözleşmelerle ve ayrımcılık ve haksız işten çıkartmaya ilişkin işveren sorumluluklarıyla ve işverenin kötü niyetli eylemlerine ilişkin kanunlarla/doktrinlerle sınırlandırılabilir.
- Program, suiistimal ve yasa dışı eylemleri bilen veya bilmesi gereken ve bunları rapor etmeyen müdürlere ve başka sorumlu kişilere uygulanacak disiplin cezalarını da düzenlemelidir. Programın bunu yapmaması, bir mahkemenin programın etkin ve verimli olmadığı sonucuna varmasına yol açabilir; bu durumda, programın cezalandırma üzerinde faydalı bir etkisi olmayacaktır.
- Kurumlar, personelin disipliniyle ilgili kayıtlarda titiz ve dikkatli davranmalıdır. Kurum, disiplin olayları hakkında gerekli bilgileri toplamak için elinden gelen her türlü çabayı gösterdiğini ve mevcut bilgiler esasında uygun tedbirleri aldığını ve gereken işlemleri yaptığını kanıtlayabilmelidir.

8. Bir suç eylemi tespit edildiğinde, kurum, bu suç eylemine uygun cevabı vermek ve gelecekte benzer suçları önlemek için gereken bütün makul önlemleri almalı ve bu bağlamda, kanunun ihlâllerini önlemek ve tespit etmek amacıyla programda gereken değişiklik ve uyarlamaları yapmalıdır.

    - Kurum, mevzuata uyum programıyla tespit edilen her suç eylemine uygun tepkiyi göstermeli ve uygun cevabı vermelidir. Uygun tepki ve cevaplar; yasa dışı eyleme katılanlarla ilgili disiplin cezalarını da kapsar.
    - Bazı durumlarda uygun cevap, ihlâlin resmî makam ve yetkililere bildirilmesini, resmî makamların yaptığı soruşturmalara katılmayı ve ihlâlle ilgili sorumluluğun kabul edilmesini de gerektirebilir. Etkin ve verimli bir mevzuata uyum programının varlığı gibi, bu tür uygun cevapları vermek de bir mahkemenin kuruma vereceği para cezası tutarını indirmesini sağlayabilir.
    - Ciddî bir ihlâlin önlenememesi veya tespit edilememesi mevzuata uyum programında büyük bir değişiklik gerektiğini gösterebilir. En azından, bir ihlâl tespit edildiğinde, mevzuata uyum personelinin herhangi bir değişikliğe gerek olup olmadığını anlamak amacıyla programı incelemesi gerekir.
    - Bir ihlâlin ışığında gerekli olabilecek değişikliklerden biri de, *mevzuata uyum personelinin* değiştirilmesi veya görev tanımlarının birbirleri arasında değiştirilmesi olabilir. Kurumun, kendi denetim ve kontrol alanları içinde yapılan ihlâlleri ve yasa dışı eylemleri önlemekte veya tespit etmekte başarısız olan bir müdürü, özellikle ihlâlin, o müdürün tespit etmesi gereken bir ihlâl olduğu durumlarda, değiştirmesi veya ona disiplin cezası uygulaması gerekebilir.

# Uygulama Önerisi 2100-6: E-Ticaret Faaliyetlerinin Kontrol ve Denetimi

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**

İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *Hem işten işe uygulamalar hem de işten tüketiciye uygulamalarda e-ticaret hızla büyümeye ve gelişmeye devam etmektedir. Bir e-ticaret stratejisinin başarıyla geliştirilmesi ve uygulanmasında, etkin ve amaca uygun kontrol ve süreçler hayatî öneme sahiptir. Böylece, pek çok şirkette, etkin e-ticaret değerlendirme çabaları yıllık denetim planının aslî bir unsuru olabilir. Bu Uygulama Önerisi, kontrol ve denetim konularında bir genel değerlendirme sunmaktadır. Meslek sahiplerinin başvurabileceği ek kaynaklar şunlardır: IIA'nın Sistem Güvence ve Kontrolü (SAC)[1] ürünü ve diğer teknoloji raporları ve ISACA'nın yayınları. Her iki yayın da elektronik sistem ve modellerin değerlendirilmesi için ilke ve kıstaslar önermektedir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Elektronik ticaret (e-ticaret), genel olarak, "ticarî faaliyet ve işlerin internet üzerinden yürütülmesi" şeklinde tanımlanır. Bu ticarî faaliyetler; '*işten işe*' (B2B[2]), '*işten tüketiciye*' (B2C[3]) ve '*işten personele*' (B2E[4]) şeklinde olabilir. E-ticaret hızla gelişmiş ve büyümüştür ve önümüzdeki yıllarda daha da hızlı büyümesi beklenmektedir. IIA Araştırma Vakfı'nın son yayını olan

[1] SAC: Systems Assurance and Control
[2] B2B: Business-to-Business
[3] B2C: Business-to-Consumer
[4] B2E: Business-to-Employee

"*Sistem Güvence ve Kontrolü*" (SAC) ve ayrıca, web-temelli www.ITAudit.org'un kazandığı başarı ve çeşitli IIA e-posta haber bültenleri, teknolojinin sadece e-ticaret stratejilerini desteklemekle kalmadığını, aynı zamanda onun tamamlayıcı bir parçası da olduğunu teyit etmektedir. Web-temelli ve diğer teknolojilerdeki değişikliklerin toplum, yönetişim, ekonomi, rekabet, pazarlar, örgütsel yapı ve ulusal savunma üzerinde çok önemli bir etkisi vardır. E-ticaretin hızlı büyümesinin ve bu teknoloji değişikliklerinin, denetim planlarının hazırlanması ve uygulanmasında iç denetçilerin dikkate alması gereken önemli kontrol ve yönetim sorunları yarattığı açıktır.

**Bir E-Ticaret Görevinin Anlaşılması ve Planlanması:**

2. Teknolojideki devamlı ve kesintisiz değişiklikler, iç denetim mesleği için hem büyük fırsatlar hem de büyük riskler yaratmaktadır. Sistemler ve süreçler hakkında bir güvence vermeden önce, bir iç denetçi, işteki ve bilgi sistemlerindeki değişiklikleri, bunlarla ilgili ve bağlantılı riskleri ve ayrıca stratejilerin kurumun tasarımına ve pazar koşullarına uygun olup olmadığını anlamalıdır. İç denetçi, yönetimin stratejik planlama ve risk değerlendirme süreçlerini ve *aşağıdaki sorulara ilişkin kararlarını* incelemelidir:
   - Hangi riskler ciddî ve önemlidir?
   - Hangi riskler sigortalanabilir?
   - Mevcut kontrollerin hangileri riskleri azaltabilir?
   - Hangi ilâve dengeleyici kontroller gereklidir?
   - Ne tür bir gözleme ihtiyaç vardır?
3. E-ticaret faaliyetlerinin denetiminin temel unsurları şunlardır:
   - Üst yönetimin belirlediği tarz da dahil iç kontrol yapısını değerlendirmek,
   - Hedef ve amaçlara ulaşılabileceği konusunda makul güvence sağlamak,
   - Risklerin kabul edilebilir olup olmadığını tespit etmek,
   - Bilgi akışını anlamak,

- Arayüz sorunlarını (donanımdan donanıma, yazılımdan yazılıma ve donanımdan yazılıma gibi) incelemek,
- İş devamlılığı ve felâket sonrası toparlanma planlarını değerlendirmek.

4. İç denetim yöneticisinin bir e-ticaret işinin yürütülmesinde ilgilenmesi gereken konular, iç denetim faaliyetinin yetkinliği ve kapasitesiyle ilgilidir. İç denetim faaliyetini *sınırlandırabilecek muhtemel etkenler* arasında şunlar sayılabilir:
   - İç denetim birimi yeterli *becerilere* sahip midir? Sahip değilse, bu beceriler edinilebilir mi?
   - Eğitim veya başka kaynaklara ihtiyaç var mıdır?
   - İşgücü/kadro düzeyi kısa ve uzun vadede yeterli midir?
   - Beklenen denetim planı verilebilir mi?

5. İç denetçinin risk değerlendirmesinde *sorması gereken sorular:* IIA'nın SAC yayını, denetim planlamasında ve risk değerlendirmesinde iç denetçiye faydalı olabilir. Bu yayın, bir görev üstlenen ve risk değerlendirmesi yapan bir iç denetçinin ilgilenmesi ve dikkate alması gereken e-ticaret konularının bir listesini vermekte ve içermektedir. İç denetçinin sorması gereken sorular şunlardır:
   - E-ticaret projesi veya programı için bir iş planı var mı?
   - Bu plan, e-ticaret sisteminin planlama, tasarım ve uygulamasının kurumun stratejileriyle bütünleştirilmesi konusunu da kapsıyor mu?
   - Sistemin performansı, güvenliği, güvenilirliği ve kullanıma hazırlığı üzerindeki etkileri neler olacaktır?
   - Sistemin işlevselliği son kullanıcıların (yani, çalışanlar, müşteriler ve iş ortakları) istek ve ihtiyaçlarını ve yönetimin hedeflerini karşılayacak mı?

- İdarî ve hukukî koşullar analiz edildi ve dikkate alındı mı?
- Donanım ve yazılım ne kadar güvenlidir ve bu güvenlik yetkisiz erişimi, uygun olmayan kullanımı ve başka zararları etkileri ve kayıpları önleyecek veya tespit edecek mi?
- İşlem süreçleri güncel, doğru, tam ve itiraz edilemez olacak mı?
- Kontrol ortamı, kurumun kavramlardan sonuçlara e-ticaret hedeflerine ulaşmasına olanak sağlıyor mu?
- Risk değerlendirmesi hem iç hem de dış kuvvetleri kapsıyor mu?
- İnternet ve internet servis sağlayıcıya bağlı içsel riskler (temel iletişimin güvenilirliği, kullanıcı kimlik doğrulaması ve kimlerin erişim yetkisine sahip olduğu gibi) dikkate alındı mı?
- Diğer sorunlar dikkate alındı mı (örneğin, işle ilgili gizli bilgilerin ifşa edilmesi, fikrî mülkiyet haklarının kötüye kullanılması, telif hakkı ihlâlleri, ticarî marka tecavüzleri, internet sitelerinde onur kırıcı ifadeler, suiistimaller, elektronik imza suiistimalleri, özel hayatın ve bilgilerin gizliliğinin ihlâl edilmesi ve isme ve üne verilen zararlar gibi)?
- Dış satıcılar kullanılmışsa, bu satıcıyı kontrol ve tasdik etme yetkisine sahip bir güvenilir üçüncü şahıs tarafından bir "yürüyen iş" değerlendirmesi yapıldı mı?
- Satıcılar hosting (ana bilgisayar) hizmetleri veriyorlarsa, test edilmiş bir beklenmedik durum (contingency) planları var mı? Son SAS-70 raporlarını sundular mı? (SAS 70 raporları, kullanıcı kurumlara iç kontroller hakkında değerli bilgiler verebilir.) Ayrıca, özel hayatın ve bilgilerin gizliliği sorunları çözüldü mü?
- Sözleşme, denetim haklarını içeriyor mu?

**E-Ticaret Riskleri ve Kontrol Sorunları:**

6. E-ticaret risk ve kontrol ortamı oldukça karmaşıktır ve

gelişmektedir. *Risk*, hedeflere ulaşılması üzerinde olumsuz etki yapabilecek bir olayın meydana gelme belirsizliği olarak tanımlanabilir. Her şirketin ve her kamu tüzel kişisinin kendi *içsel riskleri* vardır. Örgütsel faaliyetlerin itici etkenleri, genellikle, yönetimin varsaydığı iş fırsatı riskleridir. Bu fırsatların altında, açıkça anlaşılmayan ve tam olarak değerlendirilmeyen ve iş yapmanın bir parçası olarak kolayca benimsenebilen tehditler ve başka tehlikeler de bulunabilir. Riski yönetme çabasında, öncelikle, risk unsurlarının anlaşılması ve kavranması şarttır. Bilgi güvenliği konusunda yeni zayıf ve savunmasız noktalar açan teknoloji değişikliklerinin ve yeni tehditlerin bilinmesi ve anlaşılması da önemlidir. Yönetim amaçlarıyla, örgütsel risklerin tanımlanması ve bu risklerin kontrol altına alınıp azaltılabileceği potansiyel yolların belirlenmesi ve hedeflenmesi için aşağıdaki *yedi temel soru* kullanılabilir. (Risk yöneticileri çeşitli farklı risk yönetim yaklaşımları kullanır; bu sorular bir yaklaşımı göstermektedir.) Bu sorularla bağlantılı *risk unsurları* parantez içinde gösterilmektedir.

**(a) Riskin Tanımlanması ve Miktar Tayini:**

- Kurumun hedeflerine ulaşma ve stratejilerini uygulama kabiliyetini olumsuz etkileyebilecek neler olabilir? [*Tehditler*]
- Bu *tehditler* gerçekleşirse, bunların muhtemel mali etkisi nedir? [*Tek Zarar Risk Değeri*]
- Bu olaylar ne sıklıkta olabilir? [*Sıklık*]
- İlk üç sorudakilerin gerçekleşme olasılığı nedir? [*Belirsizlik*]

**(b) Riskin Yönetilmesi ve Azaltılması:**

- Riskleri önlemek, kaçınmak, azaltmak ve tespit etmek ve gerekli bildirimde bulunmak için neler yapılabilir? [*Güvence ve Kontroller*]
- Bunun maliyeti nedir? [*Güvence ve Kontrol Maliyeti*]

- Bu ne kadar etkin olacaktır? [*Maliyet/Fayda veya ROI (Yatırım Geri Dönüşü) Analizi*]

7. İç denetçinin ele alması gereken daha hayatî risk ve kontrol sorunlarının bazıları şunlardır:
   - Genel proje yönetim riskleri,
   - Hizmetin reddi, fiziksel saldırılar, virüsler, kimlik hırsızlığı ve verilere yetkisiz erişim veya verilerin ifşası gibi özel güvenlik tehditleri,
   - Eski fakat hâlen kullanılmakta olan sistemler (legacy systems) ve veri depolarına bağlantıların karmaşık ağında işlem bütünlüğünün korunması,
   - 24 saat (bütün gün) hizmet sunan karmaşık ve gelişmiş müşteri özellikleri ve yeteneklerinin ve sık değişikliklerin bulunduğu durumlarda web sitesi içerik incelemesi ve onayı,
   - Hızlı teknoloji değişiklikleri,
   - Dünya çapında bireylerin özel hayat ve bilgilerinin korunması amacına yönelik düzenlemelerin artması; kurumun kendi ülkesi dışında sözleşmelerin ifa edilebilirliği ve vergi ve muhasebe sorunları gibi hukukî konu ve sorunlar,
   - Çevresel iş süreçlerinde ve örgütsel yapılardaki değişiklikler.

**E-ticaret Faaliyetlerinin Denetlenmesi:**

8. Genel denetim hedefi, bütün e-ticaret süreçlerinde etkili iç kontrollerin bulunmasını sağlamak olmalıdır. E-ticaret inisiyatiflerinin yönetimi, çok iyi geliştirilmiş ve onaylanmış bir stratejik planla belgelendirilmelidir. E-ticarete katılmama kararının alınması hâlinde, bu karar dikkatle analiz edilmeli, yazılı hâle getirilmeli ve yönetim mercii tarafından onaylanmalıdır.

9. Bir e-ticaret görevinde denetim hedefleri şunları içerebilir:

- E-ticaret işlemlerinin delilleri,
- Güvenlik sisteminin kullanılmaya hazırlık durumu ve güvenilirliği,
- E-ticaret ve finans sistemleri arasında etkin arayüz,
- Parasal işlemlerin güvenliği,
- Müşteri kimlik doğrulama sürecinin etkinliği,
- Operasyonların tekrar başlatılması da dahil, iş devamlılığı süreçlerinin yeterliliği,
- Genel ortak güvenlik standartlarına uyum,
- Dijital imzaların etkin kullanımı ve kontrolü,
- (Açık anahtar (public key) şifreleme tekniklerini kullanan) açık anahtar sertifikalarını kontrol etmek için uygulanan sistemler, politikalar ve prosedürlerin yeterliliği,
- İşletme verileri ve bilgilerinin yeterliliği ve zamanında elde edilmesi,
- Etkin bir iç kontrol sistemini gösteren deliller.

10. Belirli kurumlarda e-ticaret faaliyetlerini denetlemek için kullanılan denetim programının ayrıntıları, ilgili sektöre, ülkeye ve hukuk ve iş modellerine göre değişir. Temel alanlarda kullanılabilecek e-ticaret denetim protokolünün ana unsurları şunlardır:

**(a) E-ticaret örgütlenmesi:** İç denetçi şunları yapmalıdır:

- işlemlerin değerini tespit etmeli,
- hissedar ve diğer hak sahiplerini (iç ve dış) tanımlamalı,
- değişim yönetimi sürecini gözden geçirmeli,
- onay sürecini incelemeli,
- e-ticaret faaliyetleri iş planını gözden geçirmeli,
- açık anahtar sertifikalarına ilişkin politikaları değerlendirmeli,

- dijital imza prosedürlerini gözden geçirmeli,
- alıcı, tedarikçi ve sertifikalandırma yetkilisiyle yapılan hizmet düzeyi anlaşmalarını incelemeli,
- kalite güvencesi politikasını araştırmalı,
- e-ticaret faaliyetlerinde özel hayat ve bilgiler politikasını ve bu politikaya uyumu değerlendirmeli,
- arızalara müdahale (cevap) yeteneğini incelemeli ve değerlendirmelidir.

**(b) Suiistimal:** İç denetçi şu konularda uyanık olmalıdır:

- Yetkisiz para hareketleri (yani, fonların geri alınması ve kurtarılmasının güç olacağı ülkelere para transferleri),
- Ödemelerin tekrarlanması (çifte ödemeler),
- Verilen veya alınan siparişlerin, teslim alınan malların veya yapılan ödemelerin reddedilmesi,
- Kural dışı durum (istisna) raporları ve prosedürleri ve takip etkinliği,
- Dijital imzalar: Bütün işlemlerde dijital imza kullanılıyor mu? Bunlara kim yetki veriyor? Bunlara kimler erişim hakkına sahip?
- Virüslere ve korsanlık faaliyetlerine karşı koruma tedbirleri (geçmiş işlemler kütüğü, araç kullanımı),
- Erişim hakları: Erişim hakkı düzenli olarak gözden geçiriliyor mu? Personel değişikliği olduğunda erişim hakları da derhal değiştiriliyor mu?
- İşlemlerin yetkisiz kişiler tarafından engellenmesi ve durdurulmasıyla ilgili geçmiş kayıtlar.

**(c) Kimlik Doğrulaması** (Authentication): İç denetçi, yapılan işlemlerde kimlik doğrulamasıyla ve uygulanan kontrollerin değerlendirilmesiyle ilgili politikaları gözden geçirmelidir.

- Düzenli inceleme ve gözden geçirme delilleri,
- Yönetimin kullandığı kontrol özdeğerlendirme (CSA[5]) araçları,
- Düzenli bağımsız kontroller,
- Görevler ayrımı,
- Yönetimin sahip olması gereken araçlar: Kalkanlar (firewalls) (çoklu seviyeden dilimlemeye e-ticaret ve diğer faaliyetler), şifre yönetimi, bağımsız mutabakat ve denetim izleri.

**(d) Verilerin Bozulması:** İç denetçi, veri bütünlüğü üzerindeki kontrolleri değerlendirmelidir.

- Kataloglarda ve fiyatlar veya ücretlerde kimler değişiklik yapabilir? Onay mekanizması nedir?
- Herhangi biri denetim izlerini imha edebilir mi?
- Elektronik bülten panosu değişikliklerine kim onay verme yetkisine sahiptir?
- Sipariş ve kayıt prosedürleri nelerdir?
- Çevrimiçi ihale sürecinde yeterli dokümantasyon veriliyor mu?
- Yönetimin sahip olması gereken araçlar: Saldırıya karşı savunma yönetimi [gözlem yazılımı, otomatik zaman aşımı (time out) ve eğilim analizi], e-ticaret sunucuları için fiziksel güvenlik, değişim kontrolü ve mutabakat.

**(e) İş kesintisi:** İç denetçi, iş devamlılığı planını incelemeli ve planın test edilip edilmediğini tespit etmelidir. Yönetim, bir kesinti hâlinde işlem ve hareketlerin süreci için alternatif bir yol geliştirmiş olmalıdır. Yönetimin aşağıda sayılan potansiyel durumları çözümlemeye yönelik bir süreci bulunmalıdır:

[5] CSA: Control Self Assessment

- Disk ya da manyetik bant alanı saldırıları,
- Servisin reddi (DoS[6]) saldırıları,
- E-ticaret ile finans yönetimi sistemleri arasındaki arayüzde yetersizlik,
- Yedekleme imkânları,
- Korsanlık, saldırılar, güvenlik engellerini kırma, virüsler, solucanlar (worms), Truva atları (Trojan horses) ve arka kapılar (back doors) gibi sorunlarla mücadele stratejileri.

**(f) Yönetim Sorunları:** İç denetçi, iş birimlerinin e-ticaret sürecini iyi yönetip yönetmediğini değerlendirmelidir. İlgili bazı konular aşağıda sunulmaktadır:

- Bireysel inisiyatifler ve geliştirme projeleri hakkında proje yönetim incelemeleri,
- Sistem Geliştirme Yaşam Çevrimi (System Development Life Cycle) incelemeleri,
- Satıcı seçimi, satıcıların yetenekleri, personel gizliliği ve bağlılık,
- Uygulama sonrası ekonomik incelemeler: Beklenen faydalar elde ediliyor mu? Başarıyı ölçmek için hangi kıstaslar kullanılıyor?
- Uygulama sonrası süreç incelemesi: Yeni süreçler var mı ve etkin çalışıyor mu?

[6] DoS: Denial of Services

# Uygulama Önerisi 2100-7: Çevresel Risklerin Tanımlanması ve Rapor Edilmesinde İç Denetçinin Rolü

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**

İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *Bu Uygulama Önerisinin amacı, çevresel denetim faaliyetleriyle ilgili risk ve bağımsızlık konuları hakkında iç denetim birimlerine yol göstermektir. İç denetçiler, çevreyle ilgili denetçilerin kurum içindeki yeri ve hiyerarşik ilişkilerinden kaynaklanabilecek potansiyel riskler konusunda uyanık olmalıdır. Bu Uygulama Önerisi, önemli çevre sorunlarının uygun kademeye zamanında rapor edilmesini sağlamak amacına yönelik asgarî güvence araçları konusunda önerilerde bulunmaktadır. Çevre mevzuatına uymama riskleri, para cezaları ve cezalar ve diğer kötü yönetim riskleri kurum için önemli zararlara yol açabilir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. İç denetim yöneticisi, kurum çapında risk yönetim değerlendirmesine *çevre, sağlık* ve *emniyet* (ÇSE) *risklerini* de dahil etmeli ve faaliyetleri kurumun işleriyle bağlantılı diğer risk tiplerine kıyasla dengeli bir şekilde değerlendirmelidir. Değerlendirilmesi gereken risk tehditleri arasında şunlar sayılabilir: Kurum içi raporlama yapıları; çevresel zarar, para cezaları ve diğer cezalara neden olma olasılığı; Çevre Koruma Dairesi'nin (EPA) veya diğer kamu kurumlarının öngördüğü harcamalar; yaralanma ve ölüm kayıtları; müşteri kayıpları kaydı, kurum hakkında olumsuz yayınlar,

kurumun toplumsal imaj ve itibar kaybı.

2. İç Denetim Yöneticisi, ÇSE riskleri yönetiminin büyük ölçüde bir *çevre denetim* fonksiyonuna bağlı olduğunu tespit ettiği takdirde, İç Denetim Yöneticisinin bu örgütsel yapının sonuçları yanında, faaliyetlerine ve raporlama mekanizmalarına etkilerini değerlendirmesi gerekir. İç Denetim Yöneticisi, risk yönetiminin yeterli olmadığını ve bakiye (artık) bir riskin var olduğunu tespit ederse, bu sonuç, tabiatıyla, iç denetim faaliyetinin görev planında bir değişikliği ve daha ileri incelemeleri gerektirecektir.

3. Çevre denetim fonksiyonlarının çoğu, İç Denetim Yöneticisine değil, kendi kurumunun *çevre yöneticisine* veya *genel danışmana* bağlıdır. Çevre denetimi için tipik örgütsel modeller, aşağıdaki senaryolardan birinin kapsamına girer:

   - İç denetim yöneticisi ve çevre denetim yöneticisi, birbirleriyle çok az teması bulunan *ayrı* fonksiyonel birimlerdir.
   - İç denetim yöneticisi ve çevre denetim yöneticisi, ayrı fonksiyonel birimlerdir ve faaliyetlerinin *eşgüdümünü* sağlarlar.
   - İç Denetim Yöneticisinin çevre sorunlarını denetleme *sorumluluğu vardır*.

4. Çevre denetim sorunlarına ilişkin IIA'nın hazırladığı bir geçici durum raporuna göre:

   - Çevre denetçilerinin yaklaşık yarısı, nadiren, yönetim birimine bağlı bir kurulla toplanır ve sadece %40'ının İç Denetim Yöneticisi ile bir teması vardır.
   - Kurumların %70'i, çevreyle ilgili sorunların yönetim birimi toplantılarının gündemine düzenli olarak konulduğunu bildirmiştir.
   - Kurumların yaklaşık %40'ı, son üç yıl içinde çevre mevzuatı ihlâlleri sebebiyle para cezalarına veya diğer cezalara

çarptırıldıklarını bildirmiştir. Ankete katılanların üçte ikisi, çevresel risklerini önemli olarak tanımlamıştır.

5. Çevre, Sağlık ve Emniyet Denetimi Yuvarlak Masası (yeni adı *"Denetim Yuvarlak Masası"*), Utah Eyalet Üniversitesi'nden Richard L. Ratliff ve bir grup araştırmacıdan, bir çevre, sağlık ve emniyet denetimi araştırması yapmalarını talep etmiştir. Bu araştırma sonucunda, araştırmacıların risk ve bağımsızlık sorunlarına ilişkin bulguları aşağıdaki gibidir:

   - ÇSE denetim işlevi, diğer kurum içi denetim faaliyetlerinden biraz tecrit edilmiştir. ÇSE denetim fonksiyonu, iç denetimden ayrı teşkilâtlanmıştır; mali tabloların dış denetimiyle bağlantısı çok güçlü değildir ve yönetim mercii veya üst yönetime değil bir ÇSE yöneticisine bağlıdır. Bu yapı, yönetimin ÇSE denetimini, sadece kurumun ÇSE işlevi içinde yeri olan teknik bir alan olarak gördüğünü göstermektedir.
   - Bu örgütsel konumda, ÇSE denetçileri, etkin bir denetim fonksiyonunun temel şartlarından biri olarak görülen *bağımsızlıklarını* koruyamaz. ÇSE denetim müdürleri, normalde, idarî yapı içinde, denetlenen fiziksel tesislerden sorumlu olan yöneticilere bağlıdır. Bundan ötürü, zayıf ÇSE performansı, ilgili tesislerin yönetiminden sorumlu ekibi kötü etkileyecektir. Bu nedenle, *tesis yönetim ekibi*, denetim bulguları olarak neyin rapor edileceği, denetimin nasıl yapılacağı ya da denetim planına nelerin alınacağı gibi konularda etki ve nüfuzunu kullanmayı deneyecektir. Denetçilerin meslekî kararlarının bu etki ve nüfuz altında kalma potansiyeli, sadece görünürde olsa bile, denetçi bağımsızlığını ve objektifliğini ihlâl eder.
   - Yazılı denetim raporlarının, kurum içinde, en fazla üst seviye çevre yöneticileri kademesine kadar dağıtılması da yaygın bir uygulamadır. Ancak bu yöneticiler, potansiyel bir menfaat çatışması içinde olabilecekleri için, ÇSE denetim bulgularının

daha üst yönetime, denetim komitesine ve yönetim kuruluna iletilmesine engel olabilirler.

- Denetim bilgileri genellikle (a) avukat-müvekkil ilişkilerinin gizliliği kapsamındaki bilgiler veya avukatın meslekî çalışmaları kapsamındakiler, (b) gizli ve özel, (c) gizli değilse de, sıkı kontrol altında tutulan bilgiler olarak sınıflandırılır. Bu da, ÇSE denetim bilgilerine erişimin, son derece kısıtlı olmasıyla sonuçlanır.

## İÇ DENETİM YÖNETİCİSİNE ÖNERİLER:

6. İç denetim yöneticisi, *çevre koruma* yöneticisiyle yakın bir iş ilişkisi kurmalı ve faaliyetlerini çevre denetim planıyla uyumlu yürütmelidir. Çevre denetim biriminin İç Denetim Yöneticisi dışında bir kişiye bağlı olduğu durumlarda, İç Denetim Yöneticisi, görevin ifasını ve denetim planını gözden geçirmeyi teklif etmelidir. Çevre denetim birimi, *örgütsel* olarak iç denetim biriminden *bağımsız ise*, İç Denetim Yöneticisi, dönemsel olarak çevre denetim biriminin kalite güvencesi kontrolünü planlamalı ve uygulamalıdır. Bu kontrol sonucunda, çevre risklerine karşı yeterli tedbirin alınıp alınmadığı tespit edilmelidir. Bir ÇSE denetim programı (a) *uyum odaklı* (yani, kanunlara, mevzuata ve kurumun kendi ÇSE politikaları, prosedürleri ve performans hedeflerine uyulup uyulmadığının kontrolü), (b) *yönetim sistemleri odaklı* (yani, risklerin azaltılması ve hukukî ve iç gereklere uymak amacına yönelik olarak, yönetim sistemlerinin değerlendirilmesi) veya (c) bu iki yaklaşımın bir *karışımı* olabilir.

7. İç Denetim Yöneticisi, kendisinin yönettiği birimin bir parçası olmayan çevre denetçilerinin genel kabul gören meslekî denetim standartlarına ve genel kabul gören etik kurallarına uyup uymadıklarını değerlendirmelidir. Hem *Çevre, Sağlık & Emniyet Denetçisi Sertifikalandırma Kurulu* (BEAC) hem de IIA, uygulama standartlarını ve etik kurallarını yayınlamaktadır.

8. İç denetim yöneticisi, kurumun karşılaştığı ciddî risklerden kaynaklanan önemli sorunların hiyerarşi içinde yönetim kurulunun denetim komitesine veya bağlı başka bir komitesine rapor edilmesini sağlamak amacıyla, çevre denetim biriminin kurum örgütlenmesi içindeki konumunu ve bağımsızlığını değerlendirmelidir. İç Denetim Yöneticisi, önemli ÇSE riskleri ve kontrol sorunlarının denetim komitesine (veya yönetim kurulunun başka bir komitesine) rapor edilmesini de mümkün kılmalıdır.

# Uygulama Önerisi 2100-8: Bir Kurumun Gizlilik Politikasının Değerlendirilmesinde İç Denetçinin Rolü

Uluslararası İç Denetim Standartlarından
Standart 2110'un Yorumu

## İligili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bir kurumun gizlilik politikasıyla ilgili faaliyetlerinin kontrolü ve değerlendirilmesinde aşağıdaki önerileri dikkate almalıdır. Bu Uygulama Önerisinin, gizlilik politikasıyla bağlantılı kapsamlı bir güvence sağlama veya danışmanlık görevi için gereken bütün prosedürleri kapsamak gibi bir amacı yoktur; kılavuz sadece denetim komitesinin, yönetim kurulunun ve yönetimin ilgili sorumluluklarını tamamlayıcı nitelikte üst düzey denetçinin sorumlulukları konusundaki bir öneriler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Bilgi teknolojisi ve iletişimdeki gelişmeler, özel hayata ve gizliliğe yönelik yeni riskler ve tehditler yaratmaya devam ettikçe, kişisel mahremiyet ve gizliliğin korunmasıyla ilgili kaygılar giderek daha belirgin, merkezî ve evrensel bir duruma gelmektedir. Dünyanın büyük bir kısmında, gizlilik kontrolleri, iş hayatıyla ilgili hukukî düzenlemelerin bir parçasıdır.

2. *Gizlilik tanımları* ülkeye, kültüre, siyaset ortamına ve hukuk sistemine göre büyük farklılık göstermektedir. Gizlilik kavramı kişisel gizliliği (fiziksel ve psikolojik); *yer* gizliliğini (gözetimden

uzak olmak); *iletişim* gizliliğini (izleme ve gözlemden uzak olmak) ve *bilgi* gizliliğini (kişisel bilgilerin başkalarınca toplanması, kullanılması ve ifşa edilmesi) kapsar. Kişisel bilgiler, genel olarak, belirli bir bireyle ilgili olan bilgiler ya da başka bilgilerle bağlantı kurulabilecek ayırt edici nitelikteki bilgiler anlamına gelir. Kişisel bilgiler, herhangi bir ortam veya formatta kaydedilmiş olsun ya da olmasın maddî olgularla ilgili veya subjektif bilgileri içerebilir. Kişisel bilgilere örnek olarak, şunlar sayılabilir:

- İsim, adres, kimlik numaraları, gelir seviyesi veya kan grubu,
- Değerlendirmeler, görüşler, sosyal statü veya sabıka kayıtları veya disiplin cezaları,
- Personel özlük dosyaları, kredi ve borç kayıtları.

3. Gizlilik, bir *risk yönetim sorunu*dur. Gizliliğin ve kişisel bilgilerin uygun kontrollerle korunamaması, bir kurum için ciddî ve önemli sonuçlar yaratabilir. Örneğin, kişilerin ve kurumun itibarına zarar verebilir, hukukî sorumluluklara neden olabilir, tüketicilerde ve personelde güven kaybına yol açabilir.

4. Kişisel bilgilerin korunması konusunda dünya çapında geliştirilmekte olan çeşitli kanun ve düzenlemeler vardır. Ayrıca, gizlilik konusunda uygulanabilecek genel kabul gören politika ve uygulamalar da vardır.

5. Başarılı gizlilik uygulamalarının iyi yönetişime ve yönetim sorumluluğuna katkıda bulunduğu açıktır. Kurumun temel ve büyük risklerinin belirlenmesinden ve belirlenen bu riskleri azaltmak için uygun sistemlerin uygulanmasından, nihaî olarak yönetim mercii (yani, yönetim kurulu, bir kurumun veya tüzel kişinin başkanı veya yöneticisi) sorumludur. Bu sorumluluk, kurum için gereken gizlilik politikasının oluşturulmasını ve uygulamasının gözlenmesini de kapsar.

6. İç denetçi, kuruma, gizlilik hedeflerine uymasında yardımcı olarak,

iyi bir yönetişime ve yönetim sorumluluğunun sağlanmasına katkıda bulunabilir. İç denetçi, kendi kurumundaki gizlilik politikasının değerlendirilmesi, önemli risklerin belirlenmesi ve bu riskleri azaltıcı tavsiyelerin yapılması konusunda, benzersiz bir konumdadır.

7. Gizlilik politikasının değerlendirilmesinde, iç denetçi şunları dikkate almalıdır:
   - Kendi ülkelerindeki (kurumun faaliyet yürüttüğü diğer ülkelerdekiler de dahil) gizlilikle ilgili çeşitli kanun, düzenleme ve politikalar,
   - Kurumun faaliyet yürüttüğü ülke/ülkelerde geçerli olan ve kurumun tâbi olduğu kanun, düzenleme ve diğer standartların ve uygulamaların niteliğinin tam olarak belirlenmesi konusunda kurumun hukuk danışmanıyla irtibat,
   - Bilgi güvenliği ve veri koruma kontrollerinin bulunmasını sağlamak; bunları düzenli olarak gözden geçirmek ve uygunluklarını tespit etmek ve değerlendirmek için bilgi teknolojisi uzmanlarıyla irtibat,
   - Kurumun gizlilik uygulamalarının seviyesi veya gelişmişliği. Bu seviyeye bağlı olarak, iç denetçi, farklı ve değişen roller üstlenebilir. Denetçi; gizlilik programının geliştirilmesini ve uygulanmasını kolaylaştırabilir; kurumun ihtiyaç ve risklerini tespit etmek amacına yönelik bir gizlilik risk değerlendirmesi yapabilir ya da kurumun gizlilik politikaları, uygulamaları ve kontrollerinin kurum yapısı içindeki etkinliğini inceleyebilir ve bu konuda güvence verebilir. İç denetçi, bir gizlilik programının geliştirilmesi ve uygulanması sorumluluğunun bir kısmını üstlenirse, bu durum iç denetçinin bağımsızlığına halel getirebilir.

8. Normal olarak, bir iç denetçiden beklenebilecekler, kendi

kurumunun topladığı, kişisel veya özel sayılan bilgilerin türlerini tanımlaması, uygunluklarını belirlemesi; kullanılan bilgi toplama yöntemini tanımlaması, kurumun topladığı bu bilgileri asıl kullanım amacına ve kanunlara uygun kullanıp kullanmadığını ve bu bilgilerin toplandığı, tutulduğu ve kullanıldığı alanları belirlemesidir.

9. Bu konunun son derece teknik ve hukukî niteliğinden dolayı, iç denetçi, gizlilik politikasını değerlendirme çalışması yapabilmesi için yeterli bilgiye ve niteliklere sahip olmalı ve bu amaçla, gerekirse, üçüncü şahıs uzmanlardan yararlanmalıdır.

# Uygulama Önerisi 2100-9: Uygulama Sistemlerinin İncelenmesi

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**

İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu-Uygulama Sistemlerinin İncelenmesi, Doküman G14'ten uyarlanmıştır. Bahsi geçen BS Denetim kılavuzu ISACA tarafından Kasım 2001'de yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın çıkarttığı ve yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, uygulama sistemleri incelemesi yaparken aşağıdaki önerileri dikkate almalıdırlar. Bu kılavuzun, uygulama sistemleri incelemesiyle ilgili kapsamlı bir güvence veya danışmanlık görevi için gereken bütün prosedürleri yansıtmak gibi bir amacı yoktur; klavuz, sadece, ayrıntılı denetim planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumluluklarından oluşan bir temel öneriler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

**1.** İç denetim yöneticisi, iç denetim faaliyetinin, bir uygulama sistemleri incelemesi yapmak ve bağlantılı risklere maruziyet düzeyini değerlendirmek için bağımsız[1] ve yetkin denetim kaynaklarına

[1] *Bağımsızlık,* denetçinin ilgili uygulama sisteminin geliştirilmesi, edinilmesi, uygulanması veya sürdürülmesi gibi işlerde görev almamış olmasıdır.

sahip olup olmadığını veya bu tip kaynaklara erişim olanağının bulunup bulunmadığını tespit etmelidir.

**Planlama Mülâhazaları:**

**2.** Denetçinin, kurumun bilişim sistemlerinin büyüklüğü ve karmaşıklık düzeyi ile kurumun bilişim sistemlerine bağımlılığının derecesini tespit edebilmesi için yeterli bir düzeyde kurumun bilişim sistemleri yapısını anlaması, planlamanın tamamlayıcı ve ayrılmaz bir parçasıdır. Denetçi, kurumun misyonu ve hedefleri, bilişim teknolojisi (BT) ve bilişim sistemlerinin (BS) nasıl ve hangi düzeyde kullanıldığı, kurumun hedefleri ve bilişim sistemleri açısından karşılaşılan riskler ve olasılık düzeyleri konularında da bilgi sahibi olmalıdır. Ayrıca, denetçi, kilit BS personeli ve uygulama sistemi iş süreci sahibinin görev ve sorumlulukları da dahil kurumun örgütlenme yapısını da bilmelidir. Denetim planlaması sırasında, kurumun faaliyet alanlarındaki riskler de dikkate alınmalıdır.

Planlamanın aslî ve temel hedefi, uygulama düzeyi risklerini tanımlamak ve belirlemektir. Riskin nisbî seviyesi, gereken denetim bulguları ve delilleri seviyesini etkiler. Sistem ve veri seviyesinde yer alan *uygulama düzeyi riskleri*nden bazıları aşağıda yer almaktadır:

- Sistem işletim kapasitesinin yetersizliği ile ilgili olarak sistemin *uygunluk* riskleri.
- Sistemlere ve/veya verilere yetkisiz erişimle ilgili *sistem güvenliği* riskleri.
- Verilerin eksik, hatâlı veya yetkisiz işlenmesi ya da zamanında işlenmemesiyle ilgili *sistem bütünlüğü* riskleri.
- Sistemin uygunluğu, güvenliği ve bütünlüğünü sağlamak ve sürdürmek için gerekli olan sistem güncellemesindeki yetersizlik ile ilgili *sistem sürdürülebilirliği* riskleri.

- Verilerin tam ve eksiksiz olması, bütünlüğü, gizliliği, mahremiyeti, doğruluğu ve zamanında verilmesiyle ilgili *veri* riskleri.

Uygulama düzeyi risklerine yönelik *uygulama kontrolleri*; sistemin içine yerleştirilmiş bilgisayarlı kontroller, manuel uygulanan kontroller veya bunların bir kombinasyonu şeklinde olabilir. Örnek olarak, dokümanların (sipariş, fatura ve irsaliye) bilgisayar ortamında eşlenmesi, bilgisayardan alınan bir kontrol çıktısının kontrol edilmesi ve imzalanması ile hatâ raporlarının üst yönetim tarafından incelenmesi verilebilir.

*Programlanmış* kontrolleri dayanak kabul etme seçeneği seçildiği takdirde, hem denetim hedefiyle ilgili özel kontroller, hem de ilgili *BT kontrolleri* dikkate alınmalıdır. Genel BT kontrolleri, ayrı bir incelemenin konusu da olabilir ve aşağıda sayılanlar gibi kontrolleri içerir: Fiziksel kontroller, sistem güvenliği, ağ yönetimi, veri yedekleme ve beklenmedik durum planlaması. İncelemenin kontrol hedeflerine bağlı olarak, bir uygulama sisteminin satın alımının düşünüldüğü durumlar gibi hallerde, denetçinin genel kontrolleri incelemesi gerekmeyebilir.

*Uygulama sistemi* incelemeleri, bir paket uygulama sistemi satın alımı gündeme geldiğinde, uygulama sistemi kullanıma alınmadan önce (uygulama öncesi) ve uygulama sistemi kullanıma alındıktan sonra (uygulama sonrası) yapılabilir. Uygulama öncesinde yapılan uygulama sistemi incelemesinin kapsamı; uygulama düzeyi güvenliğinin mimarisini, güvenlik uygulamasına yönelik planları, sistem ve kullanıcı dokümantasyonunun yeterliliğini ve fiilî veya planlanmış kullanıcı kabul testlerinin yeterliliğini içerir. Uygulama sonrasında yapılan incelemenin kapsamı ise; uygulamadan sonraki uygulama düzeyi güvenliğini içerir ve eski sistemden yeni sisteme veri transferi ve ana dosya bilgileri transferi yapılmışsa, sistem dönüşümünü de kapsayabilir.

Bir uygulama sistemleri incelemesinin hedefleri ve kapsamı, genellikle, görev planının bir parçasını oluşturur. Görev planının biçimi ve içeriği değişebilir, fakat şunları içermelidir:

- Uygulama sistemleri incelemesinin hedefleri ve kapsamı.
- İncelemeyi yapan denetçi(ler).
- Projede görev alan denetçi(ler)in bağımsızlığına ilişkin bir açıklama.
- İncelemenin ne zaman başlayacağı ve zaman çizelgesi.
- Kapanış toplantısı düzenlemeleri de dahil raporlama düzenlemeleri.
- Hedefler 7 COBIT[2] bilgi kriterini işaret edecek şekilde oluşturulmalı ve kurum tarafından benimsenmelidir. 7 COBIT bilgi kriteri, aşağıda sayılanları içerebilir:
  - Etkinlik, Verimlilik, Gizlilik, Bütünlük, Müsaitlik[3], Uyum ve Bilgilerin Güvenilirliği.

Denetçi, daha önce, bir uygulama sisteminin geliştirilmesi, iktisabı, uygulanması veya idamesinde görev almışsa ve bir denetim görevi için tayin edilmişse, bu durum denetçinin bağımsızlığına zarar verebilir. Denetçi, bu tür durumlarda ilgili kurallara başvurmalıdır.

**Denetim Çalışmasının Yapılması:**

**3.a. İşlem Akışının Kaydedilmesi:**

Toplanan bilgiler, sistemin hem bilgisayarlı hem de manuel yönlerini ve özelliklerini kapsamalıdır. Bu konuda, denetim hedefleri açısından önem taşıyan veri girişi (elektronik veya manuel), işlenmesi, saklanması ve çıktısı üzerinde odaklanılmalıdır. Denetçi, uygulanan iş süreçlerine ve teknolojinin kullanımına bağlı olarak, işlem akışını kaydetmenin ve dokümante etmenin pratik olmayabileceğini düşünebilir. Bu durumda, denetçi, bir üst düzey *veri akış şeması* veya açıklaması hazırlamalı ve/veya verilmişse sistem dokümantasyonunu kullanmalıdır.

---

(2) COBIT: Control Objectives for Information and Related Technology

(3) Müsaitlik: Mevcut ve kullanıma hazır olma hâli (İng. Availability).

Diğer sistemlerle *uygulama arayüzleri*nin dokümante edilmesi de düşünülmelidir. Denetçi, *gözden geçirme testi* gibi prosedürleri uygulayarak dokümantasyonu teyit etmeli ve doğrulamalıdır.

**3.b. Uygulama Sistemi Kontrollerinin Tanımlanması ve Testi:** Uygulama risklerini azaltmak amacına yönelik *özel kontroller* tanımlanabilir ve kontrollerin amaçlandığı gibi çalıştığı ve işlediği konusunda denetçiye güvence vermek için yeterli denetim bulguları ve delilleri toplanır. Bu, sorgulama ve gözlem, dokümantasyonun gözden geçirilmesi ile programlanmış kontrollerin test edildiği durumlarda uygulama sistemi kontrollerinin test edilmesi gibi prosedürlerle gerçekleştirilebilir (BDDT'lerin kullanılması da düşünülebilir).

Testlerin niteliği, zamanlaması ve kapsamı, incelenen alanın risk düzeyine ve denetim hedeflerine göre belirlenmelidir. Güçlü genel BT kontrollerinin bulunmadığı durumlarda, denetçi, bu zayıflığın bilgisayarlı uygulama kontrollerinin güvenilirliği üzerindeki etkisini değerlendirebilir. BS Denetçisi bilgisayarlı uygulama kontrollerinde önemli bir zayıflık bulduğu takdirde, mümkünse, manuel olarak yapılan süreç kontrollerinden yeterli güvence alınmalıdır (denetim hedeflerine bağlı olarak).

Bilgisayarlı kontrollerin etkinliği, güçlü genel BT kontrollerinin varlığına bağlıdır. Bu nedenle, genel BT kontrollerinin gözden geçirilmemesi halinde, uygulama kontrollerine güvenme olanağı ciddi ölçüde sınırlanmış olur ve bu durumda, denetçi alternatif prosedürleri düşünmelidir.

**Raporlama:**

**4.** Bir uygulama sistemleri görevinin sonuçlarını içeren rapor, görevin niteliği ile sınırlamalar, kısıtlamalar ve bilgi kullanıcılarının haberdar olması gereken diğer faktörleri açıkça göstermeli ve tanımlamalıdır. Denetçi raporda, kontrollerin güçlendirilmesine

yönelik önerilerini de belirtmelidir.

Uygulama incelemesi sırasında tespit edilen ve kontrollerin bulunmamasından veya bunlara uyulmamasından kaynaklanan zayıflıklar, hem ilgili iş süreci sahibine hem de uygulamaya destek olmaktan sorumlu olan BS yönetimine bildirilmelidir. Bir uygulama sistemleri incelemesi sırasında önemli veya esaslı olduğu düşünülen zayıflıkların tespit edilmesi durumunda, ilgili yönetim kademesi, gerekli düzeltici işlemleri derhal yapması hususunda bilgilendirilmelidir. Etkin bilgisayarlı uygulama kontrolleri genel BT kontrollerine bağlı olduğundan dolayı, bu alandaki zayıflıklar da rapor edilmelidir. Genel BT kontrolleri incelenmemişse, bu durum raporda belirtilmelidir.

# Uygulama Önerisi 2100-10: Denetim Örnekleme Çalışması

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu-Denetim Örnekleme Çalışması, Doküman G10'dan uyarlanmıştır. Bahsi geçen BS Denetim kılavuzu ISACA tarafından Mart 2000'de yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın çıkarttığı ve yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, test için Denetim Örnekleme tekniklerini kullanırken aşağıdaki önerileri dikkate almalıdırlar. Bu kılavuzun, denetim örnekleme çalışması için gereken bütün prosedürleri yansıtmak gibi bir amacı yoktur; klavuz, sadece, ayrıntılı denetim planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumluluklarından oluşan bir temel öneriler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## I. DENETİM ÇALIŞMASININ YAPILMASI:

**Denetim Örnekleme Çalışması:**
İstatistiksel olan veya olmayan örnekleme yöntemlerini kullanırken, denetçi, yeterli, güvenilir, amaca uygun ve kullanışlı denetim delilleri elde etmek için, bir denetim örneklemi tasarlamalı ve seçmeli, denetim prosedürlerini uygulamalı ve örneklem sonuçlarını değerlendirmelidir. Bir denetim mütalaası oluştururken denetçiler, örnekleme yöntemiyle

de geçerli sonuçlara ulaşılabileceği ve bilgilerin tümünü incelemek pratikte mümkün olmayabileceği için, genellikle, mevcut bilgilerin tümünü incelemezler.

Denetim *örnekleme* çalışması; popülasyon hakkında bir sonuca varmak veya bir sonuca varılmasına yardımcı olmak amacıyla seçilen süjelerin belirli özellikleri hakkında denetim bulguları ve delillerini denetçinin değerlendirebilmesi için, denetim prosedürlerinin o popülasyonun %100'ünden daha az bir kısmına uygulanması olarak tanımlanır. İstatistiksel örnekleme çalışması, popülasyon hakkında matematiksel yöntemlerle oluşturulan sonuçlara varılabilecek tekniklerin kullanılmasını kapsar.

İstatistiksel olmayan örnekleme çalışması ise, istatistik bazlı olmayıp alınan örneklemin tüm popülasyonu temsil etmesi muhtemel olmadığından bu çalışmanın sonuçlarının tüm popülasyona mal edilmemesi gerekir.

**Örneklemin Tasarlanması:**
Bir denetim örnekleminin büyüklüğü ve yapısını tasarlarken, denetçiler, somut denetim hedeflerini, popülasyonun niteliğini ve örnekleme ve seçim yöntemlerini dikkate almalıdırlar. Denetçi, örneklemlerin tasarımı ve analizi çalışmasına ilgili uzmanların da katılması gereğini dikkate almalıdır.

*Örneklem Birimi:* Örneklem birimi, örneklemin amacına bağlı olacaktır. Kontrollerin uyum testi için, normalde, örneklem birimi bir olay veya işlem olan nitelik örneklemesi yöntemi uygulanır (örneğin, bir faturada yetkilendirme gibi bir kontrol). Nicelik testi için, genellikle, örneklem birimi parasal bir büyüklük olan değişken veya tahmin örnekleme yöntemleri uygulanır.

*Denetim Hedefleri:* Denetçi, ulaşmak istediği somut denetim hedeflerini ve bu hedeflere ulaşma olasılığı en fazla olan denetim prosedürlerini

dikkate almalıdır. Denetim örnekleme çalışması uygun ise, aranan denetim bulgu ve delillerinin niteliği ve muhtemel hatâ durumları dikkate alınmalı ve değerlendirilmelidir.

*Popülasyon:* Popülasyon, denetçinin popülasyon hakkında bir sonuca ulaşmak için örnek seçmek istediği tam veri seti anlamına gelir. Bu nedenle, örnekleme yapılacak olan popülasyonun uygun olması ve somut denetim hedefi için tam ve eksiksiz olduğunun doğrulanması gerekir.

*Katmanlama* (Stratification): Örneklem tasarımının etkin ve verimli olmasına yardımcı olmak için, katmanlama çalışması uygun olabilir. Katmanlama, her örneklem birimi sadece tek bir katmana girecek şekilde, bir popülasyonun açıkça tanımlanmış benzer özellik ve niteliklere sahip alt-popülasyonlara bölünmesi işlemidir.

*Örneklem büyüklüğü:* Örneklem büyüklüğünü tespit ederken, denetçi, örnekleme riskini, kabul edilebilecek hatâ miktarını ve beklenen hatâların kapsamını dikkate almalıdır.

*Örnekleme riski:* Örnekleme riski, denetçinin vardığı sonucun ilgili popülasyonun tümü aynı denetim prosedürüne tâbi tutulsaydı ulaşılacak olan sonuçtan farklı olabileceği olasılığından kaynaklanır. İki tip örnekleme riski vardır:

- Yanlış kabul riski: gerçekte popülasyonun önemli ölçüde hatâlı değerlendirilmesine rağmen, hatâlı değerlendirme yapılması ihtimalinin olmadığı şeklinde bir değerlemede bulunma riskidir.
- Yanlış red riski: gerçekte popülasyonun önemli ölçüde hatâlı değerlendirilmemiş olmasına rağmen, hatâlı değerlendirme yapılması ihtimalinin olduğu şeklinde bir değerlemede bulunma riskidir.

Denetçinin kabul etmeye razı olduğu örnekleme riski düzeyi, örneklem

büyüklüğünü etkiler. Örnekleme riski, denetim riski modeli ve onun unsurları, içsel risk, kontrol riski ve tespit riskiyle ilişkili olarak değerlendirilmelidir.

*Tolere edilebilir hatâ:* Tolere edilebilir hatâ, denetçilerin kabul etmeye razı oldukları ve yine de denetim hedefine ulaşıldığı sonucuna vardıkları, popülasyondaki azami hatâ düzeyidir. Nicelik testlerinde tolere edilebilir hatâ, denetçinin önemlilik düzeyi hakkındaki kanısıyla ilişkilidir. Uyum testlerinde tolere edilebilir hatâ, denetçinin, öngörülmüş bir kontrol prosedüründen sapma hususunda kabul etmeye razı olduğu azami orandır.

*Beklenen hatâ:* Denetçi popülasyonda hatâların bulunacağını beklediği takdirde, popülasyonda fiilen mevcut hatâların planlanmış tolere edilebilir hatâlardan daha fazla olmadığı sonucuna varmak için, normal olarak hiç bir hatânın beklenmediği duruma göre daha büyük bir örneklem grubu seçilmeli ve incelenmelidir. Popülasyonda herhangi bir hatâ bulunmaması beklenen durumlarda ise, daha küçük örneklem grupları kullanılabilir. Bir popülasyonda beklenen hatâyı belirlerken, denetçi, daha önceki denetimlerde tespit edilen hatâ seviyeleri, kurumun prosedürlerinde yapılan değişiklikler ve bir iç kontrol değerlendirmesinin sonuçları ile analitik inceleme prosedürlerinin sonuçları gibi konuları ve etkenleri dikkate almalıdır.

**Örneklemin Seçilmesi:**
Yaygın olarak kullanılan dört örnekleme yöntemi vardır:

*İstatistiksel Örnekleme Yöntemleri:*

- *Rassal (tesadüfî) örnekleme:* Popülasyondaki örneklem birimlerinin bütün kombinasyonlarının seçilme şanslarının eşit olmasını sağlar.
- *Sistematik örnekleme:* Örneklem birimlerinin, seçmeler arasında belirli sabit bir aralık bırakılarak ve ilk aralığın rastgele bir

başlangıç noktasından başlatılarak seçildiği örnekleme yöntemidir. Örnekleri arasında, popülasyondaki her münferit parasal değere (örneğin, 1YTL) eşit seçilme şansı verilen Parasal Birim Örneklemesi veya Değer Ağırlıklı seçme yöntemi sayılabilir. Münferit parasal birim normalde ayrıca incelenemediğinden dolayı, inceleme için, o parasal birimi içeren öğe seçilir. Bu yöntem, sistemli bir şekilde, daha büyük miktarlar lehine seçime ağırlık verir, fakat buna rağmen her parasal birime eşit seçilme fırsatını da tanır. Başka bir örnek de, her (n)inci birimin seçilmesidir.

*İstatistiksel Olmayan Örnekleme Yöntemleri:*

- *Gelişigüzel (Haphazard) örnekleme:* Denetçinin örneklemi yapısal bir teknik kullanmadan, fakat bilinçli yanlılıklardan veya önkestirimlerden kaçınarak seçtiği örnekleme yöntemidir. Bununla birlikte, popülasyon hakkında bir sonuca varmak için, gelişigüzel örneklemeyle seçilmiş bir örneklemin analiz sonuçlarına güvenmemek gerekir.
- *Yargısal (Judgemental) örnekleme:* Denetçinin örneklem üzerinde belirli bir yanlılık (bias; örneğin, belirli bir değerin üzerindeki bütün örneklem birimleri, belirli bir tipteki istisnalar için bütün örneklem birimleri, bütün eksi değerli olanlar, bütün yeni kullanıcılar, vb.) uyguladığı örnekleme yöntemidir. Ancak yargısal örneklemin istatistiksel temellere dayanmadığı ve sonuçların, örneklemin popülasyonu temsil edici nitelikte olmasının muhtemel olmaması nedeniyle popülasyonun tamamı üzerine yaygınlaştırılmaması gerektiği not edilmelidir.

Denetçinin, örneklem birimlerini, test edilen özellikler açısından örneklemin popülasyonu temsil edici nitelikte olmasının beklenebileceği bir şekilde seçmesi gerekir (yani, istatistiksel örnekleme yöntemlerini kullanarak). Denetimin bağımsızlığını sağlamak için denetçi, popülasyonun tam ve eksiksiz olmasını sağlamalı ve örneklem seçimini kontrol etmelidir.

Bir örneklemin popülasyonu temsil edici nitelikte olması için, popülasyondaki bütün örneklem birimlerinin eşit veya bilinen bir seçilme şansı bulunmalıdır (yani, istatistiksel örnekleme yöntemleri). Yaygın kullanılan iki seçme yöntemi vardır: kayıtlara göre seçme ve nicel alanlara göre seçme (örneğin, parasal birimler).

*Kayıtlara göre seçme yöntemi* için yaygın olarak kullanılan yöntemler şunlardır:

- Rassal (tesadüfî) Örneklem (istatistiksel örneklem)
- Gelişigüzel Örneklem (istatistiksel olmayan örneklem)
- Yargısal Örneklem (istatistiksel olmayan örneklem; yanlı bir sonuca varma olasılığı yüksek)

*Nicel alanlara göre seçme yöntemi* için yaygın olarak kullanılan yöntemler ise şunlardır:

- Rassal (tesadüfî) Örneklem (parasal birimlere dayanan istatistiksel örneklem)
- Sabit Aralık Örneklemi (sabit bir aralık kullanılarak seçilen istatistiksel örneklem)
- Hücre Örneklemi (bir aralık içinde rastgele seçme yöntemi kullanılarak seçilen istatistiksel örneklem)

**Dokümantasyon:**
Denetim çalışma kâğıtları, örnekleme hedefini ve kullanılan örnekleme sürecini açıkça tanımlayan yeterli ayrıntı içermelidir. Çalışma kâğıtları, popülasyonun kaynağını, kullanılan örnekleme yöntemini, örnekleme parametrelerini (örneğin, rastgele başlama sayısı veya rastgele başlamanın elde edildiği yöntem, örnekleme aralığı), seçilen birimleri, yapılan denetim testlerinin ayrıntılarını ve ulaşılan sonuçları da göstermelidir.

**Örneklem Sonuçlarının Değerlendirilmesi:**
Her örneklem birimine, belirlenen denetim hedefi için uygun olan denetim prosedürlerini uyguladıktan sonra, denetçi, örneklemde tespit edilen muhtemel hatâları, bunların gerçekten hatâ olup olmadığını ve uygunsa, hatâların niteliğini ve sebebini tespit etmek amacıyla analiz etmelidir. Hatâ olarak değerlendirilenler için, kullanılan örnekleme yöntemi istatistiksel temellere dayanan bir yöntemse, hatâlar popülasyona uygun bir şekilde tahmin edilir.

Tespit edilen muhtemel hatâların gerçekten hatâ olup olmadığı incelenmeli ve belirlenmelidir. Denetçi hatâların niteliksel yönlerini değerlendirmelidir. Bunlar; hatânın niteliği, sebebi ve hatânın denetimin diğer aşamaları üzerindeki muhtemel etkilerini içerir. Bir otomatik sürecin bozulmasının sonucu olan hatâlar hatâ oranı üzerinde, genellikle, insan hatâsından daha geniş bir etkiye sahiptir.

Belirli bir örneklem birimi hakkında beklenen denetim bulgu ve delilleri elde edilemediği takdirde, denetçi, seçilen birim üzerinde alternatif prosedürleri uygulayarak yeterli denetim bulgu ve delilleri elde edebilir.

Denetçi, örneklem sonuçlarını popülasyona uygulamak için, örneklemi seçmek için kullandığı yönteme uygun bir tahmin yöntemi bulmalı ve kullanmalıdır. Örneklemin tahmini, popülasyondaki muhtemel hatâları ve kullanılan tekniğin belirsizliği nedeniyle tespit edilemeyebilecek hatâları, bulunan hatâların niteliksel yönleriyle birlikte tahmin etmeyi gerektirebilir.

Denetçi, popülasyondaki hatâların tolere edilebilir hatâ düzeyini aşıp aşmadığını tahmini popülasyon hatâsını tolere edilebilir hatâ düzeyiyle karşılaştırarak ve denetim hedefine uygun başka denetim prosedürlerinin sonuçlarını dikkate alarak belirlemeli ve değerlendirmelidir. Tahmini popülasyon hatâsı tolere edilebilir hatâ

düzeyini aşmışsa, denetçi, örnekleme riskini tekrar değerlendirmeli ve bu risk kabul edilemez düzeydeyse, denetim prosedürünü genişletmeyi ya da alternatif denetim prosedürleri uygulamayı düşünmelidir.

# Uygulama Önerisi 2100-11: Yaygın Etkili Bilişim Sistemleri (BS) Kontrollerinin Etkisi

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu-Yaygın Etkili BS Kontrollerinin Etkisi, Doküman G11'den uyarlanmıştır. Bahsi geçen BS BS Denetim kılavuzu ISACA tarafından Mart 2000'de yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, BS kontrollerini gözden geçirirken aşağıdaki önerileri dikkate almalıdırlar. Bu kılavuzun, bir BS denetim çalışması için gereken bütün prosedürleri yansıtmak gibi bir amacı yoktur; klavuz, sadece, ayrıntılı denetim planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumluluklarından oluşan bir temel öneriler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## I. KONTROLLER ÇERÇEVESİ:

**Tanımlar:**
*Uygulama kontrolleri:* Her bir bilgisayar temelli uygulama sistemi ile ilgili işlem ve verileri ifade eder ve bu sebeple bu tür her uygulamaya özgüdürler. Uygulama kontrollerinin, manuel veya programlanmış olsun, hedefleri; kayıtların bütünlük ve doğruluğu ile hem manuel hem de programlanmış süreçler sonucu yapılan girişlerin/kayıtların geçerliliğini garanti etmektir.

*Genel bilgisayar kontrolleri:* Uygulama kontrolleri dışında kalan, bilgisayar temelli uygulama sitemlerinin geliştirildiği, tutulduğu ve işletildiği ortam ile ilişkili olan, bu sebeple de tüm uygulamalar açısından uygulanabilir olan kontrollerdir. Genel kontrollerin hedefleri, uygulamaların uygun bir şekilde geliştirilmesi ve uygulanması, program ve veri dosyaları ile bilgisayar operasyonlarının bütünlüğünün/doğruluğunun garanti edilmesidir. Uygulama kontrolleri gibi genel kontroller de manuel veya programlanmış olabilir.

*Yaygın etkili (pervasive) BS kontrolü:* BS ortamının yönetilmesi ve izlenmesi için tasarlanmış olan ve bu sebeple BS ile ilişkili faliyetleri etkileyen genel kontrollerdir.

*Ayrıntılı BS kontrolleri:* BS sistemleri ve hizmetlerinin edinilmesi, uygulanması, teslimi ve desteği üzerindeki kontrollerdir. Bunlar uygulama kontrolleri ile yaygın etkili kontollere dahil edilmemiş bulunan genel kontrollerin toplamından oluşur.

Her BS denetimi için denetçiler, denetim çalışmalarını denetim hedefi ile ilgili risk alanlarına odaklamak için bütün bilgi sistemleri ve operasyonlarını etkileyen genel kontroller (yaygın etkili BS kontrolleri) ile daha özel bir seviyede işleyen kontrolleri (ayrıntılı BS kontrolleri) ayrıştırmalıdırlar. Aşağıda açıklanan kontrol çerçevesi denetçiye, bu odak noktasına erişmede yardımcı olacaktır.

**Yaygın Etkili BS Kontrolleri:**

Yaygın etkili BS kontrollerinin örnekleri arasında, COBIT'in[1] Planlama ve Örgütleme alanında ve İzleme alanında tanımlanan BS süreçleri üzerindeki kontroller sayılabilir; örneğin, "PO1 -Stratejik Bir BT Planı Tanımlamak" ve "M1 - Süreçleri İzlemek". Yaygın etkili BS kontrolleri, genel kontrollerin bir alt kümesi olup BS yönetimi ve izlemesi üzerinde odaklanan genel kontrollerden ibarettir.

Yaygın etkili *BS kontrolleri*nin etkisi, finansal sistemlerdeki uygulama kontrollerinin güvenilirliğiyle sınırlı değildir. Yaygın etkili BS kontrolleri,

[1] COBIT: Control Objectives for Information and Related Technology

- Program geliştirme
- Sistem uygulama
- Güvenlik yönetimi
- Yedekleme prosedürleri

üzerindekiler gibi ayrıntılı BS kontrollerinin güvenilirliğini de etkiler. BS'nin zayıf yönetimi ve izlemesi (zayıf yaygın etkili BS kontrolleri), denetçiyi, ayrıntılı düzeyde uygulanmak üzere tasarlanan kontrollerin etkisiz olması riskinin yüksek olasılık olduğu konusunda uyarmalıdır.

**Ayrıntılı BS Kontrolleri:**
Ayrıntılı BS kontrolleri, uygulama kontrolleri ile yaygın etkili BS kontrollerine dahil edilmemiş bulunan genel kontrollerden oluşur. Örnekler arasında:

- Yazılım paketlerinin uygulanması
- Sistem güvenlik parametreleri
- Felâket kurtarma planlaması
- Veri girdi onaylaması
- Hatâ raporu üretimi
- Kullanıcı hesaplarına erişim için geçersiz teşebbüsler olması halinde kullanıcı hesaplarının kilitlenmesi üzerindeki kontroller

sayılabilir.

Uygulama kontrolleri, ayrıntılı BS kontrollerinin bir *alt kümesi*dir. Örneğin veri girdi onaylaması, hem bir ayrıntılı BS kontrolü hem de bir uygulama kontrolüdür. Kurulum ve akreditasyon sistemleri (AI5) ise bir ayrıntılı BS kontrolüdür, fakat bir uygulama kontrolü değildir.

BS kontrolleri arasındaki ilişkiler aşağıda gösterilmektedir.

BS Kontrolleri

- Genel kontroller

- Yaygın etkili BS kontrolleri
- Ayrıntılı BS kontrolleri

• Uygulama kontrolleri

Denetçi, BS-dışı kontrollerin kapsam ve denetim prosedürleri üzerindeki etkisini de dikkate almalıdır.

**Yaygın Etkili ve Ayrıntılı BS Kontrollerinin Etkileşimi:**
COBIT çerçevesi, BS kontrol süreçlerini dört alana ayırır:

• Planlama ve Örgütleme

• İktisap (Edinim) ve Uygulama

• Teslim ve Destek

• İzleme

İktisap ve Uygulama (Acquisition and Implementation-AI) ve Teslim ve Destek (Delivery and Support-DS) alanlarındaki kontrollerin etkinliği, Planlama ve Örgütleme (Planning and Organization-PO) ve İzleme (Monitoring-M) alanlarında uygulanan kontrollerin etkinliğinden etkilenir. Yönetimin yetersiz planlama, örgütleme ve izleme yapması, iktisap, uygulama ve hizmet teslimi ve desteği alanlarındaki kontrollerin de etkisiz olacağını gösterir. Öte yandan, güçlü planlama, örgütleme ve izleme işlevleri, iktisap, uygulama ve hizmet teslimi ve desteği alanlarındaki etkisiz kontrolleri belirleyebilir ve düzeltebilir.

Örneğin, "Uygulama Yazılımını Edinmek ve Bakımını Yapmak" isimli süreç (COBIT süreç referans numarası AI2) üzerindeki etkin ayrıntılı BS kontrolleri:

• "Bir Stratejik BT Planı Tanımlamak" (COBIT süreç referans numarası PO1)

• "Projeleri Yönetmek" (COBIT süreç referans numarası PO10)

• "Kaliteyi Yönetmek" (COBIT süreç referans numarası PO11)

- "Süreçleri İzlemek" (COBIT süreç referans numarası M1)

süreçleri üzerindeki yaygın etkili BS kontrollerinin yeterliliğinden etkilenir.

Bir uygulama sistemi iktisabı denetimi, BS stratejisinin etkisinin, proje yönetimi yaklaşımının, kalite yönetiminin ve izleme yaklaşımının tanımlanmasını da içermelidir. Örneğin, proje yönetiminin yetersiz olduğu durumlarda, denetçi:

- belirli bir projenin etkin bir şekilde yönetildiğine ilişkin güvence elde etmek amacıyla ek çalışmalar yapmayı ve
- yaygın etkili BS kontrollerinde tespit edilen zayıflıkları yönetime rapor etmeyi

düşünmelidir.

Başka bir örnek de şudur: "Sistem Güvenliğini Sağlamak" süreci (COBIT süreç referans numarası DS5) üzerindeki etkin ayrıntılı BS kontrolleri:

- "BT Örgütlenmesi ve İlişkilerini Tanımlamak" (COBIT süreç referans numarası PO4)
- "Yönetim Hedefleri ve Yönü Bildirmek" (COBIT süreç referans numarası PO6)
- "Riskleri Değerlendirmek" (COBIT süreç referans numarası PO9)
- "Süreçleri İzlemek" (COBIT süreç referans numarası M1)

süreçleri üzerindeki yaygın etkili BS kontrollerinin yeterliliğinden etkilenir.

Bir sistemde (örneğin UNIX, Windows NT, RACF) güvenlik parametrelerinin yeterliliği hakkında bir denetim; yönetimin uyguladığı güvenlik politikalarının (PO6), güvenlik sorumlulukları dağılımının (PO4), risk değerlendirmesi prosedürlerinin (PO9) ve güvenlik politikalarına uyumun izlenmesi prosedürlerinin (M1) değerlendirilmesini içermelidir. Parametreler denetçinin "en iyi

uygulamalar"la ilgili görüşüne uymasa bile, bunlar, yönetimin tanımladığı risklerin ve bu risk düzeyinin nasıl ele alınması gerektiğini gösteren yönetim politikalarının ışığında yeterli kabul edilebilir. Denetim tavsiyeleri, risk yönetimi veya politikalarına ve ayrıntılı parametrelerin kendilerine yönelik olmalıdır.

## II. PLANLAMA:

### İlgili Yaygın Etkili BS Kontrolleri Yaklaşımı:

BS Denetiminin Planlanmasına İlişkin Denetim Kılavuzu, denetçinin denetlenen işlev üzerinde bir kontrol ön değerlendirmesi yapması gerektiğini belirtir. Bu ön değerlendirme, ilgili yaygın etkili BS kontrollerinin tanımlanması ve değerlendirilmesini içermelidir. Yaygın etkili BS kontrollerinin testi, yapılmakta olan belirli denetime göre farklı bir çevrimde gerçekleştirilebilir, çünkü bunlar niteliği gereği BS kullanımının pek çok farklı özelliklerini kapsarlar. Bu nedenle, denetçi, bu kontrolleri tanımlamak ve değerlendirmek için, bu alanda daha önce yapılmış bulunan denetim çalışmalarının sonuçlarının dayanak kabul edilip edilemeyeceğini de düşünmelidir. Denetim çalışması, yaygın etkili BS kontrollerinin tatmin edici olmadığını gösterdiği takdirde, denetçi, bu bulgunun denetim hedefine ulaşmak için planlanmış yaklaşım üzerindeki etkisini dikkate almalıdır:

- Güçlü yaygın etkili BS kontrolleri, bir denetçinin ayrıntılı BS kontrolleri hakkında elde edebileceği güvenceye katkıda bulunabilir.
- Zayıf yaygın etkili BS kontrolleri, güçlü ayrıntılı BS kontrollerini zayıflatabilir ya da ayrıntılı düzeydeki zayıflıkları daha da kötüleştirebilir.

### Yeterli Denetim Prosedürleri:

Yaygın etkili BS kontrollerinin denetim hedefi üzerinde önemli bir potansiyel etkiye sahip olduğu durumlarda, sadece ayrıntılı kontrolleri denetlemeyi planlamak yeterli olmaz. Yaygın etkili BS kontrollerini denetlemenin pratik veya mümkün olmadığı durumlarda, bu kapsam kısıtlaması rapor edilmelidir. Denetçi, denetim hedefine ulaşmaya

katkıda bulunacağı durumlarda, ilgili yaygın etkili BS kontrollerini test etmeyi planlamalıdır.

**İlgili Kontroller:**
İlgili yaygın etkili BS kontrolleri, görev için belirlenen belirli denetim hedefleri üzerinde bir etkisi bulunan BS kontrolleridir. Örneğin, denetim hedefinin belirli bir program kütüphanesindeki değişikliklere ilişkin kontrolleri rapor etmek olduğu durumlarda, güvenlik politikalarına (PO6) ilişkin yaygın etkili BS kontrolleri amaca uygun olacaktır, fakat teknolojik yönün tespitine (PO3) ilişkin yaygın etkili BS kontrolleri ilgili ve amaca uygun olmayabilir.
Denetimi planlarken, denetçi, yaygın etkili BS kontrolleri toplam popülasyonu içinde hangi kontrollerin belirli denetim hedefleri üzerinde bir etkisi olduğunu tanımlamalı ve tespit etmeli ve bunları denetimin kapsamına dahil etmek için planlama yapmalıdır. COBIT'in "Planlama ve Örgütleme" ve "İzleme" alanları için kontrol hedefleri, BS Denetçisinin ilgili yaygın etkili BS kontrollerini belirlemesine ve tanımlamasına yardımcı olabilir.

**Denetim Delilleri:**
Yaygın etkili BS kontrollerinin kaydedilmesi ve dokümante edilmesi gerekli olmayabilir, fakat BS Denetçisi, ilgili kontrollerin etkin bir şekilde işlediğine dair denetim bulgusu ve delili elde etmeyi planlamalıdır. Potansiyel testler, Denetim Çalışmasının Yapılması başlıklı bölümde açıklanmaktadır.

**İlgili Ayrıntılı BS Kontrolleri Yaklaşımı:**
Denetim çalışmasının yaygın etkili BS kontrollerinin tatmin edici olduğunu gösterdiği durumlarda, denetçi, ayrıntılı BS kontrolleri için planlanan test düzeyini azaltmayı düşünmelidir, çünkü güçlü yaygın etkili BS kontrolleriyle elde edilen denetim bulgu ve delilleri, bir denetçinin ayrıntılı BS kontrolleri hakkında elde edebileceği güvenceye katkıda bulunur.

BS denetim çalışmasının yaygın etkili BS kontrollerinin tatmin edici olmadığını gösterdiği durumlarda ise, denetçi, ilgili yaygın etkili BS kontrollerindeki zayıflıklara rağmen ayrıntılı BS kontrollerinin etkin bir şekilde işlediğine dair denetim bulguları ve delilleri elde etmek amacıyla ayrıntılı BS kontrollerini yeterince test etmelidir.

## III. DENETİM ÇALIŞMASININ YAPILMASI:

**Yaygın Etkili BS Kontrollerinin Test Edilmesi:**
Denetçi, ilgili yaygın etkili BS kontrollerinin denetim süresi içinde veya belirli bir anda etkin bir şekilde işlediğine dair güvence elde etmek için bu kontroller yeterince test edilmelidir. Test prosedürleri şunları içerebilir:

- Gözlem
- Destekleyici (doğrulayıcı) sorgular
- İlgili dokümantasyonun incelenmesi (politikalar, standartlar, toplantı tutanakları, vb.)
- Yeniden yapma (örneğin BDDT'leri[2] kullanarak)

İlgili yaygın etkili BS kontrolleri testi bunların tatmin edici olduğunu gösterdiği takdirde, denetçi, denetim hedefine doğrudan yönelik olan ayrıntılı BS kontrolleri üzerinde planlanmış denetim çalışmasıyla devam etmelidir. Bu testin düzeyi, yaygın etkili BS kontrolleri tatmin edici olmasaydı uygun olacak olan test düzeyinden daha düşük olabilir.

## IV. RAPORLAMA:

**Yaygın Etkili BS Kontrolü Zayıflıkları:**
Denetçinin yaygın etkili BS kontrollerinde zayıflıklar bulduğu durumlarda, bu alanların nasıl değerlendirileceği kararlaştırılan iş kapsamında özel olarak tanımlanmış olmasa bile, bu zayıflıklar yönetime rapor edilmelidir.

---

[2] BDDT: Bilgisayar Destekli Denetim Teknikleri

**Kapsam Kısıtlamaları:**
Yaygın etkili BS kontrollerinin ayrıntılı BS kontrollerinin etkinliği üzerinde önemli bir etki yapabileceği ve yaygın etkili BS kontrollerinin denetlenmediği durumlarda, denetçi bu durumu, bunun denetim bulguları, sonuçları ve tavsiyeleri üzerindeki potansiyel etkilerine dair bir açıklamayla birlikte nihai raporunda yönetime bildirmelidir. Örneğin, bir denetçi bir paket çözümün iktisabına ilişkin denetim hakkında rapor yazıyorsa, fakat kurumun BS stratejisini görmemişse, raporunda, BS stratejisinin kendisine verilmediğini veya mevcut olmadığını belirtmelidir. Gerekirse denetçi, bunun denetim bulguları, sonuçları ve tavsiyeleri üzerindeki potansiyel etkisini rapor etmelidir. Örneğin, paket çözümün iktisabının BS stratejisine uygun ve uyumlu olup olmadığını ve işletmenin geleceğe yönelik planlarına destek olup olmayacağını söylemenin bu nedenle mümkün olmadığı açıklanabilir.

# Uygulama Önerisi 2100-12: Bilişim Sistemleri (BS) Faaliyetlerinin Başka Kurumlara Yaptırılması

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu-BS Faaliyetlerinin Başka Kurumlara Yaptırılması, Doküman G4'ten uyarlanmıştır. Bahsi geçen BS Denetim kılavuzu ISACA tarafından Eylül 1999'da yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, dışarıya yaptırılan BS faaliyetlerini denetlerken aşağıdaki önerileri dikkate almalıdırlar. Bu kılavuzun, dışarıya yaptırılan BS faaliyetlerinin denetlenmesiyle ilgili kapsamlı bir güvence veya danışmanlık görevi için gereken bütün prosedürleri yansıtmak gibi bir amacı yoktur; klavuz, sadece, ayrıntılı denetim planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumluluklarından oluşan bir temel öneriler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

**Denetimi Yapmadan Önce Değerlendirilmesi Gereken Mülahazalar**

**1.** İç Denetim Yöneticisi (Cheif Audit Executive-İDY) iç denetim biriminin, başka bir kuruma yaptırılan Bilişim Sistemleri (BS) faaliyetlerinde denetim çalışması yapmak ve ilişkili risklere maruziyet düzeyini değerlendirmek için bağımsız[1] ve yetkin

[1] *Bağımsızlık,* denetçinin ilgili uygulama sisteminin geliştirilmesi, edinilmesi, uygulanması veya sürdürülmesi gibi işlerde görev almamış olmasıdır.

denetim kaynaklarına sahip olup olmadığını veya bu tip kaynaklara erişim olanağının bulunup bulunmadığını tespit etmelidir.

2. Bir dış kaynak hizmetleri sağlayıcısını denetleme hakları çoğu zaman belirli ve açık değildir. Aynı şekilde uygunluk denetimi sorumluluğu da çoğu zaman açık ve belirli değildir. İDY ve/veya onun tayin ettiği bir denetçi, Hukuk Birimi, Sözleşme Yönetim Birimi ve/veya başka bir sorumlu birimle birlikte, dış kaynaktan temin sözleşmesinin ilgili hizmet sağlayıcısının denetimine ne ölçüde izin verdiğini tespit etmeli ve bu hükmün yeterli olup olmadığını değerlendirmelidir. Gerekirse uzman hukukçulardan görüş ve tavsiye de alınmalıdır.

3. İDY ve/veya onun tayin ettiği denetçi, ilgili hizmet sağlayıcısının kendi iç denetçilerinin ya da ilgili hizmet sağlayıcısının tayin ettiği bağımsız bir üçüncü şahsın yaptığı BS denetim çalışmalarının potansiyel güvenilirliğini de değerlendirmelidir. Denetim çalışmasına başlanmadan önce, denetim yapma hakkı ve/veya başka bir şahsın yapmış olduğu denetim çalışmasına güvenilip güvenilemeyeceği belirlenmelidir.

**Planlama Mülâhazaları:**

1. **Durum Tespiti:**
   Denetçi, dış kaynaktan temin edilen hizmetlerin niteliği, zamanlaması ve kapsamını anlamalı ve bilmelidir. Denetçi, hizmet kullanıcısının "üçüncü tarafların görevlerinin ve sorumluluklarının açıkça tanımlanmasını, bunlara uyulmasını ve bunların koşullara uygun olmaya devam etmesini sağlamak" olarak ifade edilen iş koşuluyla (COBIT[2] Üst Düzey Kontrol Hedefi DS2) ilgili olarak hangi kontrolleri uyguladığını belirlemelidir.

[2] COBIT: Control Objectives for Information and Related Technology

Dış kaynaktan temin edilen hizmetlerle ilgili *riskler* tanımlanmalı ve değerlendirilmelidir.

Denetçi, hizmet kullanıcısının yaptığı kontrollerin, iş hedeflerine ulaşılacağı ve istenmeyen olayların önleneceği veya tespit edileceği ve düzeltileceği konusunda makul bir güvence sunup sunmadığını ve hangi oranda sunduğunu da değerlendirmelidir.

2. **Planlama:**
Denetçi, hizmet sağlayıcısı için hazırlanan önceki denetim raporlarını değerlendirmeli ve planlama sırasında elde ettiği bilgileri dikkate alarak, hizmet sağlayıcısının ortamına uygun denetim hedeflerine ulaşmak için gereken bilişim sistemleri denetim çalışmasını planlamalıdır.

Denetim hedefleri, hizmet sağlayıcısına bildirilmeden önce, hizmet kullanıcısının yönetimiyle birlikte kararlaştırılmış olmalıdır. Hizmet sağlayıcısının denetim hedeflerinde talep edebileceği *değişiklikler* de, hizmet kullanıcısının yönetimiyle birlikte kararlaştırılmalıdır.

Denetçi, denetim çalışması hizmet kullanıcısının kendi ortamında yapılacakmış gibi, bilişim sistemleri denetim çalışmasını ilgili meslekî denetim standartlarına uygun bir şekilde planlamalıdır.

**Denetimin Yapılması:**

1. **Denetim Delili Koşulu:**
Denetim çalışması, ilgili hizmet, hizmet kullanıcısının kendi BS ortamında sağlanıyormuş gibi yapılmalıdır.

2. **Hizmet Sağlayıcısıyla Mutabakat:**
Denetçi, aşağıda sayılan konuları dikkate almalıdır:

   - Hizmet sağlayıcısı ile hizmet kullanıcısı arasında resmî bir sözleşmenin bulunup bulunmadığı.

- Dış kaynaktan temin sözleşmesinde, hizmet sağlayıcısının kendi faaliyetlerine ilişkin bütün kanuni koşulları yerine getirmekle ve hizmet kullanıcısı adına yapacağı iş ve işlevlere ilişkin bütün kanunlara ve mevzuata uymakla yükümlü olduğunu açıkça belirten bir maddenin bulunup bulunmadığı.
- Dış kaynaktan temin sözleşmesinde, hizmet sağlayıcısının yapacağı faaliyetlerin hizmet kullanıcısının kendisi tarafından yapılmış gibi kontrol ve denetimlere tâbi olduğunun belirtilip belirtilmediği.
- Hizmet sağlayıcısıyla yapılan sözleşmeye *denetim erişim hakları*nın da dahil edilip edilmediği.
- Performans izleme prosedürlerini içeren *Hizmet Düzeyi Sözleşmeleri*nin (Service Level Agreements-SLAs) bulunup bulunmadığı.
- Hizmet kullanıcısının *güvenlik* politikalarına uyulup uyulmadığı.
- Hizmet sağlayıcısının *emniyeti suiistimal sigortası* düzenlemelerinin yeterli olup olmadığı.
- Hizmet sağlayıcısının uyguladığı *personel politikaları* ve *prosedürleri*nin yeterli olup olmadığı.

**3. Dış Kaynaktan Temin Edilen Hizmetlerin Yönetimi:**

Denetçi:

- SLA'lara uyumu izlemek için kullanılan bilgilerin toplanmasına yönelik *iş süreçleri*nin uygun bir şekilde kontrol edilmediğini,
- SLA'lara uyulmaması halinde, hizmet kullanıcılarının çözüm aradığını ve düzeltici işlemlerin dikkate alındığını,
- Kararlaştırılan hizmet düzeyine ulaşıldığını,
- Hizmet kullanıcısının verilen hizmetleri izlemek ve incelemek için yeterli yetkinlik ve kapasiteye sahip olduğunu doğrulamalıdır.

4. **Kapsam Kısıtlamaları:**
   Hizmet sağlayıcısının denetçiyle işbirliği yapmak istememesi durumunda, denetçi konuyu hem hizmet kullanıcısının yönetimine hem de İDY'ye bildirmelidir.

**Raporlama:**
Denetçi, denetim çalışması bittikten sonra, hedeflenen hizmet alıcılarına uygun formda bir rapor sunmalıdır.

Denetçi, yayımlamadan önce raporu hizmet sağlayıcısıyla tartışmayı düşünmelidir, fakat denetçi nihai raporunu hizmet sağlayıcısına sunmaktan sorumlu olmamalıdır. Eğer hizmet sağlayıcısı raporun bir suretini alacaksa, bu suret, normal olarak, hizmet kullanıcısının yönetimi tarafından ona gönderilmelidir.

Rapor, denetçinin veya hizmet kullanıcısı yönetiminin uygulamayı kararlaştırdığı dağıtım sınırlamalarını da açıkça belirtmelidir. Örneğin, hizmet sağlayıcısı, denetçinin kurumunun ve gerekirse hizmet kullanıcısının iznini almadan, hizmet sundukları diğer kullanıcılarına rapor suretlerini verme hakkına sahip olmamalıdır. Denetçi, üçüncü taraflara karşı sorumlu olunmadığına dair bir ifadeyi de rapora koymayı düşünmelidir.

Denetim raporu, denetim erişim haklarının reddedilmesi ve tanınmaması durumundaki kapsam kısıtlamasını açıkça tanımlamalı ve bu kısıtlamanın denetim üzerindeki etkisini açıklamalıdır.

**İzleme Faaliyetleri:**
Denetçi, denetim hizmet kullanıcısının kendi ortamında yapılmış gibi, hem hizmet kullanıcısından hem de hizmet sağlayıcısından daha önceki ilgili bulgular, sonuçlar ve tavsiyeler hakkında gerekli bilgileri talep etmelidir. Denetçi, hizmet sağlayıcısının uygun düzeltici önlemleri zamanında uygulayıp uygulamadığını tespit etmelidir.

# Uygulama Önerisi 2100-13: Üçüncü Tarafların Bir Kurumun Bilişim Teknolojileri (BT) Kontrolleri Üzerindeki Etkisi

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu- Üçüncü Tarafların Bir Kurumun BT Kontrolleri Üzerindeki Etkisi, Doküman G16'dan uyarlanmıştır. Bahsi geçen BS Denetim kılavuzu ISACA tarafından Mart 2002'de yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, üçüncü tarafların bir kurumun BT kontrolleri üzerindeki etkisi hakkında bir denetim çalışması yaparken aşağıdaki önerileri dikkate almalıdırlar. Bu kılavuzun, üçüncü tarafların bir kurumun BT kontrolleri üzerindeki etkisini denetlenmesiyle ilgili kapsamlı bir güvence veya danışmanlık görevi için gereken bütün prosedürleri yansıtmak gibi bir amacı yoktur; klavuz, sadece, ayrıntılı denetim planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumluluklarından oluşan bir temel öneriler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## 1. ÜÇÜNCÜ TARAF HİZMET SAĞLAYICILARININ HİZMETLERİ:

Kurumlar, internet ve kurumsal intranetleri çok çeşitli amaçlarla

kullanmaktadırlar. Bu amaçlar arasında, çalışanlar, satıcılar ve müşterilerin mevcut ve/veya yeni insan kaynakları, finans, satış ve satın alma uygulamalarına erişimine olanak sağlamak da vardır. Bu erişim, pek çok durumda, bir veya birden fazla üçüncü taraf hizmet sağlayıcısı aracılığıyla sağlanmaktadır.

Üçüncü taraflar, aşağıda sayılanlar gibi hizmetleri verebilirler:

- Dahilî ağların internete bağlanabilirliği.
- Kurumun ortaklarına sanal özel ağlar veya extranet'ler aracılığıyla bağlanabilirlik.
- Müşterilere kablosuz teknoloji kullanarak bağlanabilirlik.
- İnternet sitesi geliştirme.
- İnternet sitesi bakım, yönetim ve izleme.
- İnternet sitesi güvenlik hizmetleri.
- Donanım için fiziksel yer temini (sunucu barındırma-co-location).
- Sistem ve uygulama erişimini izleme.
- Yedekleme ve kurtarma hizmetleri.
- Uygulama geliştirme, bakım ve barındırma hizmetleri (ERP sistemleri, e-ticaret sistemleri gibi).
- Nakit yönetimi, kredi kartı, sipariş işleme ve çağrı merkezi hizmetleri de dahil işle ilgili hizmetler.

## 2. ÜÇÜNCÜ TARAF HİZMET SAĞLAYICILARIN BİR KURUM ÜZERİNDE ETKİSİ:

Üçüncü taraf hizmet sağlayıcıları, bir kurumu (ortakları da dahil), süreçlerini, kontrollerini ve kontrol hedeflerini pek çok farklı düzeyde etkileyebilirler. Bu, aşağıdakiler gibi faktörlerden

(1) ERP: Enterprise Resource Planning (Kurumsal Kaynak Planlaması)

kaynaklanan etkileri içerir:

- Üçüncü taraf hizmet sağlayıcının ekonomik yeterliliği.
- Üçüncü taraf hizmet sağlayıcısının kendi iletişim sistemleri ve uygulamaları kanalıyla iletilen bilgilere erişim olanağı.
- Sistem ve uygulamaların müsaitliği.
- İşleme bütünlüğü (doğruluğu).
- Uygulama geliştirme ve değişim yönetimi süreçleri.
- Sistemlerin ve bilgi varlıklarının yedekleme kurtarma, beklenmedik durum planlaması ve artıklık (redundancy) kontrolü yoluyla korunması.

Üçüncü taraflar, bir kurumun kontrollerinde ve kurumun ilgili kontrol hedeflerine ulaşmasında kilit bir unsur haline gelebilirler. Denetçi, üçüncü tarafın BT ortamı, ilgili kontroller ve kontrol hedefleri konusunda verdiği hizmetleri değerlendirmelidir.

Üçüncü taraf hizmet sağlayıcılarını sunucu barındırma hizmetleri gibi sınırlı amaçlarla kullanan bir kurum, üçüncü taraf kontrollerine, kendi kontrol hedeflerine ulaşmada ilgili oldukları ölçüde güvenebilir. Bununla birlikte, üçüncü taraf hizmet sağlayıcılarını, mali muhasebe sistemlerinin ve e-ticaret sistemlerinin barındırılması gibi başka amaçlarla kullanan bir kurum, kendi kontrol hedeflerine ulaşmak için, üçüncü taraf hizmet sağlayıcısının kontrollerini tamamen ya da kendi kontrolleriyle birlikte kullanır.

Benzer şekilde, kurumun kendi kontrol hedeflerine ulaşma kabiliyeti, üçüncü tarafların uyguladığı kontrollerin nisbî etkinliği veya etkisizliğiyle kuvvetlendirilebilir ya da zayıflatılabilir. Zayıflıklar, aşağıdakiler de dahil pek çok kaynak ve sebepten kaynaklanabilir:

- Hizmetlerin üçüncü tarafa yaptırılmasından kaynaklanan

kontrol ortamı boşlukları.

- Kontrollerin etkisiz olmasına neden olan zayıf kontrol tasarımı.
- Kontrol işlevlerinden sorumlu personelin bilgi eksikliği ve/veya deneyimsizliği.
- Üçüncü tarafın uyguladığı kontrollere aşırı güvenmek (kurum içinde telâfi edici kontrollerin bulunmadığı durumlarda).

Kontrollerin eksik olması ve/veya kontrol tasarımı, işletimi veya etkinliğindeki zayıflıklar, aşağıdakiler gibi sonuçlara yol açabilir:

- Bilgi gizliliği ve mahremiyetinin ihlâli.
- Sistemlerin ihtiyaç olduğunda kullanıma hazır olmaması.
- Sistemler, uygulamalar veya verilere yetkisiz erişim ve değişiklikler.
- Sistemler, uygulamalar veya verilerde yapılan ve sistem arızalarına veya güvenlik sorunlarına, veri kaybına, veri bütünlüğü kaybına, veri koruma kaybına veya sistemlerin kullanıma hazır olmamasına yol açan değişiklikler.
- Sistem kaynakları ve/veya bilgi varlıkları kaybı.
- Yukarıda sayılan sebeplerin herhangi birisinden dolayı kurumun maliyetlerinde artışlar.

## 3. DENETÇİNİN UYGULAYACAĞI PROSEDÜRLER:

**Bilgi toplamak:**

Planlama sürecinin bir parçası olarak, denetçi, üçüncü tarafın sunduğu hizmetler ile kurumun kontrol ortamı arasında mevcut ilişkiyi anlamalı ve dokümante etmelidir. Denetçi, üçüncü taraf ile kurum arasındaki sözleşme, hizmet düzeyi sözleşmesi, politikalar ve prosedürler gibi konuları incelemeyi de düşünmelidir.

Denetçi:

- Üçüncü tarafın uyguladığı ve kurumun süreçleri ve kontrol hedefleri üzerinde doğrudan etkide bulunan süreçler ve kontrolleri dokümante etmeli;
- Her kontrolü, onun bütün kontrol ortamındaki yerini (dahilî veya haricî), kontrol tipini, kontrol işlevini (önleyici, tespit edici veya düzeltici) ve o işlevi yerine getiren kurumu (dahilî veya haricî) tanımlamalı;
- Üçüncü tarafın kuruma verdiği hizmetlerin riskini, kontrollerini ve kontrol hedeflerini değerlendirmeli;
- Üçüncü taraf kontrollerinin kurumun kendi kontrol hedeflerine ulaşma kapasitesi açısından önemini tespit etmeli;
- Kontrol ortamı hakkında anladıklarını sorgulama, gözlem ve işlemleri gözden geçirme gibi yollarla teyit etmelidir.

**Üçüncü taraf kontrollerinin rolünü değerlendirmek:**
Üçüncü tarafın kurumun kontrol hedefleri üzerindeki etkisi veya rolü önemli ise, denetçi, bunların tanımlandığı gibi işlev görüp görmediğini, etkin çalışıp çalışmadığını ve kuruma kontrol hedeflerine ulaşmasında yardımcı olup olmadığını tespit etmek için bu kontrolleri değerlendirmelidir.

**Tanımlanan kontrol zayıflıklarını değerlendirmek:**
Denetçiler, BT ortamındaki kontrollerin varlığı, tasarımı veya işletiminde zayıflıkların olasılığını (veya kontrol riskini) değerlendirmelidirler. Denetçi, hangi konularda kontrol zayıflığı bulunduğunu belirlemelidir.

Daha sonra, denetçi, kontrol riskinin önemli olup olmadığını ve bu riskin kontrol ortamı üzerinde hangi etkiyi yaptığını değerlendirmelidir.

Zayıflıkların tespit edilmesi hâlinde, denetçi, tespit edilen bu

zayıflıkların etkisini dengelemek için telâfi edici kontrollerin bulunup bulunmadığını belirlemelidir (bu telâfi edici ve dengeleyici kontroller kurumda, üçüncü taraf hizmet sağlayıcısında veya her ikisinde bulunabilir). Telâfi edici ve dengeleyici kontroller mevcut ise denetçi, bunların ilgili kontrol zayıflıklarının etkisini azaltıp azaltmadığını tespit etmelidir.

## 4. ÜÇÜNCÜ TARAF HİZMET SAĞLAYICILARLA SÖZLEŞMELER:

**Roller ve sorumluluklar:**

Kurum ile bir üçüncü taraf hizmet sağlayıcı arasındaki ilişki, imzalanmış bir sözleşmeyle belgelendirilmelidir. Bu sözleşme, kritik bir unsurdur ve tarafların her birinin eylem ve sorumluluklarını düzenleyen pek çok hüküm içerir.

Denetçi, üçüncü tarafın kuruma kontrol hedeflerine ulaşmak için yardım etmek konusundaki rolünü ve sorumluluğunu belirlemek amacıyla sözleşmeyi (muhtemelen kurumun hukuk danışmanının da yardımıyla) incelemelidir. Bir sözleşmenin nasıl incelenmesi gerektiği konusu bu kılavuzun kapsamı dışındadır; ancak, aşağıdaki liste, dikkate alınması gereken konuların örneklerini içermektedir:

- Üçüncü tarafın (kuruma, ortaklarına veya her ikisine) vereceği hizmetin düzeyi.
- Üçüncü tarafın alacağı ücretlerin makul olup olmadığı.
- Veri ve uygulama mahremiyeti ve gizliliğine ilişkin sorumluluklar.
- Sistem, iletişim, işletim sistemi, yardımcı program yazılımı, veri ve uygulama yazılımı erişim kontrolleri ve yönetimine ilişkin sorumluluklar.
- Varlıkların ve ilgili veri ve yanıtların izlenmesi (kurum ve üçüncü taraf) ve raporlama prosedürleri (rutin, olaya ilişkin raporlama).

- Veriler ve alan adları da dahil bilgi varlıklarının sahipliğine ilişkin koşullar.
- Değişiklik dokümantasyonu, *kaynak kodu* ve *yeddiemin sözleşmeleri* (escrow agreements) de dahil, üçüncü taraf hizmet sağlayıcının kurum için geliştirdiği özel programların sahipliğine ilişkin koşullar.
- Yedekleme ve kurtarma, beklenmedik durum planlaması ve artıklık kontrolü de dahil, sistem ve veri korumaya ilişkin hükümler.
- Denetim hakkı maddesi (üçüncü taraf hizmet sağlayıcının iç denetim personeliyle görüşme ve onların denetim çalışma kâğıtlarını ve raporlarını inceleme imkanı gibi konular da dahil).
- Sözleşmede ve ilgili dokümanlarda yapılan değişikliklerle ilgili müzakere, inceleme ve onay süreçleri (hizmet düzeyi sözleşmeleri ve prosedürleri gibi).

En azından, denetçi, üçüncü tarafın kurum adına üstlendiği kontrollere ilişkin sorumlulukların kapsamını belirlemek amacıyla sözleşmeyi incelemelidir. Bu süreç, tanımlanmış kontrollerin ve uyum izleme/raporlama sürecinin, bunların tasarımının ve işletim etkinliğinin yeterliliğini değerlendirmelidir.

**Kurumsal Yönetişim:**
Üçüncü taraf hizmet sağlayıcılar görevlendirilmiş olsa bile, ilgili kontrol hedeflerine ulaşma sorumluluğu yine de kurum yönetimindedir. Bu sorumluluğun bir parçası olarak, yönetim, üçüncü taraf hizmet sağlayıcıyla ilişkiyi ve üçüncü taraf hizmet sağlayıcının performansını düzenleyen bir sürece sahip olmalı ve bu süreci uygulamalıdır. Denetçi, bu sürecin unsurlarını tanımlamalı ve incelemelidir. Denetçi, yönetimin üçüncü taraf hizmet sağlayıcıyla bağlantılı riskleri tespit etmek için uyguladığı süreç, üçüncü tarafın verdiği hizmetler ve yönetimin bu iki kuruluş arasındaki ilişkiyi nasıl yönettiği gibi konuları incelemelidir.

Denetçinin kurumsal yönetişim incelemesi, yönetimin üçüncü taraf hizmet sağlayıcıların performansını sözleşmede öngörülen performans standartları veya kriterleriyle ve ilgili düzenleyici organların belirlediği standartlarla karşılaştırıp karşılaştırmadığı gibi konuları incelemeli ve değerlendirmelidir. Yönetişim süreci, aşağıda sayılanlar gibi konuların incelenmesini içermelidir:

- Üçüncü taraf hizmet sağlayıcının mali performansı.
- Sözleşme koşullarına uyum.
- Üçüncü tarafın, onun denetçilerinin ve/veya düzenleyici organların kontrol ortamında öngördüğü değişiklikler.
- Üçüncü tarafın denetçileri, danışmanları veya kişilerin yaptığı kontrol incelemelerinin sonuçları.
- Yeterli düzeyde sigortanın yaptırılması.

## 5. ÜÇÜNCÜ TARAF HİZMET SAĞLAYICI KONTROLLERİNİN İNCELENMESİ:

**Sözleşmeyle ilgili konular:**
Üçüncü taraf hizmet sağlayıcı kontrollerini incelerken, denetçi, kurum ile üçüncü şahıs hizmet sağlayıcı arasındaki akdi ilişkiyi ve üçüncü taraf hizmet sağlayıcının kendi kontrollerine ilişkin değerlendirme ve raporunu dikkate almalıdır.

Sözleşme hükümleri, bir denetçinin üçüncü taraf hizmet sağlayıcıdaki kontrolleri incelemesini engelleyebilir. Bu durumlarda, denetçi, bilişim sistemi kontrol ortamını değerlendirme imkanı üzerindeki bu kapsam sınırlamasını değerlendirmelidir.

**Bağımsız raporlar:**
Üçüncü taraf hizmet sağlayıcılar, kendi kontrolleri hakkında bağımsız kaynaklardan alınmış raporlar sunabilirler. Bu raporlar, hizmet bürosu denetim raporları veya başka kontrol bazlı raporlar formunda olabilir. Denetçiler, bu raporları, bilişim sistemi kontrol ortamındaki

kontrollere güven için dayanak noktası olarak kullanabilirler. Denetçi bir bağımsız raporu üçüncü taraf hizmet sağlayıcıdaki bilişim sistemi kontrollerine dayanak noktası olarak kullanmaya karar verirse, denetçi bu raporları aşağıdakileri tespit etmek amacıyla incelemelidir:

- Bağımsız tarafın vasıflı olması. Bu inceleme, bağımsız tarafın uygun meslekî sertifika veya lisansa sahip olup olmadığı, gerekli deneyime sahip olup olmadığı ve ilgili meslek kuruluşlarıyla ve (mümkünse) düzenleyici organlarla ilişkilerinin iyi düzeyde olup olmadığı konularını içerebilir.
- Bağımsız tarafın, üçüncü taraf hizmet sağlayıcıyla, kendi bağımsızlığını ve objektifliğini engelleyebilecek bir ilişkisinin bulunmaması.
- Raporun kapsadığı dönem.
- Raporun yeterli olup olmadığı (raporun ilgili sistemleri ve kontrolleri kapsayıp kapsamadığı ve bu çalışmayı kendisi yapsaydı denetçinin kapsama dahil edeceği alanlara ilişkin testleri içerip içermediği).
- Kontrollerde yapılan testin, denetçinin bağımsız tarafın yaptığı çalışmaya güvenmesi için yeterli olup olmadığı (kontrollerde yapılan testin uygulanan prosedürlerin niteliği, zamanlaması ve kapsamı açısından yeterli olup olmadığı).
- Raporun hizmet sağlayıcının sorumlulukları ile kullanıcı kurumun sorumluluklarını ayrı ayrı tanımlaması.
- Kullanıcı kurumun uygun kontrollerle ilgili kendi sorumluluklarına dikkat edip etmediği.

**Üçüncü taraf kontrollerinin test edilmesi:**
Denetçi, üçüncü taraf sağlayıcıda yapılan kontrolleri doğrudan doğruya incelemeye ve test etmeye karar verdiği takdirde, aşağıdakileri yapmalıdır:

- Görevi planlamak, görevin hedeflerini ve inceleme kapsamını belirlemek ve zamanlama, personel ihtiyaçları ve diğer konuları tespit etmek amacıyla, yönetimle ve uygunsa veya uygun görüldüğü takdirde, üçüncü taraf hizmet sağlayıcının iç denetim birimiyle birlikte çalışmak.
- Üçüncü taraf sistemleri ve varlıklarına erişim ve gizlilik gibi konuları ele almak.
- Bir denetim programı, bütçe ve görev planı hazırlamak.
- Kontrol hedeflerini doğrulamak.

Denetçi, bu saha çalışmasını bitirdikten sonra, test edilen kontrollerin işletme etkinliği hakkında bir sonuca varmalıdır. Denetçi, her kurum içinde kontrollerin etkinliğini ve kurum ile üçüncü taraf arasında kontrollerin etkileşimini incelemelidir. Çoğu durumda, kurum ile üçüncü taraf arasında kontroller konusunda bir örtüşme olur. Denetçi, kontrollerin birlikte ve toplu işletme etkinliğini tek tek etkinlikleriyle karşılaştırarak değerlendirmelidir.

Belirli bir hedef için, kurumların her ikisinde de kontrolün bulunmadığı ya da etkin çalışmadığı durumlar söz konusu olabilir. Ayrıca, bir kurumdaki kontrol gücünün diğer kurumdaki kontrol zayıflıklarıyla kısmen veya tamamen ortadan kalktığı durumlar da söz konusu olabilir. Bu tip durumlarda, denetçi, bu zayıflıkların genel kontrol ortamı üzerindeki ve prosedürlerin kapsamı üzerindeki etkisini değerlendirmelidir.

**Üçüncü tarafın iç denetçileri:**
Denetçi, üçüncü tarafın bir iç denetim bölümü bulunup bulunmadığını dikkate almalıdır. İç denetçilerin varlığı, kontrol ortamının gücünü artırabilir. Bir iç denetim bölümü varsa, denetçi onların kurumu etkileyen sistemler ve kontrollerle ilgili faaliyetlerinin kapsamını incelemeli ve değerlendirmelidir.

Denetçi, mümkünse, ilgili denetim raporlarını incelemelidir. Bu

raporları incelemenin mümkün olmadığı durumlarda, denetçi yapılan denetimlerin kapsamını, denetim kapsamındaki sistem ve kontrolleri ve tespit edilen önemli sorunları veya zayıflıkları tartışmalıdır. Üçüncü taraf, denetçinin bu raporlara erişmesine izin vermek istemiyorsa, denetçi, prosedürlerin kapsamı üzerindeki bu kısıtlamayı değerlendirmelidir.

Denetçi, iç denetim personelinin becerileri ve uzmanlığını değerlendirmeyi de dikkate almalıdır. Bu, söz konusu kişilerle görüşmeler yapmak ve onların çalışma planları, çalışma kâğıtları ve raporlarının incelenmesi gibi ilave prosedürler yoluyla yapılabilir.

## 6.ÜÇÜNCÜ TARAFLARIN TAŞERONLARI:

Denetçi, üçüncü tarafın sistemleri ve hizmetleri sunmak için taşeron kullanıp kullanmadığını belirlemelidir. Taşeronların kullanıldığı durumlarda, denetçi, bu taşeronların kurumla ilgili olan üçüncü taraf kontrolleri üzerindeki etkisini tespit etmek amacıyla bu taşeronların önemini incelemelidir.

Taşeronun kurumla ilgili kontroller üzerinde önemli bir etkisi yoksa, denetçi bu durumu kendi çalışma kâğıtlarında belirtmelidir. Taşeronun kurumla ilgili kontroller üzerinde önemli etkiye sahip olduğu tespit edilirse, denetçi, üçüncü tarafın, taşeronla ilişkisini yönetmek ve izlemek amacıyla kullandığı süreçleri değerlendirmelidir. Denetçi, bu değerlendirmeyi yaparken bu önerinin 4 ve 5. bölümlerini dikkate almalıdır.

## 7.RAPORLAMA:

Denetçinin raporu, hem kurum hem de üçüncü taraf içinde kontrollerde yapılan denetimin kapsamını göstermelidir. Denetçi, her kurum içinde mevcut kontrolleri, kontrol zayıflıklarını ve telâfi edici kontrolleri belirtmeyi ve tanımlamayı dikkate almalıdır. Denetim sonuçları ve tavsiyelerinin hangi oranda bildirileceğinin

tespitinde, kurum ile üçüncü taraf arasındaki ilişkiye bakılmalıdır. Bazı üçüncü taraflar, bu tavsiyeleri uygulamak istemeyebilir veya uygulayamayabilirler. Bu durumlarda, denetçi, üçüncü tarafta tespit edilen kontrol zayıflıklarına karşı kurumun uygulayabileceği telâfi edici ve dengeleyici kontroller tavsiye etmelidir.

# Uygulama Önerisi 2100-14: Denetim Delili Koşulu

Uluslararası İç Denetim Standartlarından
Standart 2100'ün Yorumu

## İlgili Standart

**2100 İşin Niteliği**
İç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

*Bu Uygulama Önerisi, Bilişim Sistemleri Denetim ve Kontrol Birliği (ISACA) Kılavuzu-Denetim Delili Koşulu, Doküman G2'den uyarlanmıştır. Bahsi geçen BS Denetim kılavuzu ISACA tarafından Aralık 1998'de yayımlanmıştır. Bu doküman, ISACA'nın izni ve onayıyla kullanılmıştır. Ancak bu Uygulama Önerisinin ISACA'nın yayımladığı Kılavuz/Prosedür'den farklı olduğu konularda, ISACA yapılan değişikliklerin doğruluğunu garanti etmez veya değişiklikleri onaylamaz.*

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, BS faaliyetleri konusunda bir denetim çalışması yaparken aşağıdaki önerileri dikkate almalıdırlar. Bu kılavuzun, BS faaliyetlerinin denetlenmesiyle ilgili kapsamlı bir güvence veya danışmanlık görevi için gereken bütün prosedürleri yansıtmak gibi bir amacı yoktur; klavuz, sadece, ayrıntılı denetim planlama çabalarını tamamlamak için gereken üst düzey denetçi sorumluluklarından oluşan bir temel öneriler demeti sunmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

## 1. PLANLAMA:

**Denetim Delili Türleri:**
Bilişim Sistemleri (BS) denetim çalışmasını planlarken denetçi, toplanacak denetim delillerinin tipini, bunların denetim hedeflerine ulaşmak için denetim delili olarak kullanımını ve bunların değişen güvenilirlik düzeylerini dikkate almalıdır. Dikkate alınması gereken konular arasında, denetim delilini sağlayanın bağımsızlığı ve nitelikleri de vardır. Örneğin, bağımsız bir üçüncü kişiden alınan destekleyici

deliller, denetlenen kurumun kendisinden alınan denetim delillerinden daha güvenilir olabilir. Fiziksel denetim delilleri, genellikle, bir kişinin yaptığı beyan ve açıklamalardan daha güvenilirdir.

Denetçinin kullanmayı düşünmesi gereken çeşitli *denetim delili türleri* arasında şunlar sayılabilir:

- Gözlemlenen süreçler ve fiziksel materyallerin varlığı.
- Dokümanter denetim delilleri
- Beyan ve açıklamalar
- Analizler

Gözlemlenen süreçler ve fiziksel materyallerin varlığı; faaliyetlerin, mekan ve tesislerin ve bilişim sistemleri fonksiyonlarının gözlemlenmesini içerebilir; örneğin:

- Şirket dışı bir depolama yerindeki araçların envanteri.
- Faal haldeki bir bilgisayar odası güvenlik sistemi.

Kâğıt veya başka ortamlarda bulunan *dokümanter denetim delilleri* şunları içerebilir:

- Veri çıkarma (data extraction) sonuçları
- İşlem kayıtları
- Program listeleri
- Faturalar
- Faaliyet ve kontrol günlükleri (logs)
- Sistem geliştirme dokümantasyonu.

Aşağıdakiler gibi, denetlenen kişilerin verdiği *beyan* ve *açıklamalar* denetim delili olabilirler:

- Yazılı politika ve prosedürler.
  - Sistem akış şemaları.

- Yazılı veya sözlü ifade ve beyanlar.

Bilgileri; karşılaştırmalar, simülasyonlar, hesaplamalar ve muhakeme yoluyla *analiz etmenin sonuçları* da denetim delili olarak kullanılabilir.

Örneğin:

- BS performansının, başka kurumlarla veya geçmiş dönemlerle referans noktalarına göre karşılaştırılması.
- Uygulamalar, işlemler ve kullanıcılar arasında hatâ oranı karşılaştırmaları.

**Denetim Delillerinin Mevcudiyeti:**
Denetçi, nicelik testi (substantive testing) ve eğer uygulanabilirse uyum testinin (compliance testing) niteliği, zamanlaması ve kapsamını belirlerken bilgilerin mevcut olduğu veya kullanıma hazır olduğu zamanı dikkate almalıdır. Örneğin, Elektronik Veri Değişimi (Electronic Data Interchange-EDI), Doküman Görüntü İşleme (Document Image Processing-DIP) ve hesaplama tabloları gibi dinamik sistemlerle işlenen denetim delillerine, dosya değişiklikleri kontrol altında değilse veya dosyalar yedeklenmemişse, belirli bir süre geçtikten sonra ulaşmak mümkün olmayabilir.

**Denetim Delillerinin Seçilmesi:**
Denetçi, denetim hedefinin önemi ve denetim delilini elde etmek için gereken zaman ve çaba ile uyumlu olarak, ulaşılabilecek en iyi denetim delillerini elde etmeyi ve kullanmayı planlamalıdır.

Sözlü ifade ve beyanlar şeklinde elde edilen denetim delilleri, denetim mütalaası veya sonucu açısından kritik öneme sahip ise, denetçi, bu ifade ve beyanlar için kâğıt veya başka ortamlara kayıtlı dokümanter teyitler elde etmeyi düşünmelidir.

## 2. DENETİM ÇALIŞMASININ YAPILMASI:

Denetim delilleri, bir mütalaa oluşturmak ya da denetçinin bulgu ve sonuçlarını desteklemek için yeterli, güvenilir, amaca uygun ve kullanışlı olmalıdır. Denetçinin görüşüne göre, elde edilen denetim delilleri bu kıstaslara uymuyorsa, denetçi ilave denetim delilleri toplamalıdır. Örneğin, bir program listesi, bu listenin üretim sürecinde fiilen kullanılan programı temsil ettiğini kanıtlamak için gereken diğer denetim delilleri de toplanana kadar yeterli bir denetim delili sayılmayabilir.

**Denetim Delillerinin Toplanması:**
Denetim delillerini toplamak için kullanılan prosedürler, denetlenen bilişim sistemine bağlı olarak değişir. Denetçi, denetim hedefi için en uygun olan prosedürü seçmelidir. Bu konuda, aşağıdaki prosedürler değerlendirilmelidir:

- Sorgulama
- Gözlem
- İnceleme
- Teyid
- Tekrar yapma
- İzleme

Yukarıdaki prosedürler, manuel denetim prosedürleriyle, bilgisayar destekli denetim teknikleriyle veya bu ikisinin bir kombinasyonuyla uygulanabilir. Örneğin:

- Veri giriş işlemlerinin bakiyesini almak için manuel kontrol toplamlarını kullanan bir sistem, uygun bir şekilde mutabakat yapılan ve açıklanan bir raporla, kontrol prosedürünün uygulandığı konusunda bir denetim delili sağlayabilir. Denetçi, bu raporu inceleyerek ve test ederek denetim delili toplamalıdır.
- Ayrıntılı işlem kayıtları, sadece makinede okunabilen formatta

olabilir ve bu durumda, denetçinin bilgisayar destekli denetim tekniklerini kullanarak denetim delili toplaması ve elde etmesi gerekir.

**Denetim Dokümantasyonu:**
Denetçinin topladığı denetim delilleri, denetçinin bulgu ve sonuçlarını desteklemek için uygun bir şekilde kaydedilmeli, belgelendirilmeli ve düzenlenmelidir.

## 3. RAPORLAMA:

Yeterli denetim delilinin toplanamadığına inandığı durumlarda denetçi, bu durumu denetim sonuçlarının bildirilmesine uygun bir tarzda açıklamalıdır.

# Uygulama Önerisi 2110-1: Risk Yönetim Sürecinin Yeterliliğinin Değerlendirilmesi

Uluslararası İç Denetim Standartlarından
Standart 2110'un Yorumu

## İlgili Standart

**2110 Risk Yönetimi**

İç denetim faaliyeti; önemli risk maruziyetlerini tespit edip değerlendirerek ve risk yönetimi ve kontrol sistemlerinin iyileştirilmesine katkıda bulunarak kuruma yardımcı olmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçilere, kurumun risk yönetim süreçlerinin yeterliliği konusunda yönetime ve denetim komitesine güvence verme sorumluluğu verilebilir. Bu sorumluluk, denetçinin, kurumun risk yönetimi sürecinin kurumun varlıklarını, itibarını ve devam etmekte olan faaliyet ve işlemlerini korumak için yeterli olup olmadığı konusunda bir inceleme yapıp görüş belirtmesini gerektirir. Bu uygulama önerisi, denetçinin kurumun risk yönetimi sürecinin yeterliliği hakkında bir görüş belirtirken dikkate alması gereken önemli risk yönetimi hedef ve amaçları hakkında bilgiler vermektedir. Bu uygulama önerisi, sadece kurumun risk yönetimi sürecinin etkinliğinin değerlendirilmesi ve rapor edilmesi konularını kapsar. Kontroller ve danışmanlık görevleri, diğer uygulama önerilerinde daha derinlemesine ele alınacaktır. Bu uygulama önerisi, bir kurumun risk yönetimi sürecinin stratejik açıdan önemli olan diğer süreçlere benzer bir tarzda ve şekilde değerlendirilebileceğini ve değerlendirilmesi gerektiğini savunmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Risk yönetimi, kurum *yönetiminin* temel sorumluluklarından biridir. İş hedeflerine ulaşabilmek için, yönetimin, kurum içinde sağlam risk yönetimi süreçlerinin bulunmasını ve kullanılmasını sağlaması gerekir. Denetim komitesi ve yönetim kurulu, uygun risk yönetimi süreçlerinin bulunup bulunmadığını ve bu süreçlerin yeterli ve etkin olup olmadığını tespit etmek konusunda denetleyici

bir rol oynar. İç denetçiler, yönetimin uyguladığı risk süreçlerinin yeterliliği ve etkinliğini inceleyerek, değerlendirerek, rapor ederek ve bu konuda iyileştirici önlemler önererek hem yönetime hem de denetim komitesine yardımcı olmalıdır. Kurumun risk yönetimi ve kontrol süreçlerinden yönetim, denetim komitesi ve yönetim kurulu sorumludur. Ancak, danışmanlık rolünü üstlenen iç denetçiler de, bu risklerin tanımlanması, değerlendirilmesi ve risk yönetimi yöntemlerinin uygulanması ve bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında yardımcı olabilir.

2. Kurumun risk yönetimi süreçleri hakkında değerlendirme ve incelemeler yapmak ve raporlar yazmak, normal olarak, *yüksek denetim önceliğine* sahip bir görevdir. Yönetimin uyguladığı risk süreçlerini değerlendirme görevi, denetçilerin denetim çalışmalarını planlamak için risk analizlerini kullanması gereğinden *farklıdır*. Bununla birlikte, yönetimin, denetim komitesinin ve yönetim kurulunun endişe duyduğu konuların tespiti de dahil, kapsamlı bir risk yönetim sürecinden elde edilen bilgiler, iç denetçilerin denetim faaliyetlerini planlamasına yardımcı olabilir.

3. Her kurum, risk yönetimi sürecini uygulamak için kendisine özgü bir yöntem seçebilir. İç denetçi, bu yöntemin denetim komitesi ve yönetim kurulu da dahil, kurum yönetimine katılan bütün önemli grup veya kişiler tarafından anlaşılıp anlaşılmadığını tespit etmelidir. İç denetçiler, kurumun risk yönetimi süreçlerinin genel yeterliliği hakkında bir görüş belirtebilmek için, kurumun risk yönetimi süreçlerinin beş temel hedefe uygun olduğundan emin olmalıdır. Bir risk yönetimi sürecinin *beş temel hedefi* şunlardır:

    - İş stratejileri ve faaliyetlerinden kaynaklanan risklerin belirlenmesi, tanımlanması ve öncelik sırasının tespit edilmesi,
    - Yönetimin, denetim komitesinin ve yönetim kurulunun, kurumun stratejik planlarının gerçekleştirilmesi amacına yönelik risk kabulü de dahil, kurumun kabul edebileceği risklerin düzeyini tespit etmesi,

- Riskleri yönetimin ve yönetim kurulunun kabul edilebilir bulduğu seviyelere düşürmek veya başka yollarla yönetmek amacına yönelik risk azaltma faaliyetleri ve çalışmalarının düzenlenmesi, yapılması ve uygulanması,
- Riskleri ve risk yönetimi amacına yönelik kontrollerin etkinliğini dönemsel olarak yeniden değerlendirmek için, devamlı izleme faaliyetlerinin yürütülmesi,
- Risk yönetimi süreçlerinin sonuçları hakkında, yönetime ve yönetim kuruluna dönemsel rapor verilmesi. Kurumun kurumsal yönetim süreçleri kapsamında; riskler, risk stratejileri ve kontroller hakkında hissedarlara ve diğer hak sahiplerine dönemsel bilgi verilmelidir,

4. İç denetçiler, muhtelif kurumların kendi risk yönetimi uygulamalarında kullandığı teknikler arasında önemli farkların olabileceğini bilmelidir. Risk yönetimi süreçleri, bir kurumun faaliyetlerinin niteliğine uygun tasarlanmalı ve uygulanmalıdır. Kurumun işle ilgili faaliyetlerinin büyüklüğüne ve karmaşıklık düzeyine bağlı olarak, risk yönetimi süreçleri:
   - resmî veya gayriresmî olabilir,
   - kantitatif veya sübjektif olabilir,
   - ilgili iş birimlerine tahsis edilebilir veya kurumsal düzeyde merkezîleştirilebilir.

Bir kurumun kullandığı sürecin, o kurumun kültürüne, yönetim tarzına ve iş hedeflerine uygun olması gerekir. Örneğin, kurumun türev araçlar kullanması veya sermaye piyasalarının başka gelişmiş ürünlerini kullanması hâlinde, kantitatif (nicel kıstaslara bağlı) risk yönetimi araçlarının kullanılması gerekir. Daha küçük ve daha az karmaşık olan kurumlar, kurumun risk profilini tartışmak ve dönemsel eylemlere girişmek için bir gayriresmî risk kurulundan yararlanabilir. Denetçi, seçilen yöntemin kurumun faaliyetlerinin niteliğine uygunluğunu ve kapsayıcılığını belirlemelidir.

5. İç denetçiler, risk yönetimi süreçlerinin yeterliliği yönünde bir görüş belirtebilmek için, risk yönetimi süreçlerinin beş temel hedefine uygunluğundan emin olmalı ve bu konuda yeterli kanıt toplamalıdır. Bu kanıtların toplanmasında, iç denetçi, aşağıda sayılan tiplerde denetim prosedürlerini dikkate almalıdır:

   - Kurumun kullandığı sürecin uygunluğunu ve endüstrinin en iyi uygulamalarını temsil edip etmediğini tespit etmek ve değerlendirmek için, risk yönetimi yöntemlerine ilişkin referans malzemeleri ve temel bilgileri araştırmak ve gözden geçirmek,
   - Bu riskleri önlemek, izlemek ve tekrar değerlendirmek için kullanılan kontrol prosedürlerini incelemek ve kurumu etkileyebilecek riskleri ve risk maruziyetlerini tespit etmek amacıyla, kurumun yaptığı işle ilgili mevcut sektör gelişmeleri, eğilimleri, bilgileri ve başka uygun bilgi kaynaklarını araştırmak ve gözden geçirmek,
   - Kurumun iş stratejilerini, risk yönetimi felsefesini ve yöntemini, risk alma istekliliğini ve riskleri kabulünü tespit etmek amacıyla, kurumsal politikaları, denetim komitesinin ve yönetim kurulunun tutanaklarını gözden geçirmek,
   - Yönetimin, iç denetçilerin ve dış denetçilerin ve bu raporları çıkartabilecek başka kaynakların daha önce düzenlediği risk değerlendirme raporlarını gözden geçirmek,
   - İş birimlerinin hedeflerini, ilgili riskleri ve kurum yönetiminin riskleri azaltma ve kontrol izleme çalışmaları ve faaliyetlerini tespit etmek amacıyla, üst yönetimle ve birim yönetimleriyle görüşmeler yapmak,
   - Risklerin azaltılmasının, gözlenmesinin, raporlanmasının ve ilgili kontrol faaliyetlerinin etkinliğini bağımsız bir gözle değerlendirmek amacıyla bilgileri özümsemek,
   - Hiyerarşik örgütlenmenin risk gözleme faaliyetleri için uygunluğunu değerlendirmek,

- Risk yönetimi sonuçlarıyla ilgili raporlamanın yeterliliğini ve zamanında yapılıp yapılmadığını gözden geçirmek,
- Yönetimin risk analizlerinin tam olup olmadığını ve risk yönetimi süreçleriyle anlaşılan sorunları gidermek için alınan tedbirlerin uygunluğunu gözden geçirmek ve iyileştirici eylemler önermek,
- Yönetimin uyguladığı iç değerlendirme süreçlerinin etkinliğini, gözlemlerle, doğrudan kontrol testleriyle ve gözlem prosedürleriyle, gözlem faaliyetlerinde kullanılan bilgilerin doğruluğuna ilişkin testlerle ve başka uygun tekniklerle tespit etmek,
- Risk yönetimi uygulamalarındaki zayıflıkları gösteren riskle ilgili sorunları incelemek ve gerekirse, bu konuyu yönetimle, denetim komitesi ve yönetim kuruluyla tartışmak. Denetçi, yönetimin kurumun risk yönetimi stratejisi veya politikalarına uygun olmayan ya da kurumun kabul edemeyeceği bir risk düzeyi kabul ettiğine inandığı takdirde, ek tavsiyeler için, "*Yönetimin Artık Riskleri Üstlenmesi*" başlıklı Standart 2600'e ve ilgili diğer standartlara bakmalıdır.

# Uygulama Önerisi 2110-2: İş Devamlılığı Sürecinde İç Denetçinin Rolü

Uluslararası İç Denetim Standartlarından
Standart 2110'un Yorumu

## İlgili Standart

**2110 Risk Yönetimi**
İç denetim faaliyeti, önemli risk maruziyetlerini tespit edip değerlendirerek ve risk yönetimi ve kontrol sistemlerinin iyileştirilmesine katkıda bulunarak kuruma yardımcı olmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bir kurumun iş devamlılığıyla ilgili faaliyetlerini değerlendirirken aşağıdaki önerileri dikkate almalıdır. Bir felâketin meydana gelmesinden sonra kurumun işine devam edebilmesi için uygulanması gereken pek çok süreç vardır. Kapsamlı bir planın geliştirilmesi; felâketin potansiyel etkisinin ve sonuçlarının değerlendirilmesi ve risklerin anlaşılmasıyla başlar. (İş devamlılığını sağlama süreci, diğer unsurların yanı sıra, iş devamlılığı ve felâket sonrası toparlanma planlarını da kapsar.) Bu planlar, kurumun ihtiyaçlarına uygun olmalarını sağlayacak bir şekilde yapılmalı, sürdürülmeli, sınanmalı ve denetlenmelidir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Doğal âfetler, kazalar veya kasdî suç eylemleri işte *kesintilere* neden olabilir. Bu kesintilerin önemli mali ve fiilî sonuçları olabilir. Denetçiler, kurumun iş kesintilerine karşı hazır olup olmadığını değerlendirmelidir. Kapsamlı bir plan; âcil durum tedbir prosedürlerini, alternatif iletişim sistemleri ve tesislerini, bilgi sistemleri yedeklemesini, felâket sonrası toparlanma planlarını, işe etki değerlendirmesini ve işi eski hâline getirme planlarını, elektrik, su gibi kamu hizmetlerini tekrar devreye alma prosedürlerini ve kurumun âcil bir duruma veya felâkete karşı hazır olmasını sağlamak için gereken idame prosedürlerini içerir.

2. İç denetim faaliyeti, kurumun bir felâkete hazır olup olmadığı konusunda üst yönetime sürekli bilgi vermek amacıyla, kurumun iş devamlılığı planlama sürecini düzenli olarak değerlendirmelidir.

3. Kurumların çoğu, bir felâketin veya öngörülmeyen başka bir olayın vukuu hâlinde normal iş süreçleri ve faaliyetlerinde bir kesinti veya uzun süreli bir gecikme beklemez. Pek çok iş uzmanı, sorunun bir felâketin *olup olmayacağı değil, ne zaman olacağı* olduğunu söyler. Zaman içinde, bir kurum, bilgi kaybına, mallarına (maddi veya maddi olmayan) erişim kaybına veya personelin hizmet edememesine yol açan bir olayla karşılaşacaktır. Bu nedenle, bu tür potansiyel risklerin tanımlanması ve iş devamlılığı planlamasının yapılması bir kurumun risk yönetim sürecinin tamamlayıcı bir parçasıdır. Bu kayıp ve zararları asgarîye indirmek ve kurumun hayatî iş fonksiyonlarının devamlılığını sağlamak için önceden planlama yapmak gerekir. Bu planlama, kurumun felâket hâlinde kurumla menfaat ilişkisi olan herkese kabul edilebilir düzeyde hizmet vermeyi sürdürmesine olanak sağlayacaktır.

4. İş kurtarmanın yaşamsal unsurlarından biri de, güncel ve kapsamlı bir felâket sonrası toparlanma planının mevcut olmasıdır. İç denetçiler, kurumun felâket kurtarma planlamasında bir rol oynayabilir. Bu konuda, iç denetim birimi (a) risk analizine yardımcı olabilir, (b) hazırlandıktan sonra planın yeterli kapsama sahip olup olmadığını ve tasarımını değerlendirebilir, (c) planın güncel tutulmasını sağlamak amacıyla dönemsel olarak güvence görevleri yerine getirebilir.

**Planlama:**

5. Kurumlar, risk yönetim ve kontrol süreçlerinin değerlendirilmesi ve operasyonların analizi konusunda iç denetçilere güvenir. İç denetçiler, kurumun genel iş operasyonlarını ve bireylerin fonksiyonlarını ve bunların birbirleriyle ilişki ve bağlantılarını öğrenir ve kavrar. Bu durum, iç denetim faaliyetini, hazırlama

süreci sırasında felâket sonrası toparlanma planının değerlendirilmesi için çok değerli bir kaynak hâline getirir.

6. İç denetim birimi, kurumun iç ve dış ortamının ve çevresinin değerlendirilmesine de yardımcı olabilir. Göz önüne alınabilecek iç faktörler arasında yönetimde değişim/devir hızı ve bilgi sistemleri ve kontrollerinde değişiklikler ve önemli projeler ve programlar sayılabilir. Dış faktörler arasında ise, dış mevzuatta ve iş ortamında değişiklikler ve pazarlar ve rekabet koşulları, uluslararası mali ve ekonomik koşullar ve teknolojilerdeki değişiklikler sayılabilir. İç denetçiler, kilit iş faaliyetleriyle ilgili risklerin belirlenmesi ve tanımlanmasında ve kurtarma amaçlarına yönelik fonksiyon ve görevlerin öncelik sırasının tespitinde yardımcı olabilir.

**Değerlendirme:**

7. İç denetçiler, önerilen iş devamlılığı ve felâket sonrası toparlanma planlarının tasarımını, tam olup olmadıklarını ve genel yeterliliğini gözden geçirdiklerinde, objektif katılımcılar olarak katkıda bulunabilir. Denetçi, planın risk değerlendirme sürecine dahil edilmiş ve bu süreç kapsamında değerlendirilmiş bulunan operasyonları yansıtıp yansıtmadığını ve iç kontrol meselesine ve bununla ilgili tavsiyelere yeteri kadar yer verip vermediğini tespit etmek amacıyla planı inceleyebilir. İç denetçinin kurumun iş operasyonları ve uygulamaları hakkında kapsamlı bilgi sahibi olması, iş devamlılığı planının geliştirilmesi safhasında planın yapısını ve kapsamını değerlendirmesi suretiyle; felâket sonrası toparlanma sürecinde ise riskleri yönetmek ve etkin kontroller sağlamak için tavsiye edilenleri değerlendirmek suretiyle, kuruma yardımcı olmasını mümkün kılar.

**Dönemsel Güvence Denetimi Görevleri**

8. İç denetçiler, kurumun iş devamlılığı ve felâket sonrası toparlanma planlarını dönemsel olarak denetlemelidir. Bu denetimin amacı, planların olumsuz olaylardan sonra operasyon ve süreçlerin en

kısa zamanda tekrar başlatılmasını sağlamak için yeterli olup olmadığını ve planların mevcut iş-faaliyet ortamını yansıtıp yansıtmadığını tespit etmektir.

9. İş devamlılığı ve felâket sonrası toparlanma planları çok kısa zamanda güncelliğini kaybedebilir. Değişikliklerin gereğini yerine getirmek ve gereken tedbirleri almak, yönetimin görevinin olmazsa olmaz bir parçasıdır. Müdürler ve yöneticilerin değişmesinin ve sistem konfigürasyonları, arayüzler ve yazılımlardaki değişikliklerin bu planlar üzerinde büyük bir etkisi olabilir. İç denetim faaliyeti, (a) toparlanma planının zaman içinde meydana gelebilecek önemli değişikliklere cevap verebilecek bir yapıya sahip olup olmadığını tespit etmek ve (b) revize edilen planın kurum içinden ve dışından uygun kişilere bildirilmesini sağlamak amacıyla, toparlanma planını incelemelidir.

10. Denetim sırasında, iç denetçiler şunları göz önüne almalıdır:

    - Bütün planlar güncel midir? Planların güncellenmesi için prosedürler mevcut mudur?
    - Planlar, bütün hayatî iş fonksiyonları ve sistemlerini kapsıyor mu? Kapsamıyorsa, kapsamama gerekçeleri belirtilmiş mi?
    - Planlarda, iş kesintisi riskleri ve bunun muhtemel sonuçları dikkate alınmış mı?
    - Planlar tam olarak yazılı hâle getirilmiş mi ve kurum politika ve prosedürlerine uygun mu? Fonksiyonel sorumluluklar belirlenmiş mi?
    - Kurum, planları uygulama kapasitesine sahip mi ve uygulamaya hazır mı?
    - Planlar, sonuçlar esas alınarak test ediliyor ve gözden geçiriliyor mu?
    - Planlar uygun ve emniyetli bir şekilde saklanıyor mu? Planların

yeri ve planlara erişim yetkileri yönetim tarafından biliniyor mu?

- Personel, alternatif tesislerin (yedekleme tesisleri) yerini biliyor mu?
- Planlar, mahallî âcil durum servisleriyle eşgüdümü öngörüyor mu?

**Bir Felâket Durumunda İç Denetçinin Rolü:**

11. Bir felâket hâlinde iç denetçilerin derhal yerine getirmeleri gereken önemli görevleri vardır. Bir kurum, felâket durumunda daha kırılgan ve saldırıya daha açık hâle gelir ve bu durumdan kurtulmaya çalışır. Bu toparlanma sırasında, iç denetçiler, operasyonların kontrolünü ve toparlanma faaliyetinin etkinliğini gözlemeli ve izlemelidir. İç denetim faaliyeti, iç kontrollerinin ve zarar azaltıcı tedbirlerinin iyileştirilmesi gereken yönlerini tespit etmeli ve kurumun iş devamlılığı planını geliştirici tavsiyelerde bulunmalıdır. İç denetim birimi, toparlanma faaliyetleri sırasında da *destek hizmeti* verebilir.

12. Felâketten sonra, genellikle birkaç ay süreyle, iç denetçiler, felâketten ve toparlanma faaliyetlerinden öğrenilen derslerin tanımlanmasında yardımcı olabilir. Bu tespit ve tavsiyeler, kaynakların kurtarılması amacına yönelik faaliyetleri geliştirebilir ve iş devamlılığı planının bir sonraki versiyonunun güncel olmasını sağlayabilir.

13. Son tahlilde, iç denetçilerin iş devamlılığı ve felâket sonrası toparlanma süreçlerine katılım ve katkı düzeyini, onların bilgileri, becerileri, bağımsızlığı ve objektifliği gibi etkenleri dikkate alarak tespit edecek olan kurumun üst yönetimidir.

# Uygulama Önerisi 2120.A1-1: Kontrol Süreçlerinin Değerlendirilmesi ve Rapor Edilmesi

Uluslararası İç Denetim Standartlarından
Standart 2120.A1'in Yorumu

## İlgili Standart

**2120.A1** Risk değerlendirmesinin sonuçlarına bağlı olarak, iç denetim faaliyeti, kurumun yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayan kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir. Bu değerlendirme: mali ve operasyonel bilgilerin güvenilirliğini, faaliyetlerin etkinlik ve verimlililiğini, varlıkların korunmasını, kanunlara, düzenlemelere ve sözleşmelere uyum konularını kapsamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bir kurumun iç kontrol sisteminin etkin olup olmadığını inceler ve değerlendirirken, bu konuda bir görüş belirtirken ve bu görüş ve sonuçları üst yönetime ve yönetim kuruluna rapor ederken aşağıdaki önerileri dikkate almalıdır. Yıl içinde yapılan denetim çalışması sonucunda, kontrol sistemini değerlendirmek ve bu konuda bir görüş belirtmek için yeterli bilgi toplanmalı ve elde edilmelidir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Yönetim kurulunun görevlerinden biri de, kurumun yönetişim süreçlerini kurmak ve uygulamak ve risk yönetimi ve kontrolü süreçlerinin etkin olduğuna dair güvenceler elde etmektir. Üst yönetimin rolü, bu risk yönetimi ve kontrolü süreçleri sisteminin kurulmasını, yönetilmesini ve değerlendirilmesini sağlamak ve denetlemektir. Kontrol süreçlerini kapsayan bu çok yönlü sistemin amacı, kurum içindeki insanlara, risklerin yönetilmesinde ve kurumun belirlenen ve açıklanan hedeflere ulaşılmasında yardımcı olmak ve destek vermektir. Daha somut olarak, bu kontrol

süreçlerinin, diğer şeylerin yanı sıra, aşağıdaki koşulların mevcut olmasını sağlamaları beklenir:

- mali ve operasyonel bilgilerin güvenilir ve doğru ve eksiksiz olması,
- faaliyetlerin verimli bir biçimde yürütülmesi ve etkin sonuçlara ulaşılması,
- varlıkların korunması,
- kurumun eylem ve kararlarının kanunlara, mevzuata ve sözleşmelere uygun olması.

2. Kurum müdürlerinin görev ve sorumluluklarından biri de, kendi alan ve bölümlerinde kontrol süreçlerini incelemek ve değerlendirmektir. İç ve dış denetçiler, kurumun sadece belirli seçilmiş faaliyet ve işlev alanlarında risk yönetimi ve kontrolü süreçlerinin etkinliği konusunda değişen derecelerde güvence verir ve sağlarlar.

3. Üst yönetim ve denetim komitesi, normal olarak, İç Denetim Yöneticisinin kontrol süreçlerinin yeterli, uygun ve etkin olup olmadığı hakkında bir sonuca varabilmek için yıl içinde yeterli denetim çalışması yapmasını ve mevcut bilgileri toplamasını bekler. İç Denetim Yöneticisi, kurumun kontrol sistemi hakkındaki genel sonucu ve görüşünü üst yönetime ve denetim komitesine bildirmelidir. Giderek artan sayıda kurum, kurum dışındaki hak sahiplerine sundukları yıllık veya dönemsel raporlara iç kontrol sistemine ilişkin bir yönetim raporunu da dahil etmektedir.

4. İç Denetim Yöneticisi, gelecek yıl için, kontrol süreçlerinin etkinliğini değerlendirmek için yeterli kanıt ve bilgi toplanmasına imkân veren bir *denetim planı önerisi* hazırlamalıdır. Bu plan, bütün önemli faaliyet birimleri ve iş fonksiyonları hakkında gereken bilgileri toplamak amacına yönelik denetim görevlerini veya benzeri başka prosedürleri içermelidir. Denetim planı, aynı

zamanda, son değişikliklerden veya beklenen değişikliklerden en çok etkilenen faaliyetlere ve birimlere de özel önem vermelidir. Koşullarda meydana gelen değişiklikler, piyasa veya yatırım şartlarından, devralma ve tasfiye işlemlerinden veya yeniden yapılanma ve yeni girişimlerden kaynaklanabilir. Önerilen plan, yıl içinde yönetim stratejilerinde veya dış koşullarda meydana gelen değişikliklere göre ya da kurumun hedefleri ve amaçlarına ulaşma konusundaki beklentilerde yapılan revizyonlara göre ayarlamaların yapılmasına imkân verecek şekilde esnek olmalıdır.

5. Önerilen denetim planını hazırlarken, İç Denetim Yöneticisi, başka kişilerin yapacağı ilgili işleri de dikkate almalıdır. Tekrarları ve verimsizliği asgarîye indirmek için, gelecek yıla ilişkin denetim planının kapsamının tespitinde, yönetimin ilgili kontrolleri ve kalite geliştirme ve artırma süreçlerini incelerken ve değerlendirirken planladığı veya yaptığı işlerin ve dış denetçilerin planladığı işlerin de dikkate alınması gerekir.

6. Son olarak, İç Denetim Yöneticisi, önerilen denetim planının kapsamını iki açıdan değerlendirmelidir: Çeşitli birimler açısından yeterlilik ve çeşitli işlem ve iş süreçleri tiplerinin plana dahil edilmesi. Önerilen denetim planının kapsamı kurumun kontrol süreçleri hakkında bir güvence vermek için yeterli değilse, İç Denetim Yöneticisi, beklenen eksiklikleri, bunların sebeplerini ve muhtemel sonuçlarını üst yönetime ve denetim komitesine bildirmeli ve açıklamalıdır.

7. İç denetimin görevi, pek çok ayrı ve bireysel inceleme ve değerlendirme esasında, kurumun kontrol sisteminin etkin ve verimli olup olmadığını değerlendirmektir. Bu inceleme ve değerlendirmeler, çoğunlukla, iç denetim görevleri, yönetimin kendi özdeğerlendirmeleri ve dış denetçinin çalışmalarından elde edilir ve toplanır. Görev ilerledikçe, iç denetçiler, tespit edilen kontrol eksikleri veya zayıflıklarının etki ve sonuçlarını azaltmak

veya düzeltmek amacıyla gereken tedbirlerin derhal alınmasını sağlamak amacıyla, bulgularını uygun yönetim kademelerine zamanında bildirmeli ve rapor etmelidir.

8. Kurumun kontrol süreçlerinin genel etkinliği hakkında bir değerlendirmede dikkate alınması gereken üç temel husus şunlardır:

   - Yapılan denetim çalışmasıyla ve toplanan başka inceleme ve değerlendirme bilgileriyle önemli eksiklik veya zayıflıklar tespit edilmiş midir?
   - Bu eksiklik veya zayıflıklar tespit edilmişse, bu tespit üzerine düzeltici veya iyileştirici tedbirler alınmış mıdır?
   - Bu tespitler ve sonuçları, kabul edilemez düzeyde iş risklerine yol açan yaygın bir sorunun bulunduğu sonucuna varılmasını gerektiriyor mu?

   Önemli bir kontrol eksikliği veya zayıflığının geçici bir süreyle oluşması, mutlaka, sorunun yaygın olduğu ve kabul edilemez bir iş riski taşıdığı anlamına gelmez. Tüm kontrol sisteminin etkinliğinin tehlike altında olup olmadığını ve kabul edilemez risklerin var olup olmadığını tespit ederken dikkate alınması gereken etkenler; tespit yolu ve şekli, etki düzeyi, sonuçların ve risk maruziyetinin seviyesidir.

9. İç Denetim Yöneticisinin kurumun kontrol süreçlerinin durumuna ilişkin raporu, üst yönetime ve denetim komitesine, genellikle yılda bir kere sunulmalıdır. Bu rapor, kontrol süreçlerinin kurumun hedeflerine ilişkin araştırmalarda oynadığı kilit rolü vurgulamalı ve iç denetimin yaptığı önemli işlere ve genel güvencenin verilmesinde kullanılan başka önemli bilgi kaynaklarına atıf yapmalıdır. Raporun görüş kısmında, normalde, olumsuz cümlelerle güvence verilir; örneğin, ilgili dönem için yapılan denetim çalışması ve toplanan diğer bilgiler, kontrol süreçleri ve sisteminde yaygın etkiye sahip herhangi bir önemli zayıflık olduğunu göstermemiştir. Kontrol eksiklikleri ve zayıflıkları önemli ve yaygınsa, raporun

güvence ile ilgili bölümü, tespit edilen net risk düzeyinde beklenen artışa ve riskin kurumun hedefleri üzerindeki etkisine bağlı olarak, şartlı veya olumsuz bir görüş içerebilir.

10. Yıllık raporun hedef kitlesi, üst düzey yöneticiler ve denetim komitesi üyeleridir. Bu okuyucuların denetim ve işle ilgili bilgileri farklı düzeylerde olduğu için, İç Denetim Yöneticisinin yıllık raporu açık, özlü ve bilgilendirici olmalıdır. Bu rapor, tüm okuyucular tarafından kolaylıkla anlaşılabilecek bir şekilde hazırlanmalı ve kaleme alınmalı ve onların bilgi ihtiyaçlarını karşılamayı amaçlamalıdır. Raporun okuyucular açısından değerini artırmak için, teknoloji ve bilgi güvenliği riskleri, farklı iş birimleri ve bölümleri arasında kontrol eksiklik veya zayıflıklarının dağılımı ve geçerli kanunlara veya mevzuata uyma konusundaki potansiyel güçlükler gibi, güncel kontrol sorunları ve trendleri hakkında bilgiler verilmeli ve iyileştirme amacına yönelik önemli öneriler açıklanmalıdır.

11. İç denetim faaliyetinin kontrol süreçlerinin durumunu değerlendirmek ve bu konuda güvence vermek amacına yönelik çalışmalarına yönelik "beklentiler arasında büyük farklar" olduğunu gösteren çok sayıda kanıt mevcuttur. Bu farklardan biri de, yönetimin ve denetim komitesinin iç denetim hizmetlerinin değerine ilişkin normalde hayli yüksek olan beklentileri ile iç denetçinin denetimin kapsamı üzerindeki pratik sınırlamalara ilişkin bilgisine dayanan ve objektif ve sağlam temelleri olan bir sonuca varabilmek için gereken yeterli kanıtın toplanıp toplanamayacağına ilişkin kuşkularından kaynaklanan daha mütevazı beklentileri arasında mevcuttur. İç Denetim Yöneticisi, rapor okuyucusunun beklentileri ile yıl içinde fiilen gerçekleşenler arasındaki muhtemel farkı dikkate almalıdır. İç Denetim Yöneticisi, raporu, farklı düşünüş tarzları ve modellerine hitap etmek ve kontrol süreçlerinin etkinliğinin incelenmesi ve denetlenmesi konusundaki sınırlama ve kısıtlamaları azaltmak veya bu fonksiyonun kapasitesini artırmak amacına yönelik önerilerde bulunmak için bir araç olarak kullanmalıdır.

# Uygulama Önerisi 2120.A1-2: Kontrol Süreçlerinin Yeterliliğini Değerlendirmede Kontrol Özdeğerlendirme Yönteminin Kullanılması

Uluslararası İç Denetim Standartlarından
Standart 2120.A1'in Yorumu

## İlgili Standart

**2120.A1** Risk değerlendirmesinin sonuçlarına bağlı olarak, iç denetim faaliyeti, kurumun yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayan kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir. Bu değerlendirme:

- mali ve operasyonel bilgilerin güvenilirliğini,
- faaliyetlerin etkinlik ve verimlililiğini,
- varlıkların korunmasını,
- kanunlara, düzenlemelere ve sözleşmelere uyum konularını kapsamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler ve müdürler, kurumun risk yönetimi ve kontrolü süreçlerinin yeterliliğini değerlendirmek için Kontrol Özdeğerlendirme (CSA) yöntemini kullanabilir. İç denetçiler, CSA programlarını, riskler ve kontroller hakkında bilgi toplamak, denetim planını yüksek riskler ve olağandışı alanlar üzerinde odaklamak ve işletme müdürleri ve çalışma ekipleriyle daha kapsamlı bir işbirliği kurmak amacıyla kullanabilir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Risk yönetimi ve kontrolü süreçlerinin kurulması, yönetilmesi ve değerlendirilmesini sağlamak ve denetlemek üst yönetimin görevidir. İşletme müdürlerinin sorumlulukları; kendi birimlerindeki

risk ve kontrollerin incelenmesi ve değerlendirilmesini de kapsar. İç ve dış denetçiler, kurumun risk yönetimi ve kontrolü süreçlerinin etkinliği hakkında farklı derecelerde güvence verir. Hem müdürler hem de denetçiler, uygulanan risk yönetimi ve kontrolü süreçlerini değerlendirmek ve bunların etkinliğini artıracak yollar bulmak amacına yönelik çabaları genişleten ve odak noktasını vurgulayan teknikler ve araçlar kullanmalıdır.

2. Özdeğerlendirme anketleri ve çalışma grubu faaliyetlerinden oluşan ve "*Kontrol Özdeğerlendirmeleri*" (CSA) olarak anılan yöntem, müdürlerin ve iç denetçilerin kontrol prosedürlerini değerlendirmek ve incelemek konusunda işbirliği yapmaları için faydalı ve etkin bir yaklaşım ve araçtır. Özü itibariyle, CSA, iş hedefleri ve risklerini kontrol süreçleriyle bütünleştirir ve birleştirir. Kontrol Özdeğerlendirmeleri, aynı zamanda, "*Kontrol/Risk Özdeğerlendirmeleri*" (CRSA) olarak da adlandırılmaktadır. CSA yöntemini kullananlar genellikle farklı teknikler ve formatlar kullanmasına rağmen, uygulanan programların çoğunluğu bazı temel özellikleri ve hedefleri paylaşmaktadır. Özdeğerlendirme yöntemini uygulayan bir kurum, bir iş birimi, fonksiyonu veya sürecine doğrudan doğruya katılan çalışma ekiplerinin ve yöneticilerin:

   - riskleri ve risk maruziyetlerini tanımlamak ve tespit etmek,
   - bu riskleri azaltan veya yöneten kontrol süreçleri ve sistemlerini değerlendirmek,
   - riskleri kabul edilebilir düzeylere indirme amacına yönelik eylem planları yapmak,
   - iş hedeflerine ulaşma olasılığını tespit etmek

   amacıyla özel olarak hazırlanmış bir tarzda işbirliği yapmalarına imkân veren resmî ve kayıtlı bir sürece sahip olur.

3. Özdeğerlendirme yöntemlerinden alınabilecek sonuçlar şunlardır:

- İlgili birimlerdeki insanlar, risklerin değerlendirilmesi, bu riskleri yönetmek için kontrol süreçlerini kullanma ve iş hedeflerine ulaşma şansını artırma konusunda eğitimli ve deneyimli hale gelir.
- *Gayriresmî/yumuşak (soft) kontroller* (yönetim tarzı, liderlik, takım çalışması, davranış kuralları, personelin dürüstlüğü, vb.-Ç.N.) daha kolay belirlenir ve değerlendirilir.
- İnsanlar kendi birimlerindeki kontrol süreçlerine "sahip çıkmaya" teşvik edilir ve çalışma ekipleri ve gruplarının aldığı düzeltici tedbirler genellikle daha etkili olur ve zamanında alınır.
- Bir kurumun hedefisk-kontrol altyapısının tamamı, daha yoğun bir izlemeye ve kesintisiz iyileştirme ve düzeltmeye tâbi olmuş olur.
- İç denetçiler, çalışma ekipleri için kolaylaştırıcı, yazıcı ve raportör işlevini görerek ve CSA programını destekleyen risk ve kontrol kavramları hakkında eğitmenlik yaparak özdeğerlendirme sürecine katılır ve Özdeğerlendirme süreci hakkında bilgi sahibi olur.
- İç denetim bölümü, kurum içindeki kontrol süreçleri hakkında daha fazla bilgi edinir ve bu ek bilgileri, kıt olan kaynaklarını, önemli kontrol zayıflıkları olan veya yüksek risklerle karşı karşıya olan iş birimleri veya fonksiyonlarının araştırılmasına ve bu konuda gereken testlerin yapılmasına tahsis etmek amacıyla kullanabilir.
- Kurum yönetiminin kurumun risk yönetimi ve kontrolü süreçlerine ilişkin sorumlulukları güçlendirilmiş olur ve yöneticilerin bu faaliyetleri denetçiler gibi uzmanlara bırakma eğilimi azalır.
- İç denetim faaliyetinin aslî görevi, tüm risk yönetimi ve kontrolü sistemlerinin yeterliliği ve etkinliği hakkında testler

yapmak ve bu konuda profesyonel görüş ve kanaatlerini açıklamak suretiyle değerlendirme sürecinin doğrulanmasını da kapsar ve bu doğrulamayla devam eder.

4. Kurumlarda CSA süreçleri konusunda uygulanan yaklaşımların çok çeşitli olması; sektör, coğrafya, yapı, kurumsal kültür, personele yetki devrinin düzeyi, baskın yönetim tarzı ve strateji ve politikaları oluşturma tarzı konularında kurumlar arasındaki farkları yansıtır. Bu gözlem, belirli bir CSA programı tipinin belirli bir kurumda başarılı olmasının o program türünün başka bir kurumda da başarılı olacağının bir garantisi olmadığını gösterir. CSA süreci, her kurumun kendine özgü niteliklerine uyarlanmalıdır. Ayrıca, bir CSA yaklaşımının, dinamik olması ve kurumun gelişmesine bağlı ve paralel bir şekilde değiştirilmesi gerektiği anlamına da gelir.

5. CSA programlarında uygulanan üç temel form; çalışma grubu faaliyetleri, anketler ve yönetimin ürettiği analizlerdir. Kurumlar genellikle birden fazla yaklaşımı bir arada kullanmaktadır.

6. Çalışma grubu faaliyetleri, birim veya fonksiyonlardaki farklı düzeyleri temsil eden çalışma ekiplerinden bilgi toplar. Çalışmanın formatı hedeflere, risklere, kontrollere veya süreçlere bağlıdır:

   - *Hedef-esaslı format,* bir iş hedefini gerçekleştirmek için kullanılabilecek en iyi yol üzerinde odaklanır. Çalışma grubu etkinliği, hedefi desteklemek için halen mevcut olan kontrollerin tanımlanmasıyla başlar ve bakiye (artık) risklerin tespit edilmesiyle devam eder. Çalışma grubunun hedefi, kontrol prosedürlerinin etkin ve verimli olup olmadığına ve kabul edilebilir bir düzey içinde artık risklere neden olup olmadığına karar vermektir.
   - *Risk-esaslı format,* bir hedefe ulaşmanın önündeki risklerin listelenmesi üzerinde odaklanır. Çalışma grubu, kurumun belirli bir hedefe ulaşmasını engelleyebilecek bütün muhtemel

engel, tehlike ve tehdit unsurlarının listelenmesiyle başlar ve kontrol prosedürlerinin bu temel riskleri yönetmek için yeterli olup olmadığını tespit etmek için incelenmesiyle devam eder. Çalışma grubunun hedefi, önemli bakiye riskleri tespit etmektir. Bu format, çalışma ekibinin hedefler-riskler-kontroller formülünün tamamını incelemesine imkân verir.

- *Kontrol-esaslı format,* mevcut kontrollerin iyi çalışıp çalışmadığı üzerinde odaklanır. Bu format, yukarıda tanımlanan iki formattan farklıdır; çünkü bu formatta kolaylaştırıcı, çalışma grubu etkinliği başlamadan önce temel riskleri ve kontrolleri belirler ve tanımlar. Çalışma grubundaki, çalışma ekibi, kontrollerin riskleri ne ölçüde azalttığını ve kurumsal hedeflere ulaşmayı ne ölçüde kolaylaştırdığını inceler ve değerlendirir. Çalışma grubunun hedefi, mevcut kontrollerin işlerliği ile yönetimin bu kontrollerden beklediği işlerlik arasındaki açığı ve farkı analiz etmektir.

- *Süreç-esaslı format,* bir süreç zincirinin halkaları olan seçilmiş faaliyetler üzerinde odaklanır. Bu süreçler, genellikle, satın alma, ürün geliştirme veya gelir yaratmanın çeşitli kademeleri gibi, belli bir başlangıç noktasından bitiş noktasına kadar giden birbirine bağlantılı bir faaliyetler dizisinden oluşur. Bu çalışma grubu tipi, genellikle, tüm sürecin ve farklı ara kademelerin hedeflerinin tespit edilmesi ve tanımlanmasını kapsar. Çalışma grubunun hedefi, tüm süreci ve onu oluşturan faaliyetleri değerlendirmek, güncellemek, doğrulamak, geliştirmek ve düzenlemektir. Bu çalışma grubu formatı, kontrol esaslı yaklaşımdan daha geniş bir analiz yapma olanağı verir, çünkü süreç içinde birden fazla hedefi ve amacı kapsar ve yeniden yapılandırma, kalite iyileştirme ve sürekli iyileştirme insiyatifleri gibi eşzamanlı yönetim çabalarına destek olur.

7. CSA'nın anket formunda, hedef kitlenin rahatlıkla anlayabileceği

dikkatli bir dille kaleme alınmış, basit "Evet/Hayır" veya "Var/Yok" sorularından oluşan bir soru formu kullanılır. Hedef kişiler bir çalışma grubuna katılamayacak kadar çok sayıda veya çok farklı alanlardan ise, genellikle bu anket formu kullanılır. Kurumun kültürü çalışma grubunda açık ve samimi tartışmaları engelleyecek nitelikte ise ya da yönetim bilgi toplamak için harcanan zamanı ve masrafı asgarî düzeye indirmek istediğinde de bu format tercih edilir.

8. "Yönetimin ürettiği analizler" olarak adlandırılan özdeğerlendirme formu, yönetim gruplarının seçilmiş iş süreçleri, risk yönetimi faaliyetleri ve kontrol prosedürleri hakkında bilgi toplamak amacıyla kullandığı diğer yaklaşımları kapsar. Analizin amacı, genellikle, kontrol prosedürlerinin özel nitelikleri ve özellikleri hakkında somut bilgiye dayanan bir kanaati zamanında oluşturmaktır ve bu analiz genellikle mevcut kadrodan seçilmiş veya destekleyici rol oynayan bir ekip tarafından hazırlanır. İç denetçi, kontrollerle ilgili bilgiyi artırmak ve bu bilgileri kurumun CSA programının bir parçası olan iş birimleri veya fonksiyonlarının müdürleriyle paylaşmak için bu bilgileri mevcut diğer bilgilerle sentezleyebilir.

9. Bütün özdeğerlendirme programları, riskler ve kontroller ile ilgili kavramlar hakkında bilgi sahibi olan ve bu kavramları iletişim ve haberleşmede kullanan çalışma ekibi üyelerine ve yöneticilerine dayanır. Eğitim programları için, çalışma grubu tartışmalarının düzenli yapılmasını sağlamak için ve tüm sürecin tam olup olmadığını kontrol etmek amacıyla, kurumlar genellikle COSO (*Committee of Sponsoring Organizations of the Treadway Commission-Treadway Komisyonu Sponsor Organizasyonlar Kurulu*) ve COCO (*Guidance on Criteria of Control- Kontrol Kıstasları Rehberi*) modelleri gibi bir kontrol çerçevesi kullanır.

10. Tipik bir CSA çalışma grubu faaliyetinde, çalışma raporunun

büyük kısmı tartışmalar sırasında oluşur. Tartışmaların çeşitli bölüm ve kısımları için varılan grup konsensüsü kaydedilir ve grup, önerilen nihaî raporu son toplantı bitmeden önce gözden geçirir. Bazı program çalışmalarında, çalışma grubu sırasında bilgilerin ve görüşlerin serbest ifade edilmesini sağlamak ve çıkar grupları ve farklı görüşler arasındaki farklılıkları gidermek amacıyla anonim oylama teknikleri kullanılır.

11. İç denetimin bazı CSA programlarına yaptığı yatırım oldukça fazladır. İç denetim, gerekli eğitimi vererek, kolaylaştırıcı, yazıcı ve raportörleri temin ederek ve yönetimin ve çalışma ekiplerinin katılımını sağlayarak sürecin sponsorluğunu yapabilir, süreci tasarlayabilir, uygulayabilir ve fiilen sürece sahip çıkabilir. İç denetimin diğer CSA programlarına katılımı en az düzeydedir. İç denetim, bu programlarda tüm süreçle ilgilenen ve danışmanlık yapan bir taraf işlevini görür ve ekiplerin yaptığı değerlendirmelerin nihaî doğrulama merciidir. Programların çoğunda, iç denetimin kurumun CSA çalışmalarına katılım düzeyi, yukarıda bahsi geçen iki uç noktanın ortasında bir yerlerdedir. İç denetimin CSA programlarına ve münferit çalışma grubu faaliyetlerine katılım düzeyi arttıkça, İç Denetim Yöneticisi, iç denetim personelinin objektif davranıp davranmadığını izlemeli, (gerekirse) bu objektifliği sağlamak için tedbirler almalı ve personelin nihaî karar ve yargılarında taraflı davranmamasını temin etmek amacıyla iç denetim testini genişletmelidir. Standart 1120'ye göre: "*İç denetçilerin tarafsız ve önyargısız bir şekilde davranması ve çıkar çatışmasından kaçınması gerekir*."

12. Bir CSA programı, yönetimin risk yönetimi ve kontrolü süreçlerini kurma ve uygulama ve bu sistemin yeterliliğini değerlendirme konularındaki sorumluluk ve görevlerini yerine getirmesinde yönetime yardımcı olarak iç denetim faaliyetinin geleneksel rolünü artırır ve büyütür. Bir CSA programıyla, iç denetim faaliyeti ve ilgili iş birimleri kontrol süreçlerinin iyi çalışıp çalışmadığı ve

artık risklerin önem düzeyi konularında daha iyi bilgiler üretme konusunda işbirliği yapar.

13. CSA programına kolaylaştırıcı ve uzman gibi personel desteği vermesine rağmen, iç denetim faaliyeti, bu yolla, genellikle, kontrol prosedürleri hakkında bilgi toplamak için gereken çabaları azaltabilir ve bazı testleri eleyebilir. Bir CSA programı, kurum içinde kontrol süreçlerinin değerlendirme kapsamını artırmalı, süreç sahiplerinin aldığı düzeltici tedbirlerin kalitesini geliştirmeli ve iç denetim çalışmalarının yüksek risk taşıyan süreçler ve olağandışı durumların incelenmesi üzerinde odaklanmasına imkân vermelidir. Böylece, iç denetim faaliyeti, CSA süreciyle varılan değerlendirme sonuçlarının doğrulanması, kurumun çeşitli bölümleri ve unsurlarından toplanan bilgilerin sentezinin yapılması ve sonuçta, kontrollerin etkinliği hakkında üst yönetime ve denetim komitesine bir genel görüş sunulması konularında odaklanabilir.

# Uygulama Önerisi 2120.A1-3: Üç Aylık Finansal Raporlama, Özel Durum Açıklamaları ve Yönetim Onayları Konusunda İç Denetçinin Rolü

Uluslararası İç Denetim Standartlarından
Standart 2120.A1'in Yorumu

## İlgili Standart

**2120.A1** Risk değerlendirmesinin sonuçlarına bağlı olarak, iç denetim faaliyeti, kurumun yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayan kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir. Bu değerlendirme:

- mali ve operasyonel bilgilerin güvenilirliğini,
- faaliyetlerin etkinlik ve verimlililiğini,
- varlıkların korunmasını,
- kanunlara, düzenlemelere ve sözleşmelere uyum konularını kapsamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, A.B.D. Sermaye Piyasası Kurulu'nun (SEC) (SEC) kuralları ışığında, üç aylık mali raporlar, özel durum açıklamaları ve yönetim onayları konusunda aşağıdaki ilke ve önerileri dikkate almalıdır. Bu kurallar özellikle SEC'de kayıtlı olan ABD'li kurumlara yönelik olmasına rağmen, aynı zamanda hisseleri SEC'de kote edilmiş 1.300'ün üzerinde yabancı kuruma da uygulanır. Ortaklarına ve diğer hak sahiplerine daha üst düzeyde bir güvence vermek amacıyla, hisseleri halka açık olmayan ve sayıları giderek artan kurum da, üç aylık raporlama kontrolleri ve özel durum açıklamalarında 'en iyi uygulamalar' yöntemine sahip olduklarını göstermek için seçilmiş belirli SEC kurallarını kendi istekleriyle benimsemektedir. İç denetçilerin bu konuda ek tavsiyeler için "Kontrol Süreçlerinin Değerlendirilmesi ve Rapor Edilmesi" başlıklı ve 2120.A2 sayılı Uygulama Önerisine de bakmaları önerilir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Bütün mali piyasaların gücü, yatırımcıların piyasaya duyduğu güvene bağlıdır. şirket yöneticileri, bağımsız denetçiler ve başka piyasa katılımcılarının suç işlediğinin iddia edildiği bazı olaylar bu güveni azaltmış ve zayıflatmıştır. Bu tehlike karşısında, ABD Kongresi ve başka ülkelerdeki giderek artan sayıda yasama mercii ve düzenleyici merci, şirketlerin özel durum açıklamaları ve mali raporlama yükümlülüklerini düzenleyen yeni mevzuat ve kanunlar çıkartmıştır. Özellikle, ABD'de, 2002 tarihli Sarbanes-Oxley Kanunu, üst seviye yöneticilerin ve finans sorumlularının mali tabloları onaylamasını ve ek özel durum açıklamaları yapmasını öngören kapsamlı bir reform yapmıştır.
2. Bu yeni kanun, şirketlere, üst düzey yöneticilerin kişisel onaylarını dayandırabilecekleri gerekli güvenceleri elde etmelerini sağlayacak süreçleri geliştirme ve uygulama görevi yüklemiştir. Bu onay sürecinin anahtar unsurlarından biri de, mali bilgilerin kaydedilmesi ve özetlenmesiyle ilgili iç kontrollerin ve risklerin yönetilmesidir.

**Yeni Kanunî Gerekler:**

3. Sarbanes-Oxley Kanunu'nun 302. maddesi, mali raporlardan şirketin sorumlu olduğunu öngörmektedir ve SEC bu kanunun uygulanması için bir yönetmelik çıkartmıştır. Yeni çıkartılan SEC Kuralları'nın 13a-14 ve 15d-14 maddelerine göre, bir ihraççının yönetiminden sorumlu olan başkanın, yöneticilerin, mali işler müdürünün, mali işler çalışanlarının veya benzer fonksiyonları üstlenen kişilerin, ihraççının Borsa Kanunu Madde 13(a) veya 15(d) uyarınca ibraz edeceği, ara raporlar da dahil, üç aylık ve yıllık raporların her birinde,

    - Raporu incelediğini,
    - Bilgisi dahilinde, raporda, önemli bir durum veya olay hakkında gerçeğe aykırı bir beyanın bulunmadığını veya raporun kapsadığı döneme ilişkin olarak, bu dönemdeki şartlar altında beyanın yanıltıcı olmaması için lüzumlu olan önemli herhangi bir hususun ihmal edilmemiş olduğunu,

- Bilgisi dahilinde, raporda yer alan mali tabloların ve diğer mali bilgilerin, ihraççının rapora konu olan dönemler için ve bu dönemlerin sonu itibariyle mali durumunu, faaliyet sonuçlarını ve nakit akış durumunu her açıdan doğru bir şekilde yansıttığını,
- Kendisi ve onay veren diğer yetkililerin,
  - ihraççının "özel durum açıklama kontrol ve prosedürlerini" *(Kanun Madde 302(a)(4) kapsamında yer alan özel durum açıklamalarıyla ilgili kontrol ve prosedürler kavramını yansıtan ve yeni tanımlanmış bir terim)* oluşturmaktan ve uygulamaktan sorumlu olduğunu,
  - bu özel durum açıklama kontrol ve prosedürlerini, özellikle dönemsel raporun hazırlandığı süre içinde, bütün önemli veri ve bilgilerin kendilerine verilmesini sağlayacak şekilde düzenlediklerini,
  - ihraççının özel durum açıklama kontrol ve prosedürlerinin etkinliğini, raporun ibraz tarihinden önceki 90 gün içindeki bir tarih itibariyle değerlendirdiklerini,
  - bu tarih itibariyle yaptıkları değerlendirmeye göre özel durum açıklama kontrol ve prosedürlerinin etkinliği hakkında vardıkları sonuçları raporda ifade ettiklerini,
- Kendisi ve onay veren diğer yetkililerin, aşağıda sayılan durumları, ihraççının denetçilerine ve yönetim kurulunun denetim komitesine (veya denk işlevleri yerine getiren kişilere):
  - iç kontrollerin tasarımı veya uygulamasında tespit edilen ve ihraççının mali veri ve bilgileri kaydetme, işleme, özetleme ve rapor etme kabiliyetini olumsuz etkileyebilecek olan bütün önemli eksiklikleri açıkladıklarını ve iç kontrollerdeki önemli zayıflıkları tespit edip ihraççının denetçilerine bildirdiklerini,

- ihraççının iç kontrol sisteminde önemli rol üstlenen personelin ya da yöneticilerin karıştığı, önemli olsun olmasın, bütün suiistimalleri açıkladıklarını,
- iç kontrollerde veya diğer hususlarda, yapılan değerlendirme tarihinden sonra iç kontrolleri önemli oranda etkileyebilecek nitelikte, önemli bir değişiklik olup olmadığını; ayrıca, bu önemli eksiklikler ve hayatî zayıflıklar için önerilen düzeltici tedbirleri bildirip açıkladığını, onaylaması gerekir.

**İç Denetçiler İçin Tavsiye Edilen Eylemler:**

4. SEC kurallarının ve Sarbanes-Oxley Kanunu'nun hükme bağladığı gereklerle ilgili üç aylık mali raporlar, özel durum açıklamaları ve yönetim onayları konusunda, iç denetçilerin verebileceği katma değerli hizmetlerle ilgili olarak, iç denetçilere aşağıdaki eylem ve düşünceler önerilmektedir. Bu önerilen eylemler, üç aylık mali raporlama konusunda benzer süreçleri benimsemek ve uygulamak isteyen, hisseleri halka açık olmayan şirketler ve başka kurumlara da *en iyi uygulamalar* olarak önerilmektedir.

   (a) İç denetçinin bu süreçlerdeki rolü, sürecin ilk tasarımcısı, bir özel durum açıklama komitesinin üyesi, kurum yönetimi ile denetçiler arasında koordinatör veya irtibatçı ya da sürecin bağımsız değerlendirmecisi gibi farklı roller olabilir.

   (b) Üç aylık raporlama ve özel durum açıklama süreçlerinde görev alan bütün iç denetçilerin açıkça tanımlanmış bir rolü olmalı ve bu iç denetçiler, üstlendikleri sorumlulukları, ilgili *IIA Danışmanlık* ve *Güvence Standartları*na ve ilgili *Uygulama Önerileri*ndeki ilke ve tavsiyelere göre değerlendirmelidir.

   (c) İç denetçiler, kurumların, üç aylık mali raporlar, özel durum açıklamaları ve hukukî raporlama koşullarına ilişkin süreçleri düzenleyen bir resmî politikaya ve yazılı prosedüre sahip olmasını sağlamalıdır. Bu politika ve prosedürlerin avukatlar,

dış denetçiler ve başka uzmanlar tarafından incelenmesi, bunların yeterince kapsamlı olduğundan ve olması gerekenleri tam yansıttığından emin olunmasını sağlar.

(d) İç denetçiler, kurumların, süreci eşgüdümlemek ve katılımcıları izlemek amacıyla "özel durum açıklama kurulu" kurmalarını teşvik etmelidir. Bu kurulda, önemli finans müdürleri, hukuk danışmanı, risk yönetimi, iç denetim ve kanunî tablolara ve özel durum açıklamalarına veri veya girdi sağlayan diğer birimler de dahil, kurumun belli başlı temel birimlerinin temsil edilmesi gerekir. Normal olarak, İç Denetim Yöneticisi de bu özel durum açıklama komitesinin üyesi olmalıdır. Kurulda İç Denetim Yöneticisinin statüsüne dikkat edilmelidir. Kurul başkanı veya kurulda düzenli üye veya "oy hakkına sahip" üye olan İç Denetim Yöneticilerinin, bağımsızlıkları konusunda dikkatli olmaları ve bu konudaki ilkeler ve yapmaları gereken açıklamalar için *IIA Standartları*'na ve ilgili *Uygulama Önerileri*ne bakmaları tavsiye edilir. İç Denetim Yöneticisinin görevi gereği, re'sen (ex-officio) kurula üye olması onun bağımsızlığıyla ilgili bir sorun yaratmaz.

(e) İç denetçiler üç aylık raporlama ve *özel durum açıklamaları*na ilişkin süreçleri, özel durum açıklama komitesinin faaliyetlerini ve ilgili belgeleri dönemsel olarak gözden geçirip değerlendirmeli ve süreç hakkında yaptıkları değerlendirmeyi ve politika ve prosedürlere uyum hakkında ve genel faaliyetler hakkında verdikleri güvenceyi yönetime ve denetim komitesine sunmalıdır. Bu süreçte aldıkları rol nedeniyle bağımsızlıklarına halel gelebilecek olan iç denetçiler, yönetimin ve denetim komitesinin süreç hakkında başka kaynaklardan da uygun güvenceler alabilmesini sağlamalıdır. Bu başka kaynaklar arasında, kurum içi *özdeğerlendirmeler* yanında, *dış denetçiler* ve *danışmanlar* gibi üçüncü şahıslar sayılabilir.

(f) İç denetçiler, faaliyetlerle ilgili yaptıkları değerlendirmenin sonuçlarına göre, üç aylık raporlara ve özel durum açıklamalarına ilişkin politika, prosedür ve süreçlerle ilgili uygun gördükleri iyileştirmeleri tavsiye etmelidir. Bu faaliyetler için tavsiye edilen en iyi uygulamalar, aşağıda sayılan araç ve prosedürleri, her kurumun kullandığı özel sürece bağlı olarak, tamamen veya kısmen içerebilir:

- Düzgün bir şekilde yazılı hâle getirilmiş politika, prosedür, kontrol ve gözlem raporları,
- Prosedürler ve anahtar nitelikteki kontrol unsurlarını içeren üç aylık kontrol listesi,
- Anahtar nitelikteki özel durum açıklama kontrollerine dair standart kontrol raporları,
- Yönetimin özdeğerlendirmeleri ("*Kontrol Özdeğerlendirme*" (CSA) gibi),
- Anahtar nitelikteki müdürlerin onay veya teyit açıklamaları,
- Kanunî mali tablo taslaklarının ibraz edilmeden önce incelenmesi,
- Kanunî mali tabloların veri unsurlarının kaynağını, anahtar kontrolleri ve her unsurdan sorumlu olan tarafları tevsik eden süreç haritaları,
- Daha önceden rapor edilen kapatılmamış konuların takibi,
- Dönem içinde çıkartılan iç denetim raporlarının değerlendirilmesi,
- Önemli muhasebe tahminleri, karşılıklar için yapılan değerlemeler, bilanço dışı faaliyetler, önemli iştirakler, ortak girişimler ve özel amaçlı tüzel kişiler de dahil yüksek risk taşıyan, karmaşık ve sorunlu alanlar için özel veya belirli hedeflere yönelik gözden geçirmeler,

- Vazgeçilen ayarlamalar da dahil ilgili ayarlama kayıtları ve mali tablolar için "kapanış sürecinin" gözlemlenmesi,
- Kurumun bütün önemli unsurlarının katılmasını ve görüşlerinin alınmasını sağlamak amacıyla, uzak yerlerdeki anahtar üst yöneticilerle telekonferans görüşmeleri yoluyla toplantılarda bağlantı kurmak,
- Derdest ve muhtemel davaların ve şarta bağlı yükümlülüklerin incelenmesi,
- İç kontrol konusunda en azından yılda bir kere ve mümkünse her üç ayda bir çıkartılan İç Denetim Yöneticisi raporu,
- Düzenli özel durum açıklama kurulu ve denetim komitesi toplantıları.

(g) İç denetçiler, Sarbanes-Oxley Kanunu Madde 303'e uymak için uygulanan süreçleri (üç aylık mali raporlama ve özel durum açıklamaları), yönetimin iç kontrollerle ilgili yıllık değerlendirmesine ve kamuya açıklanan raporuna ilişkin Madde 404'e uymak için uygulanan prosedürlerle kıyaslamalı ve karşılaştırmalıdır. Benzer veya uyumlu bir şekilde tasarlanıp hazırlanan süreçler, faaliyetlerin verimliliğine katkıda bulunur; sorun ve hatâların olması veya fark edilmemesi risklerini veya olasılığını azaltır. Süreçler ve prosedürler benzer olabilir ve iç denetçinin rolünün değişmesi de mümkündür. Bazı kurumlarda, iç denetçilerin yaptığı işlerin sonuçları yönetimin iç kontrolle ilgili iddia ve görüşlerinin temelini oluştururken, diğer bazı kurumlarda, iç denetçilerden, yönetimin yaptığı değerlendirmeyi değerlendirmesi beklenebilir.

- İç denetçilerin yaptığı işin niteliği ve bu işin sonuçlarının kullanım şekli, dış denetçinin iç denetçinin işine duyduğu güvenin derecesi ve seviyesi üzerinde çok etkili olabilir.

İç denetçiler, her katılımcının rolünün açıkça tanımlanmasını ve faaliyetlerin kurum yönetimi ve dış denetçilerle eşgüdümlenmesini ve kararlaştırılmasını sağlamalıdır.

- Yönetimin bir fikir oluşturabilmek için kontrollerle ilgili değerlendirmeyi kendisinin yaptığı kurumlarda, iç denetçiler yönetimin yaptığı değerlendirmeyi ve bu değerlendirmeyi destekleyen belgeleri değerlendirmelidir.
- İç denetçiler, iç denetim raporundaki görüşlerin nasıl sınıflandırıldığını değerlendirmeli ve iç kontrollere ilişkin yıllık raporda veya üç aylık mali tablo onaylarında açıklanması gerekebilecek görüşlerin yönetime ve denetim komitesine uygun bir şekilde bildirilmesini sağlamalıdır. Bu görüşlerin zamanında ve uygun bir şekilde çözümlenmesini sağlamak için epey dikkat ve özen gösterilmelidir.

# Uygulama Önerisi 2120.A1-4: Finansal Raporlama Sürecinin Denetlenmesi

Uluslararası İç Denetim Standartlarından
Standart 2120.A1'in Yorumu

## İlgili Standart

**2120.A1** Risk değerlendirmesinin sonuçlarına bağlı olarak, iç denetim faaliyeti, kurumun yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayan kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir. Bu değerlendirme:

- mali ve operasyonel bilgilerin güvenilirliğini,
- faaliyetlerin etkinlik ve verimlililiğini,
- varlıkların korunmasını,
- kanunlara, düzenlemelere ve sözleşmelere uyum konularını kapsamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *Bu Uygulama Önerisi, bir kurumun mali raporlama sürecinde iç denetimin rolünü ve sorumluluklarını irdelemektedir. Üst yönetim, dış denetçiler ve iç denetçilerin rolleri şöyledir:*

- *Mali tablolarla birlikte verilen açıklayıcı notlar ve mali raporla birlikte verilen özel durum açıklamaları da dahil mali bilgilerin ve kontrol ortamının sahibi üst düzey yönetimdir.*
- *Dış denetçi, mali raporu kullanan kişiye, raporda verilen bilgilerin genel kabul gören muhasebe ilkelerine uygun olarak, kurumun mali durumunu ve faaliyet sonuçlarını âdil ve doğru bir şekilde yansıttığı konusunda güvence verir.*
- *İç denetçi, üst yönetime ve yönetim kurulunun denetim komitesine veya bağlı başka bir komitesine, mali raporun hazırlanmasında kullanılan süreçlere ilişkin kontrollerin etkin olduğu konusunda güvence vermek için gerekli prosedürleri uygular.*

*"Denetim Komitesiyle İlişkiler" başlıklı Uygulama Önerisi 2060-2, iç denetçinin denetim komitesiyle olan ilişkilerini düzenler. "Kontrol Süreçlerinin Değerlendirilmesi ve Rapor Edilmesi" başlıklı Uygulama Önerisi 2120.A1-1, bir iç kontrol sistemini değerlendirmek ve bir fikir oluşturmak için gereken delil ve bulguları tartışır. "Üç Aylık Finansal Raporlama, Özel Durum Açıklamaları ve Yönetim Onayları Konusunda İç Denetçinin Rolü" başlıklı Uygulama Önerisi 2120.A1-3, A.B.D. Sarbanes-Oxley Kanunu'nun hükümleri ve A.B.D. Sermaye Piyasası Kurulu'nun (SEC) ilgili kuralları hakkında bilgi verir. Bu Uygulama Önerisi ise, mali raporlama süreci konusunda iç denetçilerin üst yönetimle ve dış denetçilerle olan ilişkisi üzerinde durmaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Amerika Birleşik Devletleri'nde ve başka ülkelerde şirket yönetimindeki sorunlar hakkında yayınlanan raporlar, kâr amacı güden, kâr amacı gütmeyen veya kamu sektöründeki bütün kurum ve şirketlerde daha iyi bir sorumluluk dağılımı ve daha fazla saydamlık sağlamak amacına yönelik bir değişime ihtiyaç duyulduğunu göstermektedir. Etkin bir kurumsal yönetişimin, üzerinde inşa edilebileceği zeminin köşe taşları *üst yönetim, yönetim kurulu, iç denetçiler ve dış denetçilerdir*. İç denetim faaliyeti, iyi bir kurumsal yönetişimin desteklenmesinde önemli rol oynar ve risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirerek, geliştirerek kurum faaliyetlerinin iyileştirilmesinde yardımcı olabilecek özel bir konuma sahiptir. Yakın zamanda yapılan çalışmalar, üst yönetimin kurumun mali raporlarında verilen bilgilerin doğruluğu konusunda daha fazla sorumluluk üstlenmesi gerektiğini göstermiştir. Pek çok kurumda üst yönetim ve denetim komitesi, bu yönetişim ve mali raporlama süreçlerini geliştirmek amacıyla iç denetim faaliyetinden bazı ek hizmetler talep etmektedir. Bu talepler arasında, kurumun mali raporlama üzerindeki iç kontrolleri ve mali raporlarının güvenilirliği, doğruluğu hakkında değerlendirme yapılması da vardır.

**İç Kontrol Hakkında Raporlama:**

2. Bir kurumun denetim komitesinin, yönetim kurulunun diğer komitelerinin ve iç denetim faaliyetinin birbiriyle örtüşen hedefleri

vardır. İç denetim yöneticisinin temel hedefi, denetim komitesinin ihtiyaç duyduğu, talep ettiği destek ve güvence hizmetlerini almasını sağlamaktır. Denetim komitesinin temel hedeflerinden biri, kurumun mali raporlama süreçlerinin güvenilir, âdil ve doğru olmasını sağlamak ve bu amaçla bu süreçleri gözlemektir. *Denetim komitesi ve üst yönetim*, normal olarak, iç denetim biriminin iç kontrol süreçlerinin yeterliliği ve etkinliği hakkında bir fikir oluşturabilmek için yıl içinde yeterli denetim yapmasını ve mevcut bütün bilgileri toplamasını ister. İç Denetim Yöneticisi, normalde, bu genel değerlendirmesini denetim komitesine zamanında sunar. Denetim komitesi, İç Denetim Yöneticisinin raporunun kapsamını, yeterliliğini değerlendirir ve denetim komitesinin yönetim kuruluna sunduğu rapora, İç denetim Yöneticisinin görüş ve fikirlerini de ekleyebilir.

3. İç denetim faaliyetinin iş planları ve özel güvence verme görevleri, kurumun karşı karşıya olduğu tehlike ve riskler hakkında dikkatli bir tanımlama çalışmasıyla başlar ve iç denetim biriminin iş planı hem risklere hem de bu riskleri azaltmak için yönetimin uyguladığı risk yönetim ve kontrol süreçlerine dayanır. Bu risklerin tanımlanması kapsamına giren olay ve işlemler arasında şunlar sayılabilir:
   - Birleşme ve devralmalar da dahil yeni işletmeler,
   - Yeni ürün ve sistemler,
   - Ortak girişim ve ortaklıklar,
   - Yeniden yapılanma,
   - Yönetim tahminleri, bütçeleri ve öngörüleri,
   - Çevre konuları,
   - Mevzuata uyum.

**Bir İç Kontrol Çerçevesi:**

4. Bir kurumun iç kontrol sisteminin değerlendirmesinde, geniş bir kontrol tanımı esas alınmalıdır. IIA, bugün mevcut en etkili iç kontrol kaynağının Treadway Komisyonu'nun Sponsor Kurumlar Kurulu'nun (COSO) 1992 ve 1994 yıllarında yayınladığı "*İç Kontrol -Bütünleşik Çerçeve"* isimli rapor olduğuna inanmaktadır. COSO modelinin kullanılması yaygın bir kabul görmesine rağmen, bazı başka tanınmış ve güvenilir modellerin de kullanılması uygun olabilir. Bazen, kanunlar veya idarî kurallar, bir ülkede belirli bir kurum veya sektörde belirli bir modelin veya kontrol tasarımının kullanılmasını öngörebilir.

5. *İç Kontrol -Bütünleşik Çerçeve* raporunda varılan çeşitli sonuçlar bu tartışmayla ilgili ve bağlantılıdır.
    - İç kontrol *geniş bir şekilde* tanımlanır; iç kontrol sadece muhasebe kontrolleriyle sınırlı değildir ve dar bir bakış açısıyla sadece mali raporlamayla sınırlandırılamaz.
    - Muhasebe ve mali raporlar önemli konular olmakla birlikte, kaynak koruma, faaliyet verimliliği ve etkinliği, kurallara, mevzuata ve kurum içi politikalara uyum gibi iş açısından önem taşıyan başka konular da vardır. Bu etkenlerin de mali raporlama üzerinde etkisi vardır.
    - İç kontrol, yönetimin sorumluluğundadır ve etkili olabilmesi için kurum içindeki bütün kişilerin katılımını gerektirir.
    - İç kontrol çerçevesi, iş hedeflerine bağlıdır ve benimsenip uygulanabilecek kadar esnek olmalıdır.

**İç Kontrolün Etkinliğine Dair Raporlama:**

6. İç denetim faaliyetinin kontrol sisteminin etkinliğiyle ilgili değerlendirmesi ve kontrol modeli veya sisteminin yeterliliği hakkındaki görüşü, İç Denetim Yöneticisi tarafından denetim komitesine sunulmalıdır. Denetim komitesi ve yönetim kurulu, etkin ve yeterli bir iç kontrol sistemini sürdürebilmek için yönetime

güvenmelidir. Ancak bu güveni, bağımsız bir gözetim ile pekiştirir. Yönetim kurulu veya denetim komitesi (veya kurula bağlı başka bir komite) aşağıdaki soruları sormalı ve İç Denetim Yöneticisi de bu soruların cevaplanmasında ona yardımcı olabilmelidir.

**(a)** Güçlü ve sağlam bir iş etik ortamı ve kültürü var mı?

- Denetim komitesi ve yönetim kurulunun üyeleri ve üst düzey yöneticiler dürüstlük konusunda iyi örnek oluyor mu?
- Performans ve teşvik hedefleri gerçekçi mi, yoksa bunlar kısa vadeli sonuçlar üzerinde aşırı bir baskı mı yaratıyor?
- Kurumun davranış kuralları eğitimle ve yukarıdan aşağı iletişimle takviye ediliyor mu? Mesaj, sahadaki personele kadar ulaşıyor mu?
- Kurumun iletişim kanalları açık mı? Her düzeyde yöneticiler ihtiyaç duydukları bütün bilgileri alabiliyorlar mı?
- Herhangi bir düzeyde mali raporlama usulsüzlüklerine sıfır tolerans uygulanıyor mu?

**(b)** Kurum riskleri nasıl belirliyor ve yönetiyor? -Bir risk yönetim süreci var mı ve bu süreç etkin mi? -Riskler tüm kurum çapında yönetiliyor mu? -Önemli riskler denetim komitesi ve yönetim kuruluyla samimî ve açık bir şekilde tartışılıyor mu?

**(c)** Kontrol sistemi etkin mi?

- Kurumun mali raporlama süreci üzerindeki kontrolleri kapsamlı mı ve mali raporların tamamlayıcı bir parçasını oluşturan mali tabloların, dip notların, ve diğer mecburî ve isteğe bağlı özel durum açıklamalarının hazırlanmasını da kapsıyor mu?

- Üst yönetim ve birim yönetimleri kontrolle ilgili kabul ettiklerini gösteriyorlar mı?
- Kurumun rapor edilen mali sonuçlarında veya bunların ekindeki mali açıklamalarda, üst yönetimi, denetim komitesini, yönetim kurulunu veya kamuyu şaşırtan "sürprizlerin" sıklığı artıyor mu?
- Kurum çapında iyi bir iletişim ve raporlama sistemi var mı?
- Kontroller, hedeflere ulaşmanın bir aracı olarak mı yoksa "zorunlu bir belâ" olarak mı görülüyor?
- Nitelikli kişiler zamanında işe alınıyor ve bunlara yeterli eğitim veriliyor mu?
- Sorunlu alanlar hızlı ve eksiksiz bir şekilde tespit edilebiliyor mu?

**(d)** Güçlü bir gözlem sistemi var mı?

- Denetim komitesi ve yönetim kurulu kurum yönetiminden bağımsız mı, her türlü muhtemel menfaat çatışmasından uzak mı, iyi bilgilendiriliyor mu ve konuların ayrıntılarına iniyor mu?
- Üst yönetim ve denetim komitesi iç denetim birimine destek veriyor mu?
- İç ve dış denetçilerin üst yönetimin ve denetim komitesinin bütün üyelerine açık iletişim hatları ve özel erişim imkânları var mı ve bunları kullanıyorlar mı?
- Birim yönetimi kontrol sürecini gözlüyor mu?
- Kurum dışından temin edilen süreçleri gözlemek için kullanılan bir program var mı?

7. İç kontroller başarıyı *garanti edemez*. Kötü kararlar, zayıf yöneticiler

veya çevresel etkenler kontrollerin etkisini ortadan kaldırabilir. Ayrıca, dürüst olmayan yöneticiler bu kontrolleri aşabilir ve astlarından gelen mesajları göz ardı edebilir, engelleyebilir veya üstünü örtebilir. Ancak bütün yönetim unsurlarından açık ve güvenilir mesajlar alan ve yetkin finans, hukuk ve iç denetim birimlerinin desteğini alan faal ve bağımsız bir yönetim birimi, muhtemel sorunları tespit edebilir ve etkin bir gözetim yapabilir.

**İç Denetçinin Rolleri:**

8. Gelecek yılın mali raporlama rejimine ilişkin görev ve sorumlulukları için üst yönetime, denetim komitesine ve dış denetçiye yardımcı olmak amacıyla yeterli *kaynak ayrılmamışsa,* İç Denetim Yöneticisinin iç denetim biriminin o yıla ilişkin risk değerlendirme ve denetim planlarını gözden geçirmesi gerekir. Mali raporlama süreci, gerekli bilgilerin oluşturulması ve mali tabloların ve açıklayıcı dip notlarının ve kurumun mali raporlarının ekinde sunulan diğer özel durum açıklamalarının hazırlanması için gerekli işlemleri kapsar.

9. İç Denetim Yöneticisi, kurumun risk değerlendirmesine uygun olarak iç denetim biriminin kaynaklarını mali raporlama, yönetişim ve kontrol süreçlerine tahsis etmelidir. İç Denetim Yöneticisi, üst yönetime ve denetim komitesine, mali raporların hazırlanmasında kullanılan destekleyici süreçlere ilişkin kontrollerin yeterli bir şekilde tasarlandığı ve etkin bir şekilde uygulandığı konusunda bir güvence verebilmek için gereken prosedürleri uygulamalıdır. Uygulanan kontroller, önemli hatâlar, usulsüzlükler, yanlış varsayımlar ve tahminlerin ve yanlış veya yanıltıcı mali tablolara, açıklayıcı notlara veya başka açıklamalara neden olabilecek başka olayların önlenmesi ve tespiti için yeterli olmalıdır.

10. İç Denetim Yöneticisinin mali raporların güvenilirliğini ve doğruluğunu sağlamak amacıyla yönetim kurulunun veya denetim komitesinin (veya yönetim kurulunun başka bir komitesinin)

gözetim sorumluluklarına ve kurumun genel yönetişim sürecine destek olmak için dikkate alması önerilen konuların bir listesi aşağıda sunulmaktadır.

**(a) Mali Raporlama**

- Bağımsız muhasebecilerin tayini için gereken bilgileri vermek,
- Denetim planlarının, kapsamının ve iş çizelgesinin dış denetçilerle eşgüdümlü olarak belirlenmesi,
- Denetim sonuçlarını dış denetçilerle paylaşmak,
- Muhasebe politikaları ve politika kararları (*bilanço dışı işlemlere ve takdirî konulara ilişkin muhasebe kararları da dahil*), mali raporlama sürecinin özel unsurları ve olağandışı veya karmaşık mali işlem ve olaylar (*örneğin, ilgili taraflarla işlemler, birleşme ve devralmalar, ortak girişimler ve ortaklık işlemleri*) hakkındaki tespitlerini dış denetçilere ve denetim komitesine bildirmek,
- Denetim komitesi, dış denetçiler ve üst yönetimle birlikte, mali raporları ve özel durum açıklamalarını değerlendirme sürecine katılmak ve düzenleyici kurumlara sunulanlar da dahil mali raporların kalitesini değerlendirmek,
- Başta mali raporlama süreci üzerindeki kontrol uygulamaları olmak üzere kurumun iç kontrollerinin yeterliliğini ve etkinliğini değerlendirmek. Bu değerlendirmede, kurumun suiistimallere karşı duyarlılığı ve bu tehlikeleri önlemek veya azaltmak için kullanılan program ve kontrollerin etkinliği değerlendirilmelidir.
- Kurum yönetiminin kurumun davranış kurallarına uyup

uymadığını gözlemek ve etik davranışı teşvik eden etik politikalarının ve benzeri başka prosedürlerin uygulanmasını sağlamak. Kurum içinde etkili bir etik kültürü oluşturmanın önemli etkenlerinden biri de, üst yöneticilerin etik davranışlar konusunda iyi bir örnek teşkil etmesi ve çalışanlarla, denetim komitesiyle, yönetim kuruluyla ve kurum dışındaki hak sahipleriyle açık ve güvenilir iletişim kurmasıdır.

**(b) Kurumsal Yönetişim:**

- Kurumun kanunlara ve düzenlemelere uyumuna, etik ve menfaat çatışmalarına ilişkin politikalarını ve suiistimal iddialarının zamanında ve derinlemesine araştırılması ve takibiyle ilgili politikalarını gözden geçirmek,
- Kurumsal risk ve yönetişim riski taşıyan derdest davaları veya idarî soruşturma ve takipleri gözden geçirmek,
- Personelin menfaat çatışmaları, usulsüzlük ve suiistimalleri hakkında ve kurumun ilgili etik prosedür ve raporlama mekanizmalarının diğer sonuçları hakkında bilgi vermek.

**(c) Kurumsal Kontrol:**

- Kurumun derlediği ve rapor ettiği işletme ve mali bilgilerinin güvenilirliğini ve doğruluğunu gözden geçirmek,
- Önemli muhasebe politikaları hakkında bir kontrol analizi yapmak ve bunları tercih edilen uygulamalarla karşılaştırmak (meselâ, gelir kayıtları veya bilanço dışı muhasebe uygulamaları hakkında soruların sorulduğu işlemlerin genel kabul gören muhasebe standartlarına uygunluğu incelenmelidir),

- İş raporları ve mali raporların hazırlanmasında kullanılan tahmin ve varsayımların akla yatkınlığı ve uygunluğunu değerlendirmek,
- Özel durum açıklamalarında veya yorumlarda kullanılan tahmin ve varsayımların ilgili kurumsal bilgi ve uygulamalara ve - uygunsa- başka şirketlerin rapor ettiği benzer kalemlerle tutarlı olmasını sağlamak,
- Yevmiye kayıtlarının hazırlanması, incelenmesi, onaylanması ve muhasebeleştirilmesi sürecini değerlendirmek,
- Muhasebe fonksiyonunda kullanılan kontrollerin yeterli olup olmadığını değerlendirmek.

# Uygulama Önerisi 2120.A4-1: Kontrol Kıstasları

Uluslararası İç Denetim Standartlarından
Standart 2120.A4'ün Yorumu

## İlgili Standart

**2120.A4** Kontrollerin değerlendirilmesi için uygun ve yeterli kıstaslara ihtiyaç vardır. İç denetçiler, yönetimin hedef ve amaçlara ulaşılıp ulaşılmadığını belirlemek için oluşturduğu kıstasların yeterlilik derecesini tespit etmelidir. Bu kıstaslar yeterliyse, iç denetçiler de kendi değerlendirmelerinde bunları kullanabilir. Kıstaslar yeterli değilse, iç denetçiler uygun değerlendirme kıstasları geliştirmek için yönetimle birlikte çalışmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, kontrol kıstaslarını değerlendirirken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun, bir değerlendirmede dikkate alınması gereken hususların tümünü kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Kontrolleri değerlendirmeden önce, yönetim gözden geçirilecek sahayla ilgili almak istediği risk seviyesini tesbit etmelidir. İç denetçiler, risk seviyesinin ne olduğunu belirlemelidir. Bu, gözden geçirilen alanla ilgili ana hedeflerin gerçekleştirilmesine tehdit teşkil eden anahtar unsurların potansiyel etkisinin azalmasına bakılarak belirlenebilir.

2. Eğer yönetim, ana riskleri ve üstlenmek istediği artık risk seviyesini belirlememişse, iç denetim faaliyeti, risk belirleme çalıştaylarıyla veya kurumun kullandığı diğer tekniklerle, riskin belirlenmesine yardım edebilir.

3. Ancak risk seviyesi belirlendiğinde, uygulanmakta olan kontrollerin, riskin arzulanan seviyeye indirilmesinde ne kadar başarılı olduğu değerlendirilebilir.

# Uygulama Önerisi 2130-1: İç Denetim Faaliyeti ve İç Denetçinin Bir Kurumun Etik Kültüründe Oynadığı Rol

Uluslararası İç Denetim Standartlarından
Standart 2130'un Yorumu

## İlgili Standart

**2130 Yönetişim**
İç denetim faaliyeti, aşağıdaki amaçların gerçekleştirilmesi amacıyla önetişim sürecinin iyileştirilmesi için gerekli tavsiyelerde bulunmalı ve tavsiyeleri değerlendirmelidir:

- Kurum içinde gerekli etik ve diğer değerlerin geliştirilmesi,
- Etkili bir kurumsal performans yönetimi ve hesap verebilirlik,
- Risk ve kontrol bilgilerinin kurumun gerekli alanlarına etkili bir şekilde iletilmesi,
- Yönetim kurulunun, denetim komitesinin, iç ve dış denetçilerin ve üst yönetimin faaliyetleri arasında eşgüdüm sağlamak ve bunlar arasında gerekli bilgilerin etkili bir şekilde iletimini sağlamak.

## İlgili Standart

**2130.A1** İç denetim faaliyeti, kurumun etikle ilgili amaç, program ve faaliyetlerinin tasarımını, uygulanmasını ve etkinliğini değerlendirmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bir kurumun etik kültüründe oynayabilecekleri rolü tayin ederken aşağıdaki önerileri dikkate almalıdır. Bu rol, kurumun etik kültürünün yerleşikliğine veya gelişmişlik düzeyine bağlı olarak farklılık gösterebilir. Bu kılavuzun, bir kurumun etik kültürüyle ilgili kapsamlı bir güvence*

*veya danışmanlık görevi için gerekli olabilecek bütün prosedürleri kapsamak gibi bir amacı yoktur.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Bu Uygulama Önerisi, bir kurumda etik ortamının yaratılmasında kurumsal kültürün önemini vurgulamakta ve bu ortamın geliştirilmesinde iç denetçilerin oynayabileceği bir rolün de olduğunu ileri sürmektedir. Daha somut olarak, bu Uygulama Önerisi:
    - yönetişim sürecinin niteliğini tanımlar,
    - bu sürecin kurumun etik kültürüyle bağlantısını kurar,
    - başta iç denetçiler olmak üzere, kurumla ilişkisi bulunan herkesin etik savunuculuğu rolünü üstlenmesi (diğer bir deyişle, etik konusuna sahip çıkması) gerektiğini belirtir,
    - gelişmiş bir etik kültürünün unsurlarını, özelliklerini sayar.

**Yönetişim & Kurum Kültürü**

2. Bir kurum:
    (a) içinde yaşadığı toplumun hukukuna ve diğer düzenleyici kurallarına uymak,

    (b) toplumda genel kabul gören iş hayatına dair kuralları, etik hükümleri ve sosyal beklentileri karşılamak,

    (c) hem topluma faydalı olmak hem de uzun ve kısa vadede '*hissedarlarının ve diğer menfaat sahiplerinin*' çıkarlarını korumak,

    (d) kararları, faaliyetleri, yönetimi ve performansıyla ilgili hesap verme sorumluluğunu yerine getirmek üzere, büyük ortaklarına, diğer hissedarlarına, düzenleyici makamlara ve kamuya tam ve doğru bilgi vermek amacıyla çeşitli hukukî formlar, yapılar, stratejiler ve prosedürler kullanır.

Bir kurumun bu dört sorumluluğun gereğini yerine getirmek üzere seçtiği *iş yapma usullerinin bütünü*, yaygın bir şekilde, *yönetişim*

*süreci* olarak tâbir edilir. Yönetişim sürecinin amacına hizmet edecek şekilde çalışmasından, kurumun bir yönetim mercii (yönetim kurulu, mütevelli heyeti veya icra kurulu gibi) ve üst seviye yöneticileri sorumludur.

3. Bir kurumun yönetişim uygulamaları, kurumdaki rolleri ve davranışları belirleyen, sorumlulukları tanımlayan, hedefler ve stratejiler geliştiren ve performansı ölçen, kuruma özgü ve sürekli değişen bir kültürün tezahürüdür. Bu kültür, kurumun benimseyip dile getirdiği, cevaz verdiği değerleri, davranışları ve rolleri şekillendirir; kurumun topluma karşı sorumluluklarını yerine getirmek konusundaki *hassasiyetini* (bir başka deyişle, özenli veya kayıtsız olma eğilimini) ortaya koyar. Bu nedenle, kurumun genel yönetişim sürecinin kendisinden beklenen amaca ne kadar hizmet edebileceği, büyük ölçüde kurumun kültürüne bağlıdır.

**Kurumun Kültürünün Sorumluluğunun Paylaşılması**

4. Kurumla bağlantısı bulunan *herkes*, kurumun etik kültürünün durumundan bir ölçüde *sorumludur* ve bu sorumluluğu paylaşır. Kurumların çoğunda karar alma süreçlerinin çok karmaşık ve dağınık olmasından dolayı, bu rol ister ona resmen verilmiş olsun ister gayriresmî yollarla üstlenilmiş olsun, her bireyin bir etik savunucusu olmaya özendirilmesi ve teşvik edilmesi gerekir. *Davranış kuralları ve vizyon açıklamaları ve kurum politikaları*; kurumun değer ve hedeflerini, kurum çalışanlarından beklenen davranışları ve kurumun etik, hukukî ve toplumsal sorumluluklarına uygun bir kültürü sürdürmek amacına yönelik stratejilerini gösteren açık ve önemli beyanlardır. Giderek artan sayıda kurum, yöneticilere ve diğer kişilere kurum içinde danışmanlık yapması ve 'doğruları göstermesi' için bir '*etik görevlisi*' tayin etmektedir.

**Etik Savunucusu Olarak İç Denetim Faaliyeti**

İç denetçiler ve iç denetim faaliyeti, kurumun etik kültürünün desteklenmesi konusunda faal bir rol oynamalıdır. İç denetçiler,

kurum içinde dürüst ve güvenilir kişiler olarak tanınır ve tesirli bir etik savunuculuğunun gerektirdiği becerilere ve vasıflara sahiptir. İç denetçiler, kurumun yöneticileri ve diğer çalışanlarından kurumun hukukî, etik ve toplumsal sorumluluklarına uymalarını talep etmeye ehil ve yetkilidir.

İç denetim faaliyeti, etik savunuculuğu yaparken birbirinden farklı rollerden birini üstlenebilir. Bunlar, etik görevlisi olma (ombudsman, uyum görevlisi, etik danışmanı veya etik uzmanı), kurum içi etik konseyi üyeliği veya etik ortamı uzmanlığı olabilir. Bazı durumlarda, etik görevlisinin rolü, iç denetim faaliyetinin 'bağımsızlık' özelliğiyle çelişebilir. Bazı durumlarda, etik görevlisi rolü, iç denetim faaliyetinin bağımsızlık özelliğiyle çelişebilir.

**Kurumun Etik Ortamının Değerlendirilmesi**

7. İç denetim faaliyeti, en azından, kurumun etik iklimini ve kurumun istenen hukukî ve etik uygunluk seviyesine ulaşmak amacıyla uyguladığı stratejilerin, taktiklerin, raporlamaların ve diğer süreçlerin etkinliğini dönemsel olarak incelemelidir. İç denetçiler, yüksek etkinliğe sahip gelişmiş bir etik kültürde bulunması beklenen şu unsurlara, kurumun ne ölçüde sahip olduğunun muhasebesini yapmalıdır:

   (a) Açık ve anlaşılır nitelikte resmî *Davranış Kuralları*, ilgili *manifestolar*, -suiistimal ve yolsuzluğa karşı *prosedürler* de dahil- *politikalar* ve gerçekleştirmek istediklerine dair kurumun *diğer açıklamaları,*

   (b) Yöneticilerin çalışanlardan beklenen etik davranış ve vasıfları sıklıkla belirtmeleri ve kendilerinin de bunları bizzat yaşayarak göstermeleri,

   (c) Kurumun, etik kültürüne bağlılığını tazelemek amacıyla, düzenli programlarla desteklenen ve geliştirilen *açık stratejilere* sahip olması,

(d) *Davranış Kuralları*na, politikalara ve diğer düzenlemelere aykırılıkların gizlilik içinde rapor veya ihbar edilebilmesi için kolaylıkla uygulanabilir birden çok usulün mevcut olması,

(e) Çalışanlar, tedarikçiler ve müşterilerin kurum işlerini yürütürken, etik davranış gereklerine tâbi olduklarını bildiklerine dair *düzenli beyanlar*da bulunması,

(f) Etik davranış sonuçlarının değerlendirilmesini, aykırılık iddialarının araştırılmasını, hukuk danışmanıyla yürütülen işlemlerde gizliliğe riayet edilmesini ve araştırma bulgularının düzenli olarak rapor edilmesini sağlamak amacıyla *sorumlulukların* açıkça *belirlenmiş ve dağıtılmış* olması,

(g) Bütün çalışanların etik savunucusu olmasına yönelik *eğitim imkânları*ndan herkesin kolaylıkla istifade edebilmesinin sağlanması,

(h) Her çalışanın kurumun etik ortamına katkıda bulunmasını teşvik eden, *personele yönelik olumlu uygulamalar,*

(i) Kurumun etik kültürünün durumunu tespit etmek amacıyla, tedarikçiler, çalışanlar ve müşterileri kapsayan düzenli *anketler*,

(j) Etik kültürünü zayıflatıcı nitelikte *baskı* ve *sapmalar* yaratabilecek kurum içi resmî ve gayriresmî süreçlerin düzenli şekilde incelenmesi ve gözden geçirilmesi,

(k) Dürüstlük testleri, uyuşturucu taramaları ve benzeri tedbirler de dahil, işe alma prosedürlerinin bir parçası olarak uygulanan düzenli *referans* ve *özgeçmiş kontrolleri*.

# Uygulama Önerisi 2200-1: Görev Planlaması

Uluslararası İç Denetim Standartlarından
Standart 2200'ün Yorumu

## İlgili Standart

**2200 Görev Planlaması**
İç denetçiler, her görev için, kapsam, amaçlar, zamanlama ve kaynak dağılımı hususlarını da dikkate alan ayrı bir plan hazırlamalı ve kaydetmelidir.

## İlgili Standart

**2201 Planlamada Dikkate Alınması Gerekenler**
Bir görevi planlarken, iç denetçiler şu noktaları dikkate almalıdır:

- Denetlenecek olan faaliyetin hedefleri ve faaliyetin kendi performansını kontrol etmesinin araçları,
- Faaliyet ve hedeflerine, kaynaklarına ve operasyonlarına yönelik önemli riskler ve bu potansiyel risklerin etki veya ihtimallerini kabul edilebilir bir seviyede tutmanın yol ve araçları,
- Bir ilgili kontrol çerçevesi veya modeline kıyasla, ilgili faaliyetin risk yönetimi ve kontrolü sistemlerinin yeterlilik ve etkinliği,
- Faaliyetin risk yönetimi ve kontrol sistemlerinde önemli gelişme sağlama imkânları.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görevlerini planlarken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun planlama yaparken gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken konuları içeren bir öneriler demetinden oluşmaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçi, üstlerinin inceleme ve onayına tâbi olarak, görevlerini planlamaktan ve yürütmekten *kendisi* sorumludur. Bir görev programı:
    - iç denetçinin görevi sırasında ilgili bilgileri toplamak, analiz etmek, yorumlamak ve kaydetmek için uygulayacağı prosedürleri göstermeli,
    - görevin amaçlarını açıklamalı,
    - görevin her safhasında görevin amaçlarına ulaşmak için gereken testlerin derecesi ve kapsamını belirtmeli,
    - incelenmesi gereken teknik özellikleri, riskleri, süreçleri ve işlemleri tanımlamalı,
    - gereken testlerin niteliğini ve kapsamını göstermeli,
    - göreve başlanmadan önce hazır olmalı ve gerekirse, görev sırasında değiştirilmelidir.

2. Görevle ilgili sonuçların nasıl, ne zaman ve kime rapor edileceğinin tesbiti, *İç Denetim Yöneticisinin* sorumluluğundadır. Bu tespitler, görev planlama aşamasında mümkün olduğu oranda açıkça kaydedilmeli ve yönetime raporlanmalıdır. Görev sonuçlarının zamanlamasını veya raporlamasını etkileyen daha sonraki değişiklikler de, gerekiyorsa, yönetime bildirilmelidir.

3. Görevin süresi ve tahminî tamamlanma tarihi gibi, görevle ilgili diğer gerekler de tespit edilmelidir. *Nihaî rapor formatı* da düşünülmeli ve belirlenmelidir; çünkü bu safhada düzgün bir planlama, nihaî raporun hazırlanmasında kolaylık sağlar.

4. Görev hakkında bilgilendirilmesi gereken bütün *yöneticilere bilgi verilmelidir.* Denetlenmekte olan faaliyetin yöneticileriyle toplantılar yapılmalıdır. Toplantılarda konuşulan konuların özetini ve varılan sonuçları gösteren tutanaklar hazırlanıp uygun kişilere dağıtılmalı ve çalışma dosyalarında muhafaza edilmelidir. Tartışma

konuları şunlar olabilir:

- Planlanan amaçlar ve işin kapsamı,
- Göreve konu olan işlerin zamanlaması,
- Görevlendirilen iç denetçiler,
- Yöntemler, zaman kısıtları ve sorumlu kişiler de dahil, görev boyunca raporlama süreci,
- Yönetimde veya önemli sistemlerde meydana gelen son değişiklikler de dahil, denetlenmekte olan birimin çalışma şartları ve faaliyetleri,
- Yönetimin öncelikli meseleleri, endişeleri ve talepleri,
- İç denetçi için özel önem arz eden konular,
- İç denetim faaliyetinin raporlama prosedürleri ve takip sürecinin tanımı.

# Uygulama Önerisi 2210-1: Görev Amaçları

Uluslararası İç Denetim Standartlarından
Standart 2210'un Yorumu

## İlgili Standart

**2210 Görev Amaçları**
Görev amaçları, denetlenen faaliyetle ilgili riskleri, kontrolleri ve yönetişim süreçlerini kapsamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, belirli bir görevin amaçlarını belirlerken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu tespitte gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece dikkate alınması tavsiye edilen bazı konuları açıklamaktadır.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Planlama *yazılı* hâle getirilmelidir. Görevin amaçları ve işin kapsamı belirlenmelidir. *Amaçlar,* iç denetçilerin geliştirdiği kapsamlı ifadeler olup, başarmak istenilen hususları tanımlar. *Görev prosedürleri*, amaçlara ulaşmak için kullanılacak araç ve yollardır. Amaç ve prosedürler, birlikte, iç denetçinin işinin *kapsamını* tayin eder.

2. Görev amaç ve prosedürleri, denetlenen faaliyetin riskleriyle ilgili olmalıdır. Burada kullanılan "*risk*" terimi, hedeflere ulaşılmasını etkileyebilecek bir olayın meydana gelme belirsizliğini ifade eder. Risk, sonuçlar ve olasılık cinsinden hesaplanır. Planlama safhasındaki risk değerlendirmesinin gayesi, görev amacı hâline getirilip incelenmesi gereken önemli faaliyet alanlarını teşhis edebilmektir.

# Uygulama Önerisi 2210.A1-1: Görev Planlamasında Risk Değerlendirmesi

Uluslararası İç Denetim Standartlarından
Standart 2210.A1'in Yorumu

## İlgili Standart

2210.A1 İç denetçi, denetlenen faaliyetle ilgili risklerin ön değerlendirmesini yapmalıdır. Görevin amaçları, bu risk değerlendirmesinin sonuçlarını yansıtmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görev planlama safhasında riskleri değerlendirirken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun böyle bir değerlendirmede gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. İç denetçi, yönetimin denetlenen faaliyetle ilgili risk değerlendirmesini gözönüne almalıdır. İç denetçinin bu bağlamda düşüneceği hususlar şunlardır:
   - Yönetimin risk değerlendirmesinin güvenilirliği,
   - Yönetimin risk meselelerinin raporlanması ve gözlenmesine yaklaşımı,
   - Kabul edilebilir risk seviyelerini aşan durumlara dair yönetim raporları,
   - Denetlenen faaliyetle ilişkili olabilecek destek sistemlerinde ve kurumun diğer faaliyetlerinde, yönetimce teşhis edilen başka risklerin olup olmadığı,
   - Yönetimin risklerle ilgili kendi kontrol değerlendirmesi.

2. İncelenecek olan faaliyetler hakkında *temel (arkaplan) bilgiler* toplanmalıdır. Görev üzerindeki muhtemel etkilerini tespit etmek amacıyla, ayrıntısı aşağıda sayılan bu bilgiler gözden geçirilmelidir.
   - Amaçlar ve hedefler,
   - Faaliyetler ve raporlar üzerinde önemli bir etkisi olabilecek politika, plan, prosedür, kanun, yönetmelik ve sözleşmeler,
   - Çalışanların, anahtar personelin sayısı, isimleri, iş tanımları ve -önemli sistem değişiklikleri de dahil- kurum içindeki son değişiklikler hakkında ayrıntılı bilgiler gibi kuruma ait bilgiler,
   - İncelenecek olan faaliyetle ilgili bütçe bilgileri, faaliyet sonuçları ve mali veriler,
   - Daha önceki görevin çalışma kâğıtları,
   - Dış denetçilerin tamamlanmış veya devam eden işleri de dahil diğer görevlerin sonuçları,
   - Görev üzerinde önemli potansiyel etki yapabilecek sorunları tespit etmek amacına yönelik yazışma dosyaları ve
   - Faaliyet için uygun ve yetkin teknik literatür.

3. Gerekirse ve uygun görülürse, faaliyetler, riskler ve kontrollere aşina olabilmek, görev için önemli olan alan ve konuları tespit etmek ve denetlenenlerin yorum ve tavsiyelerini almak amacıyla bir anket çalışması yapılmalıdır. Anket, inceleme konusu olan faaliyet hakkında, ayrıntılı bir doğrulama olmaksızın, bir bilgi toplama sürecidir. Anketin temel amaçları şunlardır:
   - Denetlenecek faaliyeti anlamak,
   - Özel dikkat gösterilmesi gereken önemli alanları tespit etmek,
   - Denetim sırasında kullanmak üzere bilgi toplamak,
   - Ek bir denetime gerek olup olmadığına karar vermek.

4. Bir anket, görev çalışmalarının planlanmasında ve uygulanmasında somut bilgiye dayanan bir yaklaşımı mümkün kılar ve iç denetim faaliyetinin sahip olduğu kaynakların amaca en uygun alanlarda kullanılması için etkili bir araçtır. Bir anketin odak noktası, görevin niteliğine bağlı olarak değişir. Bir anketin kapsamı ve zamanlaması da değişkenlik arz eder. İç denetçinin eğitimi, tecrübesi, bilgi seviyesi, denetimin türü ve anketin rutin olarak yapılan dönemsel bir görevin veya göreve özel denetim sonrası yapılan bir *takip* çalışmasının parçası olup olmaması, anketin kalitesini ve işlevselliğini belirleyen unsurlardandır. Zaman planlamasıyla ilgili gerekler ise, denetlenen faaliyetin büyüklüğü, karmaşıklığı ve faaliyetin coğrafî dağılımından etkilenir.

5. Bir anket, aşağıda sayılan prosedürlerin uygulanmasını gerektirebilir:
   - Denetlenenlerle yapılan görüşmeler,
   - Faaliyetten etkilenen kişilerle, örneğin, faaliyetin çıktılarını kullananlarla yapılan görüşmeler,
   - Saha gözlemleri,
   - Yönetim raporları ve araştırmalarının incelenmesi,
   - Analitik denetim prosedürleri,
   - Akış şemaları,
   - İşlevsel "gözden geçirmeler" (başlangıçtan sonuna kadar belirli iş ve faaliyetlerin testleri),
   - Temel kontrol faaliyetlerinin yazılı hâle getirilmesi.

6. İç denetçi, yönetimin risk değerlendirmelerinden, temel (arkaplan) bilgilerden ve anket bulgularından elde edilen sonuçların bir özetini hazırlamalıdır. Bu özet şu hususlara temas etmelidir:
   - Önemli sorunlar ve bunların daha derinliğine incelenmesinin sebepleri,

- Anket sırasında elde edilen ilgili bilgiler,
- Görevin amaçları, prosedürleri ve bilgisayar destekli denetim teknikleri gibi özel yaklaşımlar,
- Potansiyel kilit kontrol noktaları, kontrol zaafiyetleri ve/veya aşırı kontroller,
- Zaman ve kaynak ihtiyaçları hakkında ön tahminler,
- Raporlama safhaları ve görevin tamamlanması için gözden geçirilen tarihler,
- Gerekirse, göreve devam edilmemesinin sebepleri.

# Uygulama Önerisi 2230-1: Görev Kaynaklarının Tahsisi

Uluslararası İç Denetim Standartlarından
Standart 2230'un Yorumu

## İlgili Standart

**2230 Görev Kaynaklarının Tahsisi**
İç denetçiler, görevin amaçlarına ulaşmak için gereken kaynakları tespit etmelidir. Görev kadrosu, görevin niteliği, karmaşıklığı, zaman kısıtlamaları ve mevcut kaynaklar dikkate alınarak teşkil edilmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görev kaynaklarının nasıl tahsis edileceğini belirlerken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu tespitte gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

Görevi yerine getirmek için gerek duyulan kaynakların tespitinde, aşağıdakilerin değerlendirilmesi önem taşır:

- İhtiyaç duyulan iç denetim personelinin sayısı ve deneyim düzeyi belirlenirken; görevin niteliği, karmaşıklığı, zaman kısıtlamaları ve mevcut kaynakların durumu dikkate alınmalıdır.
- Görev için uygun iç denetçilerin seçilmesinde, iç denetim personelinin bilgi, beceri ve diğer kabiliyetleri dikkate alınmalıdır.
- İç denetçilerin eğitim ihtiyaçları da dikkate alınmalıdır, çünkü her görevlendirme, iç denetim faaliyetinin gelişme ihtiyaçlarının karşılanmasına hizmet eder ve buna yardımcı olur.
- Ek bilgi, beceri ve diğer kabiliyetlerin gerektiği durumlarda, kurum dışı kaynakların kullanılması da düşünülmeli ve dikkate alınmalıdır.

# Uygulama Önerisi 2240-1: Görev Programı

Uluslararası İç Denetim Standartlarından
Standart 2240'ın Yorumu

## İlgili Standart

**2240 Görev İş Programı**
İç denetçiler, görev amaçlarına yönelik iş programları hazırlamalıdır. Bu iş programları, kayıtlı hâle getirilmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, belirli bir görev için iş programı hazırlarken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu programın hazırlanmasında gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Kullanılan test ve örnekleme teknikleri de dahil görev prosedürleri, mümkünse önceden seçilmeli ve gelişen koşullara göre genişletilmeli veya değiştirilmelidir. Bu konuda, 2210.A1-1 sayılı Uygulama Önerisinde daha ayrıntılı bilgi ve tavsiyeler verilmektedir.

2. Denetçinin objektifliğinin korunması ve görev amaçlarına ulaşılması için makul bir güvence sağlamak amacıyla, bilgi toplama, analiz, yorumlama ve belgelendirme süreçleri incelenmeli ve kontrol edilmelidir.

# Uygulama Önerisi 2240.A1-1: İş Programlarının Onaylanması

Uluslararası İç Denetim Standartlarından
Standart 2240.A1'in Yorumu

## İlgili Standart

**2240.A1** İş programları, görev sırasında uygulanacak bilgi toplama, analiz, değerlendirme ve kaydetme prosedürlerini içermeli ve göstermelidir. İş programı, işe başlanmadan önce onaylanmalıdır; programda yapılan değişiklikler için de derhal onay alınmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iş programını onaylarken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu onay için gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

Çalışma planının onaylanması sürecinde, bu planlar, görevle ilgili işlere başlanmadan önce, İç Denetim Yöneticisi veya onun tayin ettiği kişi tarafından yazılı olarak onaylanmalıdır. Çalışma planlarında yapılan değişiklikler de vakit kaybetmeden onaydan geçirilmelidir. Görevle ilgili işlere başlamadan önce yazılı onay alınmasını engelleyen etkenler var ise, bu onay, *başlangıçta, sözlü* olarak da alınabilir.

# Uygulama Önerisi 2300-1: İç Denetçinin Denetiminde Kişisel Bilgiler Kullanması

Uluslararası İç Denetim Standartlarından
Standart 2300'ün Yorumu

## İlgili Standart

**2300 Görevin Yapılması:**
İç denetçiler, üstlendikleri görevin hedeflerine ulaşmak için yeterli bilgileri belirlemeli, analiz etmeli, değerlendirmeli ve kaydetmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bir güvence veya danışmanlık görevinde kişisel veri ve bilgileri kullanmayı düşündüklerinde aşağıdaki önerileri de dikkate almalıdır. Bu Uygulama Önerisinin, kişisel bilgilerin kullanılması hakkında tam kapsamlı bir kılavuz olmak gibi bir amacı yoktur; sadece kişisel bilgilerin ilgili denetimin yapıldığı ve kurumun faaliyet yürüttüğü ülkede geçerli olan kanunlara ve politikalara uygun bir şekilde kullanılmasının önemini hatırlatmayı amaçlamaktadır.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Bilgi teknolojisi ve iletişimdeki gelişmeler, mahremiyet ve gizlilik konusunda yeni risk ve tehditler yaratmaya devam ettikçe, kişisel mahremiyetin ve bilgilerin korunmasıyla ilgili kaygılar daha da belirgin, merkezî ve evrensel bir hâle gelmektedir. Mahremiyetle ilgili kontroller, dünya ülkelerinin çoğunda iş yapmak için uyulması gereken kanunî gerekler arasındadır.

2. *Kişisel bilgiler*, genellikle, belirli bir bireyle ilgili olan bilgiler ya da başka bilgilerle bağlantı kurulabilecek ayırt edici özellikleri bulunan bilgiler anlamına gelir. Kişisel bilgiler, herhangi bir ortam veya şekilde kaydedilmiş olsun ya da olmasın, maddî olgularla ilgili veya öznel bilgileri içerebilir. Örneğin, şunlar kişisel bilgi kapsamında değerlendirilebilir:

- İsim, adres, kimlik numaraları, gelir seviyesi veya kan grubu,
- Değerlendirmeler, yorumlar, sosyal mevki, sabıka kayıtları veya disiplin cezaları,
- Personel özlük dosyaları, kredi ve borç kayıtları.

3. Çoğunlukla kanunlar kurumların, kişisel bilgileri toplamadan önce veya toplarken kişisel bilgileri hangi amaçlarla topladıklarını bildirmelerini ve bu kişisel bilgileri ilgili bireyin rızasının olduğu veya kanunların emrettiği durumlar dışında, toplama amacı dışında herhangi bir amaçla kullanmamalarını veya açıklamamalarını gerektirir.

4. İç denetçinin hem kendi ülkesinde hem de kurumun faaliyet yürüttüğü başka ülkelerde kişisel bilgilerin kullanımına ilişkin yürülükteki bütün kanunları anlaması ve bunlara uyması önemlidir.

5. İç denetçi, belirli iç denetim görevlerinin yürütülmesinde, kişisel bilgilere erişmenin, onları almanın, incelemenin, tahrif etmenin veya kullanmanın usulsüz ve bazı durumlarda yasa dışı bir hareket olabileceğini bilmelidir.

6. İç denetçinin denetim çalışmasına başlamadan önce bu konuları araştırması ve bu konuda herhangi bir sorusu veya endişesi varsa, kurumun hukuk danışmanından bilgi ve tavsiye istemesi gerekir.

# Uygulama Önerisi 2310-1: Bilgilerin Tespiti ve Tanımlanması

Uluslararası İç Denetim Standartlarından
Standart 2310'un Yorumu

## İlgili Standart

**2310 Bilgilerin Tespiti ve Tanımlanması**
İç denetçiler, görev amaçlarına ulaşmak için yeterli, güvenilir, ilgili ve faydalı olan bilgileri tespit etmeli ve tanımlamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, gereken bilgileri tespit ederken ve tanımlarken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu tespitte gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Görevin amaç ve kapsamıyla ilgili bütün konularda bilgi toplanmalıdır. İç denetçiler, bilgilerin tespit, tanımlama ve incelenmesinde analitik denetim prosedürlerini uygular. Bu prosedürler, mali ve mali olmayan bilgiler arasındaki ilişkilerin incelenmesi ve karşılaştırılması suretiyle uygulanır. İncelenecek olan bilgilerin niteliğinin belirlenmesi amacıyla analitik denetim prosedürlerinin uygulanması; normal şartlar altında, bu bilgiler arasında süreklilik arz eden bağlantılar olabileceği varsayımına dayanır. Normal dışı şartlara örnek olarak, olağandışı, tekrarlamayan işlem ve olaylar; muhasebe, örgütlenme, operasyon, çevre ve teknoloji yapısındaki değişiklikler; verimsizlikler, etkinsizlikler, hatâlar, usulsüzlükler, yolsuzluklar ve yasalara aykırı eylemler sayılabilir.

2. Bilgiler, tespit ve tavsiyelere sağlam ve güvenilir bir dayanak

oluşturacak seviyede yeterli, *tatminkâr (güvenilir)*, ilgili ve faydalı olmalıdır. *Yeterli bilgi,* konuya vâkıf ve tedbirli bir insanın da denetçiyle aynı kanaatlere varmasını sağlayacak kadar somut tesbitlere dayanan, ikna edici nitelikte bilgi anlamına gelir. *Tatminkâr (güvenilir) bilgi*, uygun görev teknikleri kullanılarak elde edilebilecek en iyi ve güvenilir bilgidir. *İlgili bilgi,* tespit ve tavsiyeleri destekleyen ve amaçlarla uyumlu bilgidir. *Faydalı bilgi* ise, kuruma, hedeflerine ulaşmasında yardımcı olan bilgidir.

# Uygulama Önerisi 2320-1: Analiz ve Değerlendirme

Uluslararası İç Denetim Standartlarından
Standart 2320'nin Yorumu

## İlgili Standart

**2320 Analiz ve Değerlendirme**
İç denetçiler, vardıkları sonuçları ve görev sonuçlarını uygun analiz ve değerlendirmelere dayandırmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, belirli bir görevle ilgili sonuçlara varmak amacıyla analiz ve değerlendirmeleri kullanırken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun söz konusu değerlendirme için gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Analitik denetim prosedürleri, iç denetçilere, görev sırasında topladıkları bilgileri verimli ve etkin bir şekilde değerlendirme olanağı sağlar. Bu değerlendirme, iç denetçinin belirlediği veya tanımladığı beklentilerle mevcut bilgilerin karşılaştırılması yoluyla yapılır. Analitik denetim prosedürleri, diğer hususların yanı sıra aşağıdakilerin tespitinde de faydalı olur:
   - Beklenmedik farklar,
   - Beklenen farkların bulunmaması,
   - Potansiyel hatâlar,
   - Potansiyel usulsüzlük veya yolsuzluklar veya mevzuata aykırı eylemler,
   - Başka olağandışı veya tekrarlamayan işlem veya olaylar.

2. Analitik denetim prosedürleri şu işlemleri içerebilir:
    - Mevcut döneme ait bilgilerin, geçmiş dönemlere ilişkin benzer bilgilerle karşılaştırılması,
    - Mevcut döneme ilişkin bilgilerin bütçelerle veya tahminlerle karşılaştırılması,
    - Mali bilgiler ile mali olmayan bilgiler arasındaki ilişkilerin incelenmesi (örneğin, ortalama personel sayısındaki değişikliklerin, personel giderleriyle kıyaslanması),
    - Bilginin unsurları arasındaki ilişkilerin incelenmesi (örneğin, faiz giderlerindeki dalgalanmaların ilgili borç bakiyelerindeki değişikliklerle mukayesesi),
    - Bilgilerin kurumun diğer birimlerindeki benzer bilgilerle karşılaştırılması,
    - Bilgilerin kurumun faaliyet gösterdiği sektörle ilgili benzer bilgilerle karşılaştırılması.

3. Analitik denetim prosedürleri; parasal tutarlar, fiziksel miktarlar, orantılar veya yüzdeler kullanılarak uygulanabilir. Belirli analitik denetim prosedürleri, bunlarla sınırlı kalmamak kaydıyla, oran, eğilim (trend) ve regresyon analizleri, uygunluk testleri, dönemler arası kıyaslamalar ve bütçelerle, tahminlerle ve dış ekonomik verilerle kıyaslamalar gibi yöntemleri içerir. Analitik denetim prosedürleri, iç denetçilere, ek görev prosedürlerini gerekli kılabilecek koşulların belirlenmesinde yardımcı olur. 2200 numaralı standartlarda (Uygulama Önerisi 2210-1) açıklanan ilkelere uygun olarak, iç denetçiler, görevi planlarken a*nalitik denetim prosedürleri*ni uygulamalı ve kullanmalıdır.

4. Analitik denetim prosedürleri, görev sonuçlarını destekleyen bilgilerin incelenmesi ve değerlendirilmesi amacıyla görev sırasında da kullanılmalıdır. İç denetçiler, analitik denetim prosedürlerinin

ne oranda kullanılması gerektiğini tespit etmek için, aşağıda sayılan etkenleri dikkate almalıdır. Bunları inceleyip değerlendirdikten sonra, iç denetçiler, görev amaçlarına ulaşmak için gereken ek denetim prosedürlerini de düşünmeli ve kullanmalıdır.

- İncelenen alanın önem derecesi,
- Denetlenen alandaki risk yönetiminin etkinliğinin ve riskin değerlendirilmesi
- İç kontrol sisteminin yeterliliği,
- Mali ve mali olmayan bilgilerin varlığı ve güvenilirliği,
- Analitik denetim prosedürlerinin sonuçlarının tahmin edilebilirlik derecesi,
- Kurumun faaliyet gösterdiği sektörle ilgili bilgilerin varlığı ve karşılaştırılabilirliği,
- Başka görev prosedürlerin görev sonuçlarına ne nisbette katkıda bulunabileceği.

5. Analitik denetim prosedürleri beklenmedik sonuçlar veya ilişkiler gösterdiği takdirde, iç denetçiler bunları incelemeli ve değerlendirmelidir. Bu inceleme ve değerlendirme sürecinde, iç denetçiler, sonuçların ve ilişkilerin yeterince açıklandığına kanaat getirene kadar, yönetimle mülâkatlara ve başka prosedürlerin uygulanmasına devam etmelidir. Açıklanamayan sonuç veya ilişkiler, bir potansiyel hatâ, usulsüzlük, yolsuzluk veya mevzuata aykırılık gibi önemli bir durumun işareti olabilir. Yeterince açıklanamayan sonuç veya ilişkiler, uygun yönetim kademelerine rapor edilmelidir. İç denetçiler, bu durumlarda, mevcut koşullara uygun eylem ve önlemler tavsiye edebilir.

# Uygulama Önerisi 2330-1: Bilgilerin Kaydedilmesi

Uluslararası İç Denetim Standartlarından
Standart 2330'un Yorumu

## İlgili Standart

**2330 Bilgilerin Kaydedilmesi**
İç denetçiler, vardıkları kanaatlere ve görev sonuçlarına da-yanak teşkil eden bütün bilgileri kaydetmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, belirli bir görevle ilgili bilgileri kaydederken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun buna yönelik bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Görevle ilgili kayıtları içeren çalışma kâğıtları, iç denetçi tarafından hazırlanmalı ve iç denetim faaliyetinin yönetimi tarafından gözden geçirilmelidir. Çalışma kâğıtlarında toplanan bilgiler ve yapılan analizler kaydedilmeli ve rapor edilecek tespit ve tavsiyelerin dayandığı temellere destek olmalıdır. Görevle ilgili çalışma kâğıtları, genel olarak;
   - göreve ilişkin raporlamaların temel desteğini oluşturur,
   - görevlerin planlanması, uygulanması ve gözden geçirilmesine yardımcı olur,
   - görev amaçlarına ulaşılıp ulaşılmadığını gösterir,
   - üçüncü şahısların incelemelerini kolaylaştırır,
   - iç denetim faaliyetinin kalite programının incelenmesi ve değerlendirilmesine temel oluşturur,
   - sigorta tazminat talepleri, suiistimal iddiaları ve davalar gibi durumlarda destek olur,

- iç denetim personelinin meslekî gelişimine yardımcı olur,
- iç denetim faaliyetinin Uluslararası İç Denetim Standartlarına uyup uymadığını gösterir.

2. Görev çalışma kâğıtlarının düzeni, tasarımı ve içeriği, görevin niteliğine bağlıdır. Denetimle ilgili çalışma kâğıtlarında, görev sürecinin aşağıdaki safhaları yer almalıdır:
   - Planlama,
   - İç kontrol sisteminin uygunluğu, yeterliliği ve verimliliğinin incelenmesi ve değerlendirilmesi,
   - Uygulanan prosedürler, toplanan bilgiler ve varılan sonuçlar,
   - Gözden geçirme,
   - Raporlama,
   - Takip.

3. Çalışma kâğıtları tam ve eksiksiz olmalı ve varılan sonuçları destekler mahiyette olmalıdır. Çalışma kâğıtları, diğer şeylerin yanı sıra, şu bilgi ve belgeleri içermelidir:
   - Planlama belgeleri ve görev programları,
   - Kontrol soru formları, akış şemaları, kontrol listeleri ve rapor formları,
   - Görüşmelerde tutulan notlar ve tutanaklar,
   - Örgütlenme şemaları ve iş tanımları gibi kuruma ait veriler,
   - Önemli sözleşme ve anlaşmaların suretleri,
   - Operasyonel ve mali politikalar hakkında bilgiler,

- Kontrol değerlendirmelerinin sonuçları,
- Teyit ve temsil mektupları,
- İşlemler, süreçler ve hesap bakiyeleri hakkında test ve analizler,
- Analitik denetim prosedürlerinin sonuçları,
- Görev hakkında nihaî raporlamalar ve yönetimin bunlar karşısındaki kararları,
- Varılan sonuçları tevsik eden görevle ilgili yazışmalar.

4. Çalışma kâğıtları kâğıt, bant, disk, disket, film veya başka ortamlarda olabilir. Çalışma kâğıtları kâğıt dışındaki bir ortamda kayıtlıysa, bunların yedek kopyalarının alınmasına dikkat edilmelidir.

5. İç denetçiler mali bilgiler hakkında raporlama yapıyorsa, çalışma kâğıtları muhasebe kayıtlarının bu mali bilgilerle uyumlu olup olmadığını ve gerekli hesap mutabakatının yapılıp yapılmadığını göstermelidir.

6. Uygulanan çeşitli görev türlerine göre çalışma kâğıdı politikaları, İç Denetim Yöneticisi tarafından belirlenmelidir. Soru formları ve denetim programları gibi standart görev çalışma kâğıtları, bir görevin etkinliğini artırabilir ve görevle ilgili işlerin başkalarına havale edilmesini kolaylaştırabilir. Bazı çalışma kâğıtları, '*sürekli*' veya '*ileride de kullanılacak*' *görev dosyaları* olarak sınıflandırılabilir. Bu dosyalar, genellikle, önemini her zaman koruyan bilgileri içerir.

7. Tipik çalışma kâğıdı hazırlama teknikleri aşağıda açıklanmaktadır:

   - Her çalışma kâğıdında görevin adı belirtilmeli ve çalışma kâğıdının içeriği veya amacı açıklanmalıdır.

- Her çalışma kâğıdı, işi yapan iç denetçi tarafından imzalanmalı (veya paraflanmalı) ve üzerine tarih atılmalıdır.
- Her çalışma kâğıdı, bir dizin veya referans numarası içermelidir.
- Denetim doğrulama sembolleri (işaretler) açıklanmalıdır.
- Veri kaynakları açıkça beliritilmelidir.

# Uygulama Önerisi 2330.A1-1: Görev Kayıtlarının Kontrolü

Uluslararası İç Denetim Standartlarından
Standart 2330.A1'in Yorumu

## İlgili Standart

2330.A1 İç Denetim Yöneticisi, görev kayıtlarına erişimi kontrol etmelidir. İç Denetim Yöneticisi, gerektiğinde, bu kayıtları kurum dışı taraflara vermeden önce, üst yönetimin ve/veya hukuk danışmanının onayını almalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görev kayıtlarının kontrolüyle ilgili olarak aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu kontrol için gerekli olabilecek bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak, isteğe bağlıdır.***

1. Görev çalışma kâğıtları, kurumun mülkiyetindedir. Çalışma kâğıtlarını içeren dosyalar, genellikle, iç denetim faaliyetinin kontrolünde kalmalı ve sadece yetkili kişilerin erişimine açık olmalıdır.

2. Kurumun yönetimi ve diğer elemanları da çalışma kâğıtlarına erişim hakkı talep edebilir. Bu erişim, tespit ve tavsiyeleri kanıtlamak veya açıklamak için ya da görev evrakını işle ilgili başka amaçlarla kullanmak için gerekli olabilir. Bu erişim talepleri, İç Denetim Yöneticisinin onayına tâbi olmalıdır.

3. İç ve dış denetçiler, genellikle ve yaygın olarak, birbirlerine, denetim çalışma kâğıtlarına erişim imkânı tanır. Dış denetçilerin çalışma kâğıtlarına erişimi İç Denetim Yöneticisinin onayına tâbi olmalıdır.

4. Dış denetçilerden başka, kurum dışından tarafların da denetim çalışma kâğıtlarına ve raporlara erişim talebinde bulunması mümkündür. Bu durumda, belgeler dışarı verilmeden önce, İç Denetim Yöneticisi, üst yönetimin ve/veya hukuk danışmanının onayını almalıdır.

# Uygulama Önerisi 2330.A1-2: Görev Kayıtlarına Erişim Hakkı Verilmesine Dair Hukukî Mülâhazalar

Uluslararası İç Denetim Standartlarından
Standart 2330.A1'in Yorumu

## İlgili Standart

**2330.A1** İç Denetim Yöneticisi, görev kayıtlarına erişimi kontrol etmelidir. İç Denetim Yöneticisi, gerektiğinde, bu kayıtları kurum dışı taraflara vermeden önce, üst yönetimin ve/veya hukuk danışmanının onayını almalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim faaliyeti dışından kişilerin görev kayıtlarına erişmesine izin verirken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu bağlamda ifade edilebilecek bütün hususları kapsamak gibi bir amacı yoktur.* ***Uygulama Önerilerine uymak isteğe bağlıdır****.*

***Dikkat:*** *İç denetçilerin hukukî sorunlarla ilgili tüm konularda hukuk danışmanına danışması tavsiye edilir; çünkü erişim koşulları, farklı ülkelerde önemli farklılıklar arz edebilir. Bu Uygulama Önerisindeki tavsiyeler, temel olarak Amerika Birleşik Devletleri'nin hukuk sistemine dayanmaktadır.*

1. İç denetim görev kayıtları; bunların hangi ortamda tutulduğuna ve saklandığına bakılmaksızın, raporları, rapor eklerini, inceleme notlarını ve yazışmaları içerir. Görev kayıtları, denetim hizmetlerinin verildiği yönetim ve yönetişim birimlerinin de desteğiyle, iç denetçiler tarafından tutulur ve hazırlanır. Görev kayıtları, genellikle, içeriklerinin gizli olduğu ve bu kayıtların hem *tesbitleri* hem de *kanaatleri* içerebileceği varsayımıyla hazırlanır. Ancak, kuruma veya iç denetim sürecine âşinâ olmayan kişiler, bu tesbit ve kanaatleri yanlış anlayabilir. Kurum dışından

kişilerin görev kayıtlarına erişimi; ceza kovuşturmaları, hukuk davaları, vergi denetimleri, idarî inceleme ve soruşturmalar, devletin sözleşme incelemeleri ve özerk kuruluşların yaptığı incelemeler gibi çeşitli farklı işlemlerde de istenmektedir. Avukat-müvekkil ilişkisinin gizliliği ilkesi ihlâl edilmediği müddetçe bütün kurum kayıtlarına, ceza kovuşturmaları ve davalarında erişilebilir. Ceza kovuşturmaları ve davaları dışındaki işlemlerde bu erişim konusu o kadar açık olmayıp kurumun tâbi olduğu mevzuata göre değişir.

2. İç denetim faaliyetinin aşağıdaki düzenlemelerine ilişkin şeffaf ve kolay anlaşılır uygulamalar, kayıtlara erişim kontrolünü kuvvetlendirebilir. Bu öneriler, aşağıdaki paragraflarda tartışılmaktadır:
   - Yönetmelik
   - İş tanımları
   - Kurum içi birimlere ilişkin politikalar
   - Hukuk danışmanıyla birlikte yürütülen soruşturmalara ilişkin prosedürler

3. Kuruma ait tüm kayıtların, bilgilerin erişimi ve kontrolü meselesi, kayıtların hangi ortamda saklandığına bakılmaksızın, iç denetim yönetmeliğinde düzenlenmelidir.

4. İç denetim faaliyetinde, işler, çeşitli ve karmaşık görevlere de açıklık getirecek şekilde, yazılı olarak tanımlanmalıdır. Bu tanımlar, iç denetçilerin görev kayıtlarına erişimini kolaylaştırabilir; ayrıca iç denetçilerin yaptıkları işin kapsamını anlamalarına; kurum dışı kişilerin ise iç denetçilerin vazifelerini kavramalarına yardımcı olur.

5. İç denetim biriminin çalışmalarını düzenleyen birim içi politikalar hazırlanmalıdır. Bu yazılı uygulamalar, diğer konuların yanı sıra,

görev kayıtlarına nelerin dahil edileceği, kayıtların saklanma süresini, kurum dışından gelen kayıtlara erişim taleplerinin değerlendirme usulünü, ve hukuk danışmanı ile yürütülen soruşturmalarda takip edilecek yöntemleri kapsamalıdır. Bunlar aşağıda tartışılmaktadır.

6. Politikalarda görev kayıtlarının içeriği, formatı ve iç denetçilerin kendi inceleme notlarının akıbeti (diğer bir deyişle, notların, ortaya çıkmış ve halledilmiş bir meselenin kaydı olarak saklanmasının mı, yoksa üçüncü şahısların kayıtlara erişiminin engellenmesini teminen imhasının mı uygun olacağı) açıkça ifade edilmelidir. Politikalarda, ayrıca, görev kayıtlarının ne kadar süreyle tutulacağı ve saklanacağı da gösterilmelidir. Bu süre sınırlamaları, hem kurumun ihtiyaçlarına hem de kanun hükümlerine göre tespit edilir. (Bu konuda da hukuk danışmanıyla istişare edilmesi önemlidir.)

7. Birim politikalarında, birim kayıtlarının kontrol ve güvenliğinden kurum içinde kimin sorumlu olduğu, kime görev kayıtlarına erişim izni verilebileceği ve erişim taleplerinde izlenmesi gereken usul açıklanmalıdır. Bu politikalar, kurumun faaliyet gösterdiği sektör veya ülkedeki genel uygulamalara ve kurumun tâbi olduğu mevzuata bağlı olabilir. İç Denetim Yöneticisi ve iç denetimde görevli diğer kişiler, sektördeki uygulama değişikliklerine ve hukukî emsal teşkil eden yeni gelişmelere karşı müteyakkız olmalıdır. Bu kişiler, bir gün çalışma kayıtlarına kimin erişim talebinde bulunabileceğini tahmin edebilmelidir.

8. Görev kayıtlarına erişim hakkının verilmesine ilişkin bir politika, aşağıda sayılan konulara da temas etmelidir:
    - Erişim sorunları ve ihtilâflarının çözümlenme süreci,
    - her türlü çalışma belgelerinin saklanma süreleri,
    - İç denetim personelinin çalışma belgelerine erişim riskleri ve

sorunları konusunda meslekî açıdan yetiştirilmesi ve sürekli bir eğitime tâbi tutulması süreci

- Gelecekte kimlerin çalışma belgelerine erişim talebinde bulunabileceğini belirlemek amacıyla sektörde dönemsel incelemeler yapmak gerektiği.

9. Bir politika, iç denetçiye, bir denetimin ne zaman bir soruşturmayı gerektirdiğini, yani bir denetimin ne zaman bir avukatla yürütülmesi gereken bir soruşturma haline geldiğini ve hukuk danışmanıyla iletişimlerde hangi özel prosedürlerin uygulanması gerektiğini tespit etmesinde yol göstermelidir. Politika, avukat görevlendirme mektubunun, avukata verilecek bilgilerin gizliliğinin korunmasını temin edecek şekilde düzenlenmesini de kapsamalıdır.

10. İç denetçiler, ayrıca, denetim ve yönetim kurulu üyelerini ve yönetimi, görev kayıtlarına erişimin riskleri hakkında eğitmeli ve bilgilendirmelidir. Kimlerin görev kayıtlarına erişimine izin verilebileceğine, bu taleplerin nasıl işleme konulacağına ve denetimin soruşturma açılmasını gerektirdiğinde hangi prosedürlerin uygulanması gerektiğine ilişkin politikalar, yönetim kurulunun denetim komitesi (veya dengi bir yönetim birimi) tarafından incelenmelidir. Bu konuya özel politikalar, kurumun niteliğine ve kanunlarla belirlenmiş erişim imtiyazlarına ve haklarına bağlı olarak, farklılık gösterir.

11. Kurum dışına bir açıklama yapmak gerektiğinde, görev kayıtlarının dikkatle hazırlanması önemlidir. Bu yapılırken, şu kurallara uyulmalıdır:

    - Sadece istenen belgeler açıklanmalı veya verilmelidir. İçinde kanaat ve tavsiyeler bulunan görev kayıtları genellikle yayınlanmaz ve verilmez. Avukatların düşündüğü süreçleri veya stratejileri açıklayan belgeler genellikle gizlidir ve zorunlu açıklamaya tâbi tutulamaz.

- Tüm belgelerin, özellikle kurşun kalemle yazılmışların, orijinalleri saklanmalı ve sadece suretleri verilmelidir. Mahkeme bu belgelerin orijinalini isterse, iç denetim birimi belgenin bir suretini elinde tutmalıdır.
- Her belgeye gizli damgası basılmalı ve başka kişilere izinsiz verilmesinin ve dağıtılmasının yasak olduğunu belirten bir not eklenmelidir.

# Uygulama Önerisi 2330.A2-1: Kayıtların Saklanması

Uluslararası İç Denetim Standartlarından
Standart 2330.A2'nin Yorumu

## İlgili Standart

**2330.A2** İç Denetim Yöneticisi, görev kayıtlarının saklanmasına ilişkin esasları belirlemelidir. Bu esaslar,kurumun temel ilkelerine ve ilgili mevzuata uygun olmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, kayıt saklama esaslarını belirlerken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu esaslar belirlenirken dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

Kayıt saklama esasları, kayıtların hangi formatta tutulduğuna ve saklandığına bakılmaksızın, bütün görev kayıtlarını kapsayacak şekilde düzenlenmelidir.

# Uygulama Önerisi 2340-1: Görevin Gözetim ve Kontrolü

Uluslararası İç Denetim Standartlarından
Standart 2340'ın Yorumu

## İlgili Standart

**2340 Görevin Gözetim ve Kontrolü**

Görevler; görev amaçlarına ulaşılmasını, kalitenin güvence altına alınmasını ve personelin geliştirilmesini sağlayacak bir tarzda gözetlenmeli ve kontrol edilmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, iç denetim görevinin gözetim ve kontrolünü yaparken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu yönde dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. İç denetim görevlerinin uygun ve yeterli bir şekilde gözetim ve kontrolünün yapılmasından İç Denetim Yöneticisi sorumludur. Planlama ile başlayan bu süreç, inceleme, değerlendirme, raporlama ve takip safhalarıyla devam eder. Gözetim ve kontrol şunları içine alır:
   - İç denetçilerin gerekli bilgilere, becerilere ve diğer kabiliyetlere sahip olmasını sağlamak,
   - Planlama safhasında gerekli talimatları vermek ve görev programını onaylamak,
   - Gerekliliği kanıtlanmış ve izni alınmış değişiklikler söz konusu olmadıkça, görev programının onaylandığı hâliyle uygulanıp uygulanmadığını gözetlemek ve kontrol etmek,
   - Görev çalışma kâğıtlarının tespitleri, sonuçları ve tavsiyeleri yeterince destekleyip desteklemediğini değerlendirmek,
   - Raporlamaların açık, doğru, objektif, özlü ve yapıcı olmasını ve zamanında yapılmasını sağlamak,

- Görev amaçlarına ulaşılmasını sağlamak
- İç denetçilerin bilgi, beceri ve diğer kabiliyetlerini geliştirmeleri için uygun imkânlar yaratmak.

2. Gözetim ve kontrole ilişkin uygun belge ve bulgular yazılı hâle getirilmeli ve saklanmalıdır. Gereken denetim kapsamı, iç denetçilerin yeterliliğine, deneyimine ve görevin karmaşıklıklığına bağlıdır. Gözetim ve kontrolün tüm sorumluluğu, İç Denetim Yöneticisine aittir; fakat İç Denetim Yöneticisi bu iş için, iç denetim bölümünden yeterli tecrübeye sahip kişileri de görevlendirebilir. Daha az deneyimli iç denetçilerin işlerinin gözden geçirmek için, yeterli tecrübeye sahip iç denetçiler kullanılabilir.

3. İç denetim birimi tarafından veya iç denetim birimi adına yapıldığına bakılmaksızın bütün iç denetim görevlerinden İç Denetim Yöneticisi sorumludur. İç Denetim Yöneticisi, görevin planlama, inceleme, değerlendirme, raporlama ve takip aşamalarında alınan bütün önemli kararlardan sorumludur. İç Denetim Yöneticisi, bu sorumluluğunun gereğini yerine getirmek için *uygun araç ve yollar* geliştirmelidir. Araç ve yollar terimi, aşağıdaki amaçlarla hazırlanmış politika ve prosedürleri kapsar:

   - İç denetçilerin veya iç denetim birimi adına çalışan başka kişilerin aldığı kararların, İç Denetim Yöneticisinin kararlarına, görevi olumsuz etkiyebilecek kadar, aykırı olması riskini asgarî düzeye indirmek
   - Görevle ilgili önemli konularda, İç Denetim Yöneticisi ile iç denetim personelinin kararları arasındaki farkları gidermek. Bu yol ve araçlardan bazıları şunlar olabilir: (a) tesbit ve bulguların tartışılması, (b) ek araştırma ve/veya inceleme yapılması, (c) çalışma kâğıtlarındaki farklı görüşlerin kaydedilmesi ve farklılıkların uzlaştırılması. Etik bir meselede fikir ayrılığı olması hâlinde, konunun kurumdaki etik

görevlilerine götürülmesi de 'uygun araç ve yollar' terimi içinde değerlendirilebilir.

4. Gözetim ve kontrol sürecine, personelin eğitim ve gelişim çalışmaları, personel performans değerlendirmeleri, zaman ve maliyet kontrolleri ve benzeri başka idarî işler de dahildir.

   Bütün görev çalışma kâğıtları, raporlamaları destekleyip desteklemediklerini ve gereken bütün denetim prosedürlerinin uygulanıp uygulanmadığını tespit etmek amacıyla, gözden geçirilmelidir. Bu işlemin yapıldığının teyidi için, kâğıtların inceleyen kişi tarafından paraflanması ve üzerlerine tarih atılması da gereklidir. Gözetim ve kontrolün yapıldığını teyide yarayan diğer teknikler arasında, gözden geçirme kontrol listesi kullanılması; gözden geçirmenin niteliği, kapsamı ve sonuçlarını gösteren bir *not hazırlanması* ve/veya elektronik çalışma kâğıdı yazılımlarında, değerlendirme ve onaya yer verilmesi sayılabilir.

5. Tüm görev çalışma kâğıtları, yapılan raporlamaları gerektiği şekilde desteklediklerinden ve gerekli tüm denetim prosedürlerinin yerine getirildiğinden emin olunacak şekilde gözden geçirilmelidir. Gözden geçirmenin yapıldığına dair kanıtlar, gözden geçirenin her gözden geçirmeden sonra attığı parafı ve tarihi de içermelidir. Bu yönde kanıt sağlayacak diğer teknikler arasında, görev çalışma kâğıdı gözden geçirme kontrol listesinin kullanılması, gözden geçirmenin nitelik, kapsam ve sonuçlarını gösteren bir tutanak düzenlenmesi ve/veya elektronik çalışma kâğıdı yazılımı içinde bir değerlendirme ve kabul yöntemi de sayılabilir.

6. Gözden geçirme yapanlar, gözden geçirme sürecinde ortaya çıkan sorular hakkında yazılı bir kayıt gözden geçirme notları) oluşturabilir. Gözden geçirme notları düzenlenirken, çalışma kâğıtlarında gözden geçirme sırasında ortaya çıkan soruların cevaplandığını tevsikeden yeterli kanıt olduğundan emin olmak

gerekir. Gözden geçirme notlarının kullanılmasıyla ilgili kabul edilebilir seçenekler şunlardır:

- Gözden geçirme notlarının, gözden geçirmeyi yapan kişinin sorduğu soruların ve aldığı yanıtların bir kaydı olarak saklanması
- Sorulan soru yanıtlandıktan ve ilgili çalışma kâğıtları istenen ek bilgileri de içerecek şekilde değiştirildikten sonra, gözden geçirme notlarının atılması.

# Uygulama Önerisi 2400-1: Sonuçların Raporlanmasına Dair Hukukî Mülâhazalar

Uluslararası İç Denetim Standartlarından
Standart 2400'ün Yorumu

## İlgili Standart

**2400 Sonuçların Raporlanması**
İç denetçilerin görev sonuçlarını raporlaması gerekir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, denetim sonuçlarını raporlarkenr aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun sonuçların raporlanmasında dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

**Dikkat:** *İç denetçilerin hukukî sorunlarla ilgili tüm konularda hukuk danışmanına danışması tavsiye edilir; çünkü konuyla ilgili koşullar ülkeler arasında önemli farklılıklar arz edebilir. Bu Uygulama Önerisindeki tavsiyeler, temel olarak Amerika Birleşik Devletleri'nin hukuk sistemine dayanmaktadır.*

1. İç denetçiler, mevzuat ihlâlleriyle ve başka hukukî sorunlarla ilgili denetim raporlarında ve çalışma kâğıtlarında sonuçları açıklarken ve fikir beyan ederken dikkatli olmalıdır. Bu konuları düzenleyen yerleşik politika ve prosedürlerin bulunması ve ilgili başka bölümlerle (hukuk danışmanı, mevzuata uyum, vb.) yakın bir çalışma ilişkisinin kurulması şiddetle tavsiye ve teşvik edilir.

2. İç denetçilerin delil toplamaları, analitik kararlar almaları, sonuçları rapor etmeleri ve gereken düzeltici tedbirlerin alınmasını sağlamaları gerekir. İç denetçinin görev kayıtlarını kaydetmesi ve belgelendirmesi koşulu, hukuk danışmanının savunmaya zarar verebilecek kanıt bırakmama isteğiyle çelişebilir. Örneğin, bir iç

denetçi bir inceleme ve soruşturmayı gerektiği gibi yapsa bile, ortaya çıkan olaylar, kurumun hukuk danışmanının iddiaları ve savunmalarına zarar verebilir. Aniden yapılan bir açıklamanın hukuk danışmanının ve iç denetçinin birbirleriyle çelişmesine yol açmasını önlemek için uygun planlama ve politikalar şarttır. Bu politikalar, *rol tanımlarını* ve *raporlama yöntemlerini* içermelidir. İç denetçi ve kurumun hukuk danışmanı, kurum yönetimini, belirlenmiş politikalar konusunda eğiterek ve bu konuda hassas davranmalarını sağlayarak, tüm kurum içinde etik ve önleyici bir bakış açısını da teşvik etmelidir. İç denetçiler, özellikle görev sonuçlarının kurum dışından kişilere açıklanması veya raporlanmasını gerektirebilecek görevlerde aşağıdakileri dikkate almalıdır:

3. Avukat-müvekkil ilişkisinin gizliliğinin korunabilmesi için gerekli dört unsur vardır. Bunun için,

   - Müvekkil için hukukî yardım istemek, almak veya vermek amacıyla
   - "bu imtiyaza sahip kişiler" arasında,
   - gizlilik içinde yapılan
   - bir iletişim

söz konusu olmalıdır.

Esas olarak avukatlarla yapılan iletişim ve görüşmelerin gizliliğini korumak amacını güden bu imtiyaz, avukatla birlikte çalışan üçüncü kişilerle yapılan iletişim ve görüşmelere de uygulanabilir.

4. Bazı mahkemeler, denetim çalışmaları sırasında oluşan belgeler gibi özeleştiri (kurum içine özel kendini değerlendirme) malzemelerini, dışarıya açıklanmaya karşı, koruyan bir 'özeleştiri imtiyazı' tanımaktadır. Genellikle, bu imtiyazın altında yatan mantık, dava konusu örneklerde, yapılan denetimin gizliliğinin

korunmasının sağlayacağı faydanın, söz konusu bilgilerin açıklanmasıyla temin edilecek kamu yararından daha fazla olduğudur. Bir mahkemenin bu konuda yaptığı açıklama şöyledir: *"Özeleştiriye yönelik analizlere tanınan gizlilik imtiyazı, bu nitelikteki değerlendirmelerin dışarıya açıklanmasını engelleyen bir 'şartlı imtiyaz' olarak kabul edilmiştir. Bu imtiyaz, kişilerin veya işletmelerin, ileride açılabilecek davalarda hasımlarınca aleyhlerine kullanabilecek bir delili kendi elleriyle yaratma korkusu olmadan, mevzuata uyup uymadıklarını samimi bir şekilde değerlendirmesini mümkün kılmaktadır. Bu doktrinin gerekçesi, bu tür özeleştiri niteliğindeki değerlendirmelerin, kurumların hukuku gözetme eğilimini güçlendirmesi ve bunun da son tahlilde kamu menfaatine bir durum olduğu düşüncesidir."*

5. Genel olarak, bu şartlı gizlilik imtiyazından istifade edebilmek için üç hususun yerine getirilmiş olması gerekir:
   - Bilgiler, imtiyaz talep eden tarafın yaptığı bir özeleştiri sonucunda elde edilmiş olmalıdır
   - Bu eleştirel analize konu bilgilerin serbest akışının korunmasında kamunun güçlü bir menfaati bulunmalıdır
   - Bilgilerin, açıklanmasına izin verildiği takdirde, serbest akışı kesilecek türde bilgiler olması gerekir.

Bazı durumlarda, mahkemeler, bu eleştirel analizin ilgili davacının zarara maruz kalmasından önce olup olmadığına veya davacının zararına neden olup olmadığına da bakmaktadır. Analizin davaya yol açan olaylardan sonra olması hâlinde, bu imtiyazın gerekçesinin en güçlü seviyede olduğu söylenir.

6. Belgelerin bir özel kişi tarafından değil de bir devlet kuruluşu tarafından talep edildiği durumlarda, mahkemeler bu özeleştiri niteliğindeki değerlendirmelere gizlilik imtiyazı tanımakta, genellikle daha isteksiz davranmaktadır; bu isteksizliğin nedeni,

muhtemelen, kanunların uygulanması konusunda devletin nispeten daha güçlü bir çıkarı olduğu fikridir. Özeleştirel değerlendirme imtiyazı, özellikle, yerleşik özdenetim ve düzenleme prosedürlerine sahip bulunan işlevler ve birimlerle bağlantılıdır. Bu tür prosedürlere sahip olanlar arasında hastahaneler, aracı kurumlar ve muhasebe ve mali müşavirlik firmaları sayılabilir. Bu prosedürlerin çoğu, bir işletme faaliyetine eklenmiş bulunan, mali denetim gibi kalite güvencesi prosedürleriyle ilgilidir.

7. *'Çalışma sonuçları doktrini'* kapsamında, belgeleri açıklama zorunluluğundan korunmak için üç hususun yerine getirilmesi gerekir: Belgeler:
   - herhangi bir çalışma sonucu türüne uymalıdır (örneğin, tutanaklar, bilgisayar programları),
   - bir dava açılabileceği düşüncesiyle hazırlanmış olmalıdır,
   - belgeleri hazırlayan kişi, avukatın bir temsilcisi olmalıdır.

8. Avukat-müvekkil ilişkisi kurulmadan önce hazırlanmış bulunan belgeler, *çalışma sonuçları doktrini* korumasından istifade edemez. Belgelerin avukat-müvekkil ilişkisi kurulmadan önce avukata teslim edilmiş olması, çalışma sonuçları doktrini kapsamında korunma için yeterli değildir. Ayrıca söz konusu doktrin, sınırlı bir şekilde uygulanabilir. Önemli bir bilgi ihtiyacı varsa ve bu bilgiler aşırı bir güçlük olmadan başka kaynaklardan temin edilemiyorsa, belgeler bu doktrinin korumasından istifade edemez. *Grand Jury* davasında, şirketin denetim komitesi, yabancı ülkelere kuşkulu bir ödeme yapılıp yapılmadığını tespit etmek amacıyla kişilerle görüşmeler yaptı. Denetim komitesinin raporu, ölmüş kişilerle yapılan görüşmelerin sonuçlarını içeren kısımları hariç, *çalışma sonuçları doktrini* kapsamında açıklama zorunluluğuna karşı korundu.

# Uygulama Önerisi 2410-1: Raporlama Kıstasları

Uluslararası İç Denetim Standartlarından
Standart 2410'un Yorumu

## İlgili Standart

**2410 Raporlama Kıstasları**
Raporlamalar, varılan sonuçlar, yapılan tavsiyeler ve önerilen eylem planlarının yanında görevin hedeflerini ve kapsamını da içermelidir.

## İlgili Standart

**2410.A1** Sonuçları gösteren nihaî rapor, gerektiğinde, iç denetçinin görüş ve kanaatlerini de içermelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görevlerin sonuçlarını rapor ederken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. Görevle ilgili nihaî raporların formatı ve içeriği kurumdan kuruma veya görevin türüne göre değişmesine rağmen, her raporda, en azından, görevin amacı, kapsamı ve sonuçları ifade edilmelidir.

2. Görevle ilgili nihaî raporlarda, temel (arkaplan) bilgiler ve özetler de yer alabilir. *Temel bilgiler*, denetlenen birimlerin ve faaliyetlerinin anlaşılmasını sağlar ve gerekli bilgi ve verileri sunar. Bu temel bilgiler, daha önceki raporlarda bulunan tespitlere, sonuçlara ve tavsiyelere de yer verebilir; raporun önceden programlanmış bir görevin sonucu mu, yoksa talep üzerine yapılan bir denetimin sonucu mu olduğunu bildirir. Raporda yer verilmişse, *özetler*, raporun esasını verecek nitelikteki ifadelerden ibaret olmalıdır.

3. Raporun "*Amaçlar*" başlığı altında, görevin hedefleri açıklanmalıdır. Gerektiğinde, okuyucu bu kısımda, görevin neden yapıldığı ve görevden ne beklendiği konusunda bilgilendirilebilir.

4. Raporun "*Kapsam*" başlığı altında, denetlenen faaliyetler belirtilmeli ve denetimin kapsadığı süre dilimi gibi destekleyici bilgiler (gerektiğinde) verilmelidir. Görevin sınırlarını açıkça çizmek amacıyla, gerekirse, denetlemeye konu olmayan ilgili faaliyetler de belirtilmelidir. Yapılan görev konusu işlerin niteliği ve kapsamı da tanımlanmalıdır.

5. Görev sonuçları; *tespitleri, kanaatleri, tavsiyeleri ve eylem planlarını* içermelidir.

6. *Tespitler*, maddî olay ve olgularla ilgili açıklamalardır. İç denetçinin vardığı sonuçları ve yaptığı tavsiyeleri desteklemek veya bunların yanlış anlaşılmasını önlemek için gerekli görülen tespitler, nihaî görev raporlarına dahil edilmelidir. Daha az önemli görülen tespitler veya tavsiyeler de gayriresmî yollarla bildirilebilir.

7. Görevle ilgili tespit ve tavsiyeler, 'olanlar' ile 'olması gerekenlerin' karşılaştırılması sonucu ortaya çıkar. Bu karşılaştırmada bir fark bulunsa da bulunmasa da, iç denetçi, raporunu üzerinde bina edebileceği bir temel kurmuş olur. Mevcut durum kıstaslara uygunsa, raporda, tatmin edici performans teyidi vermek uygun olabilir. Gözlem ve tavsiyeler, aşağıdaki özelliklere dayanmalıdır:

    - *Kıstas*: Bir değerlendirme ve/veya doğrulama yapmak için kullanılan standartlar, ölçüler veya beklentilerdir (ne olmalıdır?).
    - *Tesbit*: İç denetçinin denetleme sırasında elde ettiği belge ve bulgulardır (olan nedir?).
    - *Sebep*: Beklenen koşullar ile mevcut koşullar arasında tespit edilen farkın sebebidir (neden böyle bir fark mevcuttur?).

- *Etki* (Sonuç): Tesbitlerin kıstaslara uygun olmamasından dolayı kurumun ve/veya başkalarının karşı karşıya olduğu risk veya risk maruziyetidir (farkın etkisi nedir?). Bu riskin veya riske maruz kalma derecesinin belirlenmesinde, iç denetçi, görevle ilgili gözlem ve tavsiyelerinin, kurumun faaliyetleri ve mali tabloları üzerinde yapabileceği etkiyi düşünmelidir.
- Tesbit ve tavsiyeler, başka bir yerde söz konusu edilmemişse, denetlenenin başarılarını, ilgili konuları ve destekleyici bilgileri de içerebilir.

8. *Sonuç ve kanaatler,* iç denetçinin denetleme konusu faaliyetlere ilişkin tespit ve tavsiyelerinin nelere yol açabileceği hakkındaki değerlendirmesini yansıtır. Bu bölümde, genellikle, tespit ve tavsiyeler, bunların genel etkilerine dayanan bir bakış açısıyla yansıtılır. Görev raporuna dahil edilmişse, görevle ilgili sonuçların açıkça tanımlanması ve belirtilmesi gerekir. Sonuçlar, bir görevin kapsamının tamamını ya da sadece belirli yönlerini kapsayabilir. Sonuçlar; bunlarla sınırlı kalmamak kaydıyla, faaliyet veya program hedeflerinin ve amaçlarının kurumun hedef ve amaçlarına uyup uymadığını, kurumun hedef ve amaçlarına ulaşılıp ulaşılmadığını ve inceleme konusu olan faaliyetin amaçlandığı gibi çalışıp çalışmadığını da kapsayabilir. İç denetçinin görüşü, gözden geçirilen alan veya kontrollerin genel bir değerlendirmesini içine alabileceği gibi, gözden geçirmenin belli cepheleriyle veya belirli kontrollerle sınırlı da olabilir.

9. Görevle ilgili raporlamalar, potansiyel iyileşmeler hakkında tavsiyeleri, tatmin edici performans başarılarını ve düzeltici tedbirleri de içermelidir. Öneriler, iç denetçinin kendi tespit ve kanaatlerine dayanır. Öneriler kısmında, mevcut durumun düzeltilmesi veya faaliyetlerin iyileştirilmesine yönelik eylem çağrısı yapılır; bu kısımda yönetime, istenen sonuçlara ulaşması konusunda yol göstermek için, performansın düzeltilmesi veya iyileştirilmesine yönelik yaklaşımlar da önerilebilir. Öneriler genel veya özel nitelikte olabilir. Örneğin, bazı durumlarda, hem genel bir eylem tarzı hem

de uygulama için bazı özel öneriler sunmak uygun olabilir. Bazı durumlarda ise, sadece daha ayrıntılı bir araştırma veya inceleme önermek uygun olabilir.

10. Nihaî rapora, denetlenenlerin son denetlemeden bu yana sağladığı gelişmeler veya sürdürdüğü faaliyetlerin üzerinde iyi bir kontrol sistemi kurması gibi başarıları da yazılabilir. Bu bilgiler, mevcut durumu âdil bir şekilde yansıtmak ve görevle ilgili nihaî rapora daha uygun bir bakış açısı ve denge kazandırmak amacıyla gerekli olabilir.

11. Raporlamalarda, iç denetçinin vardığı sonuç, kanaat ve tavsiyeleri hakkında denetlenenlerin ne düşündüğüne de yer verilebilir.

12. İç denetçi, denetlenenlerle yaptığı müzakere ve görüşmelerde, gerekirse, görev sonuçları hakkında ve faaliyetleri iyileştirmek amacına yönelik bir eylem planı hakkında mutabakat sağlamaya çalışmalıdır. İç denetçi ve denetlenen, sonuçlar konusunda anlaşamadıkları takdirde, görevle ilgili raporlamalarda her iki tarafın görüşleri ve anlaşmazlık sebepleri de açıklanabilir. Denetlenenin yazılı görüşleri, görev raporuna bir ek olarak da ilâve edilebilir. Buna alternatif olarak, denetlenenin görüşleri, raporun içinde ya da bir kapak mektubunda da açıklanabilir.

13. Belirli bilgiler, gizlilik imtiyazlı, özel veya yasa dışı eylemlerle ilgili oldukları için, bütün rapor alıcılarına açıklanması uygun olmayabilir; ancak bu tür bilgiler, ayrı bir raporda açıklanabilir. Rapor edilen olay veya durumlar sadece üst yönetimi ilgilendiriyorsa, raporun sadece kurumun denetim komitesi ve yönetim kuruluna verilmesi gerekir.

14. *Ara raporlar* yazılı veya sözlü olabilir ve resmî veya gayriresmî olarak raporlanabilir. Derhal ilgilenilmesi ve işlem yapılması gereken bilgileri raporlamak için denetlenen faaliyetle ilgili bir

değişikliği bildirmek için veya görevin uzun bir süre devam etmesi hâlinde görevin seyri hakkında yönetimi bilgilendirmek için ara raporlar yazılabilir. Ancak *ara raporların* yazılması, bir nihaî rapor yazma ihtiyacını ortadan kaldırmaz.

15. Görev bittikten sonra imzalı bir rapor hazırlanmalıdır. Denetlenenin üzerindeki yöneticiler için, görev sonuçlarını açıklayan *özet raporlar* uygun olabilir. Bu raporlar, nihaî rapordan ayrı olarak ya da nihaî raporla bağlantılı olarak hazırlanabilir. "*İmzalı rapor*" terimi, rapora yetkili iç denetçi tarafından manuel olarak isminin yazılması (imzalanması) anlamına gelir. Alternatif olarak, sadece bir kapak mektubu da imzalanabilir. Raporu imzalamaya yetkili olan iç denetçi, İç Denetim Yöneticisi tarafından tayin edilmelidir. Görev raporları elektronik yollarla dağıtıldığı takdirde, iç denetim faaliyeti, raporun imzalı bir versiyonunu arşivinde saklamalıdır.

# Uygulama Önerisi 2420-1: Raporlamaların Kalitesi

Uluslararası İç Denetim Standartlarından
Standart 2420'nin Yorumu

## İlgili Standat

**2420 Raporlamaların Kalitesi**
Raporlamalar, doğru, objektif, açık, özlü, yapıcı, tam olmalı ve zamanında sunulmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görevlerin sonuçlarını raporlarken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. *Doğru* raporlamalarda hatâ ve saptırma bulunmaz ve bu tür raporlamalar, ilgili maddî olay ve gerçeklere sâdık kalır. İlgili veri ve delillerin dikkatle ve hassasiyetle toplanması, değerlendirilmesi ve raporda özetlenmesi gerekir.

2. *Objektif (nesnel)* raporlamalar, âdil, tarafsız, belge ve bulgular karşısında dürüst ve dengeli bir değerlendirmenin ürünüdür. Tespit, sonuç ve tavsiyeler, önyargısız ve tarafsız bir şekilde, kişisel çıkarlar göz önüne alınmadan ve başkalarının etkisi altında kalınmadan tespit ve ifade edilmelidir.

3. *Açık* raporlamalar, kolay anlaşılır ve mantıklıdır. Raporda açıklık, gereksiz teknik terimler kullanmaktan kaçınarak ve ilgili bütün önemli bilgiler verilerek sağlanabilir.

4. *Özlü* raporlamalar, konunun özüne inen, gereksiz ve fazla

ayrıntılardan kaçınan ve lâf kalabalığı yapmayan raporlardır. Bu tür raporlar, raporun dikkatle gözden geçirilmesi ve derlenmesi yoluyla hazırlanır. Amaç, sunulan her düşüncenin anlamlı, fakat özlü ve kısa olmasıdır.

5. *Yapıcı* raporlamalar, denetlenenlere ve kuruma faydalı olan, gereken iyileştirme ve geliştirmeleri yapmalarına yardımcı olan raporlardır. Raporun içeriği ve tonu, faydalı, olumlu, anlamlı olmalı ve kurumun hedeflerine ulaşmasına katkıda bulunmalıdır.

6. *Tam raporlamalar,* hedef okuyucu kitlesi için önemli olan hiçbir bilgiyi atlamaz; tavsiye ve sonuçları desteklemek için gereken bütün bilgi ve tespitleri içerir.

7. *Zamanında sunulan* raporlar, tavsiyelere dayanarak tasarrufta bulunabilecek kişilerin dikkatle değerlendirebilmesi için tam zamanında ve uygun zamanda verilen raporlardır. Görev sonuçlarıyla ilgili raporun zamanlaması, gereken eylemlerin derhal ve etkin bir şekilde uygulanabilmesini sağlayacak âcil raporlama düzeyinde ve gecikmeden belirlenmelidir.

# Uygulama Önerisi 2440-1: Görev Sonuçlarının Raporlanacağı Taraflar

Uluslararası İç Denetim Standartlarından
Standart 2440'ın Yorumu

## İlgili Standart

**2440 Sonuçların Raporlanması**
İç Denetim Yöneticisi, görev sonuçlarını uygun taraflara raporlamalıdır.

## İlgili Standart

**2440.A1** Görev sonuçlarının öngördüğü tedbirlerin alınmasını sağlayabilecek taraflara, nihaî görev sonuçlarının raporlanmasından İç Denetim Yöneticisi sorumludur.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, görev sonuçlarının raporlamasını yaparken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. İç denetçiler, nihaî görev raporlarını hazırlamadan önce, görev sonuçları ve tavsiyelerini uygun yönetim kademeleriyle tartışmalıdır.

2. Sonuçların ve tavsiyelerin tartışılması, genellikle, görev sırasında ve/veya görev sonrası toplantılarda (son görüşmeler) yapılır. Başka bir usul de, *taslak raporların*, tespitlerin ve tavsiyelerin denetlenen faaliyet ve birimin yönetimi tarafından gözden geçirilmesidir. Bu tartışma ve gözden geçirmelerin amacı, denetlenenler için özel

konuları açıklığa kavuşturma ve tespit, sonuç ve tavsiyeler hakkında görüşlerini ifade etme fırsatı vererek, belge ve bulguların yanlış anlaşılmamasını veya yanlış yorumlanmamasını sağlamaktır.

3. Tartışma ve gözden geçirmelere katılanların düzeyi kurumdan kuruma ve raporun niteliğine göre farklılık göstermekle birlikte, katılanlar, genellikle, faaliyetlerin ayrıntılarına vâkıf veya gerekli tedbirlerin alınmasına izin ve yetki verebilecek kişilerdir.

4. İç Denetim Yöneticisi veya onun tayin ettiği kişi, nihaî görev raporu hazırlanmadan önce, raporu gözden geçirmeli, onaylamalı ve raporun kimlere dağıtılacağına karar vermelidir. İç Denetim Yöneticisi veya tayin ettiği kişi, bütün nihaî raporları onaylamalıdır; bazı durumlarda ise raporlara imza da atabilir. Özel durumlar gerektirdiği takdirde, raporun İç Denetim Yöneticisini temsilen görevli bir denetçi veya başdenetçi tarafından imzalanması da düşünülebilir.

5. Nihaî raporlamalar, görev sonuçlarının *uygulanmasını sağlayabilecek* olan kurum çalışanlarına dağıtılmalıdır. Bunun anlamı şudur: Rapor, gerekli tedbirleri alabilecek veya alınmasını sağlayabilecek pozisyonda olan kişilere ulaşmalıdır. Nihaî raporlar, denetlenen faaliyetin yönetimine de verilmelidir. Kurum içindeki daha üst düzey yetkililere ise sadece özet bir rapor sunulabilir. Raporlar, dış denetçiler, denetim komitesi ve yönetim kurulu gibi diğer ilgili veya etkilenen taraflara da dağıtılabilir.

# Uygulama Önerisi 2440-2: Kurum Dışına Raporlamalar

Uluslararası İç Denetim Standartlarından
Standart 2440'ın Yorumu

## İlgili Standart

**2440 Sonuçların Raporlanması**
İç Denetim Yöneticisi, görev sonuçlarını uygun taraflara raporlamalıdır.

## İlgili Standart

**2440.A2** İç Denetim Yöneticisi, aksi kanunî, hukukî düzenlemelerle emredilmediği takdirde, görev sonuçlarını kurum dışındaki taraflara iletmeden önce, kuruma doğabilecek muhtemel riskleri değerlendirmeli, üst yönetim ve/veya hukuk danışmanı ile istişare etmeli ve sonuçların raporlanmasını, kullanımını kısıtlayarak, kontrol etmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, bilgileri kurum dışından kişilere raporlamaları istendiği takdirde aşağıdaki önerileri dikkate almalıdır. İç denetçilerin iç denetim hizmetini alan kurumun dışından kişilere rapor sunmaları veya başka bilgiler vermeleri istendiği takdirde böyle bir durum söz konusu olur. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama önerilerine uymak isteğe bağlıdır.***

1. İç denetçiler, görev sözleşmesindeki veya kurumsal politika ve prosedürlerdeki, bilgilerin kurum dışına verilmesiyle ilgili hükümleri gözden geçirmelidir. İç denetim yönetmeliğinde ve denetim komitesi yönetmeliğinde de, bilgilerin kurum dışına çıkartılmasıyla ilgili hükümler bulunabilir. Bu tür hükümler yoksa, iç denetçi, kurumun uygun politikalar benimsemesini ve uygulamasını önermelidir. Bu tür politikalara dahil edilebilecek bilgilerin örnekleri aşağıdadır:

- Bilgilerin kurum dışına raporlanma izni ve yetkisi,
- Bilgilerin kurum dışına raporlanmasının onay süreci,
- Kurum dışına raporlamaya izin verilebilecek ve izin verilemeyecek bilgi türlerinin çerçevesi,
- Bilgileri alma yetkisine sahip kurum dışı kişiler ve bu kişilerin alabileceği bilgi türleri,
- Bilgilerin kurum dışına raporlanmasına dair gizlilik düzenlemeleri, mevzuat gerekleri ve hukukî mülâhazalar,
- Bilgilerin kurum dışına çıkartılması sonucunu veren raporlamalara konulabilecek güvence, öneri, görüş ve diğer bilgilerin niteliği.

2. Bilgi talepleri, mevcut bilgilere (örneğin, daha önce hazırlanmış bir iç denetim raporuna) yönelik olabilir. Bilgi talebi, mevcut olmayan bir bilgiye de yönelik olabilir; bu durumda, bilginin oluşturulmasına yönelik yeni bir iç denetim görevi gerekebilir. Talep, mevcut bir bilgi veya rapora yönelik ise, iç denetçi, talebin uygunluğu açısından raporu veya bilgiyi gözden geçirmelidir.

3. Bazı durumlarda, mevcut bir rapor veya bilginin kurum dışına çıkartılmaya müsait hâle getirilmesi amacıyla, kısmen tâdil edilmesi mümkündür. Bazı durumlarda ise, daha önce yapılmış bir çalışmaya dayanarak yeni bir rapor düzenlenebilir. Bu işlemlerin tümü, dikkat ve özenle yapılmalıdır.

4. Bilgiler kurum dışına raporlanırken, aşağıdaki hususlara dikkat edilmelidir:
   - Kurum dışına çıkartılacak bilgiler hakkında yazılı bir anlaşma yapmak gereği,
   - Bilgiyi verenlerin, bilgi kaynaklarının, raporu imzalayanların, bilgiyi alanların ve bilgi veya raporun raporlanacağı kişilerin kimliklerinin belirlenmesi,

- Uygun bilgilerin ne amaçla, hangi kapsamda ve hangi prosedürler takip edilerek oluşturulacağı,
- Raporun veya kanaatler dahil diğer bildirimlerin niteliği, tavsiyelerin çıkartılması veya dahil edilmesi meselesi; sorumluluğun reddi beyanları, kısıtlamalar ve verilecek güvence veya teyidin türü,
- Telif hakkı meseleleri ve bilgilerin daha öte dağıtımı veya paylaşımı üzerindeki kısıtlamalar.

5. Kurum dışına raporlanacak iç denetim raporlarını veya bildirimlerini hazırlamak amacıyla yapılan görevler, ilgili *Uluslararası İç Denetim Standartları*na uygun yürütülmeli ve raporda veya bildirimde bu standartlara atıfta bulunulmalıdır.

6. Kurum dışına çıkartılacak bilgileri hazırlamak amacına yönelik görevler sırasında, iç denetçi, yönetime veya denetim komitesine bildirilmesi gereken bir bilgi tespit ederse, ilgili kişilere bu bildirimleri ugun bir şekilde yapmalıdır.

# Uygulama Önerisi 2440-3: Hassas Bilgilerin Hiyerarşi İçinde ve Dışında Raporlanması

Uluslararası İç Denetim Standartlarından Standart 2440 ve Standart 2600'ün ve Etik Kurallarının Dürüstlük ve Gizlilikle İlgili Davranış Kurallarının Yorumu

## İlgili Standart

**2440 Sonuçların Raporlanması**
İç Denetim Yöneticisi, görev sonuçlarını uygun taraflara raporlamalıdır.

## İlgili Standart

**2600 Yönetimin Artık Riskleri Üstlenmesinin Çözümü**
İç Denetim Yöneticisi, üst yönetimin kurum için kabul *edilemeyebilecek* bir artık (bakiye) risk düzeyini üstlenmeyi kabul ettiğine inandığı takdirde, konuyu üst yönetimle tartışmalıdır. Artık riskle ilgili bir karara varılamazsa, İç Denetim Yöneticisi ve üst yönetim, konuyu çözümlenmesi için denetim komitesi ve yönetim kuruluna rapor etmelidir.

**Etik Kurallarının Dürüstlükle İlgili Davranış Kuralları:**
İç denetçiler,

1.1. İşlerini dürüstlük, özen ve sorumluluk duygusuyla yapar,

1.2. Hukuku gözetir ve kanunların ve mesleğin emrettiği açıklamaları yapar,

1.3. Herhangi bir yasa dışı faaliyete bilerek girmez ya da iç denetim mesleği veya kurum için onur kırıcı herhangi bir fiilde bulunmaz,

1.4. Kurumun meşru ve etik hedeflerine saygı gösterir ve katkıda bulunur.

**Etik Kurallarının Gizlilikle İlgili Davranış Kuralları:**
İç denetçiler:

3.1. Görevleri sırasında edindikleri bilgileri, dikkatli ve ihtiyatlı bir şekilde kullanır ve korur,

3.2. Bu bilgileri kişisel menfaatleri için ya da ilgili kanunlara aykırı bir şekilde veya kurumun meşru ve etik hedeflerine zarar verecek bir şekilde kullanmaz.

---

**Bu Uygulama Önerisinin Niteliği:** *Bir iç denetçi, riskler, tehditler, belirsizlikler, suiistimaller, israf ve kötü yönetim, yasa dışı faaliyetler, yetkinin kötüye kullanılması, halk sağlığı veya emniyetini tehlikeye sokan suçlar veya başka haksız fiiller hakkında bilgi sahibi olabilir. Bazı durumlarda, bu yeni bilgilerin önemli sonuçları olur ve destekleyici deliller önemli ve güvenilirdir. İç denetçinin bu tür durumlarda karşı karşıya olduğu ikilem oldukça karmaşıktır ve genellikle kültürel ve iş uygulamaları farklılıkları, hukukî yapılar, mahallî ve ulusal kanunlar ve meslekî standartlar, etik kuralları ve kişisel değerler gibi etkenleri kapsar. İç denetçinin bu tür durumlarda benimsediği davranış tarzı misillemelere ve potansiyel sorumluluklara yol açabilir. Bu riskler ve sonuçlardan dolayı, dikkatle, iç denetçi, mevcut delilleri ve vardığı sonuçların makul olup olmadığını değerlendirmeli ve bu hassas bilgilerin sorunu çözümleme yetkisi bulunan kişilere bildirilmesi için yapabileceklerini incelemeli ve bu usulsüzlüğü durdurmak için gerekenleri yapmalıdır. Bazı ülkelerde, mahallî kanunlar veya mevzuat belirli eylemlerin yapılmasını gerektirebilir.*

*Bu Uygulama Önerisi, iç denetçinin bu tür durumlarda karşılaşabileceği pek çok sorun ve konu hakkında düşünmesini sağlamak amacına yöneliktir. Bir iç denetçinin göz önüne alabileceği etkenleri açıklamasına ve bilgi vermesine rağmen, bu Uygulama Önerisi, konunun tam kapsamlı bir incelemesini içermemekte ve denetçi için bir uzman tavsiyesi veya hukukî tavsiye sunmamaktadır. İç denetçiler, konunun hassas olduğu ve önemli sonuçlarının olabileceği durumlarda hukuk danışmanına başvurmalıdır. Bu Uygulama Önerisi, azamî dikkatle ve uzun görüşme ve istişarelerden sonra hazırlanmıştır. Bununla birlikte, IIA, bu Uygulama Önerisi metninde verilen bilgilerin kullanılmasının ya da bunların fiiliyatta belirli durumlara uygulanmasının sonuçlarından sorumluluk kabul etmez ve önerilen eylemlerin başarılı olacağına dair bir güvence vermez.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. İç denetçilerin eline, sık sık, kurum için hayatî önemi ve hassasiyeti olan ve önemli potansiyel sonuçlar doğurabilecek bilgiler geçer. Bu bilgiler; riskler, tehditler, belirsizlikler, suiistimaller, israf ve kötü yönetim, yasa dışı faaliyetler, yetkinin kötüye kullanılması, halk sağlığı veya emniyetini tehlikeye sokan suçlar veya başka haksız fiillerle ilgili olabilir. Bu tür konular, kurumun itibarı, imajı, rekabet gücü, başarısı, yaşamını sürdürme kabiliyeti, pazar değeri, yatırımları ve maddî olmayan varlıkları veya kârı üzerinde olumsuz etkiler yapabilir. Bunların, bir kurumun riske maruziyetini artırma ihtimali de vardır.

**Hassas Bilgilerin Hiyerarşi İçindeki Kişilere Verilmesi:**

2. İç denetçi, yeni edindiği bilgilerin önemli ve güvenilir olduğuna karar verdikten sonra, normal olarak bu bilgileri, bunlara dayanarak karar alabilecek olan *yöneticilere* zamanında bildirir. Çoğu durumda, üst yönetim bunlarla bağlantılı risklerin yönetimi için gerekli tedbiri aldığı sürece, bu raporlamalar, sorunu iç denetim açısından çözümler. Raporlamalar kurum yönetiminin tedbir almamasının veya yeterli tedbirleri almamasının kurumu kabul edilemez düzeyde bir riskle karşı karşıya bıraktığı tespitiyle sonuçlandığı takdirde, İç Denetim Yöneticisi, tatmin edici bir çözüm bulmak amacıyla mevcut başka seçenekleri değerlendirmelidir.

3. Bu muhtemel eylem ve tedbirlerin bir parçası olarak, İç Denetim Yöneticisi, risk ve tehlikelere ilişkin endişelerini, kendi normal hiyerarşisi içinde *üst yönetimle* tartışabilir. Yönetim kurulunun denetim komitesi ve diğer komitelerin de İç Denetim Yöneticisinin içinde bulunduğu hiyerarşiye tâbi olması beklenebileceği için, bu komite üyeleri de, normal olarak, İç Denetim Yöneticisinin kaygılarından haberdar olur. Üst yönetimle yaptığı bu görüşmelere rağmen İç Denetim Yöneticisi, sonuçtan tatmin olmaz ve üst yönetimin kurumu kabul edilemez bir riske soktuğuna, sorunu ortadan kaldırmak veya çözmek için gerekli tedbirleri almadığına inanırsa, üst yönetim ve İç Denetim Yöneticisi, sorunla ilgili

önemli bilgileri ve görüş farklılıklarını *yönetim kurulu üyelerine* veya *yönetim kurulunun bir komitesine* iletir.

4. Bu basit hiyerarşi içindeki iletişim senaryosu, ulusal mevzuat, düzenlemeler veya yaygın kabul gören uygulamalar uyarınca belirli hassas olay ve durumlar için hızlandırılabilir. Örneğin, Amerika Birleşik Devletleri'nde hisseleri halka açık olan ve borsada işlem gören bir şirketin mali raporlamasında usulsüzlük yaptığına dair delil bulunması hâlinde, ilgili mevzuata göre, üst yönetim ve İç Denetim Yöneticisi bu durumda alınması gereken tedbirler konusunda tam bir mutabakat içinde olsalar bile, bu yanıltıcı mali raporlarla ilgili bilgilerin yönetim kurulunun denetim komitesine derhal bildirilmesi şarttır. Çeşitli ülkelerde geçerli olan kanun ve düzenlemelere göre, ceza kanunları, menkul kıymetlerle ilgili kanunlar, gıda maddeleri, ilâç veya kirlenmeye ilişkin kanunların ihlâlleri ve devlet memurlarına veya tedarikçilerin veya müşterilerin temsilcilerine rüşvet verilmesi veya başka usulsüz ödemeler yapılması gibi benzeri başka yasa dışı eylemlerin yönetim kurulu üyelerine veya yönetim kurulunun denetim komitesine bildirilmesi gerekir.

**Bilgilerin Hiyerarşi Dışındaki Kişilere Verilmesi:**

5. Bazı durumlarda, bir iç denetçi, öğrendiği bilgileri normal hiyerarşi dışındaki, hattâ kurumun dışındaki kişilere bildirip bildirmeme konusunda bir ikilemle karşı karşıya kalabilir. Olumsuz bilgilerin kurum içinde fakat normal hiyerarşi dışındaki kişilere ya da tamamen kurumun dışında olan resmî makam ve mercilere veya başka yetkililere açıklanması eylemi, genellikle "dışarı bilgi sızdırma" tâbir edilir.

6. Dışarı bilgi sızdırma hakkında yapılan araştırmalarda, bu harekette bulunanların çoğunun, özellikle kurumun yasa dışı faaliyetlere veya usulsüzlüklere ilişkin iddiaları soruşturmak ve tedbir almak için uyguladığı politikalara ve oluşturduğu mekanizmalara güvendikleri durumlarda, hassas bilgileri, normal hiyerarşinin dışında bile olsa, içeriden kişilere sızdırdıkları bildirilmiştir. Ancak,

elinde hassas bilgiler bulunan kişilerin bazıları, özellikle kendi iş arkadaşlarının veya işverenlerinin misilleme yapmasından korktukları, konunun yeterince araştırılıp soruşturulacağı konusunda şüphelerinin bulunduğu, konunun hasır altı edileceğine inandıkları veya kurumdaki ya da toplumdaki insanların sağlığını, emniyetini veya huzurunu bozucu yasa dışı faaliyetler veya usulsüzlükler hakkında deliller elde ettikleri durumlarda, bu bilgileri kurum dışına sızdırmayı tercih edebilirler. İyi niyetli olarak dışarı bilgi sızdıran bu kişilerin çoğunun temel dürtüsü, yasa dışı, zararlı veya usulsüz faaliyeti durdurmaktır.

7. Benzer bir ikilemle karşı karşıya olan ve imkân dahilindeki tüm seçenekleri değerlendirmesi gereken bir iç denetçinin bu riski kendi hiyerarşisi dışındaki kişi veya gruplara da bildirmek için *alternatif yolları* düşünmesi gerekecektir. Bu yaklaşımların taşıdığı risklerden ve muhtemel sonuçlarından dolayı, iç denetçi, elindeki delillerin ve vardığı sonuçların makul ve doğru olup olmadığını dikkatle değerlendirmeli ve her potansiyel hareketinin avantaj ve dezavantajlarını dikkatle hesaplamalıdır. Bir iç denetçinin bu tür bir harekette bulunması, eğer üst düzey yöneticilerin veya yönetim kurulunun üyeleri ya da yönetim kurulunun komitelerinin üyeleri gibi idarî mevkilerdeki kişilerin sorumluluklarını yerine getirmelerini sağlayacaksa uygun olabilir. Bir iç denetçi, bu tür bilgileri kurumun yönetim yapısı dışındaki kişilere bildirmeyi son çare olarak görmelidir. Bir iç denetçi, bu hareketi, *sadece* mevcut riskin ve muhtemel sonuçlarının ciddî olduğuna ve kurumun mevcut yönetiminin ve yönetim mekanizmalarının bu riskle etkin bir şekilde mücadele edemeyeceğine veya etmeyeceğine inandığı *ender* durumlarda tercih etmelidir.

8. OECD *(Ekonomik İşbirliği ve Kalkınma Teşkilâtı)* üyesi olan ülkelerin çoğunda, yasa dışı veya etik dışı fiil ve eylemlerden haberdar olan kamu görevlilerinin durumu bir genel müfettişe, başka bir kamu görevlisine veya ombudsmana bildirmekle yükümlü

olduğunu öngören kanunlar veya idarî yönetmelikler mevcuttur. Dışarı bilgi sızdırma tipinde eylemlere ilişkin bazı ulusal kanunlar, belirli yasa dışı faaliyet ve eylemleri ihbar eden kişileri koruyucu hükümler içermektedir. Bu ülkelerin kanun ve yönetmeliklerinde sayılan faaliyet tipleri şunlardır:

- Suç teşkil eden eylemler ve kanunî yükümlülüklere uymamalar,
- Adlî hatâ olarak görülen eylemler,
- Bireylerin sağlığı, emniyeti veya refahını tehlikeye sokan eylemler,
- Çevreye zarar veren eylemler,
- Yukarıda sayılan eylemleri gizleyen veya saklayan faaliyetler.

Diğer bazı ülkelerde ise bu konuda herhangi bir koruyucu hüküm veya düzenleme yoktur. İç denetçi, kurumun faaliyet gösterdiği çeşitli ülkelerin ilgili kanunları ve mevzuatını bilmeli ve bu mevzuata uygun kararlar almalıdır. İç denetçi, yürülükteki kanunlardan emin değilse, hukukî tavsiye almayı düşünmelidir.

9. Pek çok meslekî örgüt, üyelerini, yasa dışı veya etik dışı faaliyetleri bildirmekten sorumlu tutar. Bir "mesleğin" ayırt edici işareti, onun kamuya ve halka karşı geniş sorumluluklarını kabul etmesi ve kamunun çıkarlarını korumasıdır. Mevzuatı incelemeye ve öğrenmeye ek olarak, IIA üyeleri ve bütün Uluslararası İç Denetçiler (CIA'lar), IIA'nın *Etik Kurallarında* yasa dışı veya etik dışı eylem ve fiiller hakkında öngördüğü koşul ve kurallara uymalıdır.

**İç Denetçinin Kararı:**
Bir iç denetçinin mevcut bütün delilleri ve vardığı sonuçların makul ve doğru olup olmadığını dikkatle değerlendirmesi ve kurumun, kurumla menfaat ilişkisi içinde olanların, dış toplumun veya toplumsal kuruluşların çıkarlarını korumak için hangi tedbirleri almak gerektiğine karar vermesi, onun hem meslekî görevi hem de etik sorumluluğudur.

Ayrıca, denetçinin, bu konuda hukukî veya meslekî bir sorumluluk ve zorunluluk altında olmadıkça, bilgilerin değerine ve sahiplerine saygı göstermek ve bilgileri uygun izin ve yetkiyi almadan başka kişilere açıklamamak konusunda IIA'nın *Etik Kurallarında* öngörülen gizlilik görevini de dikkate alması gerekir. Bu değerlendirme sürecinde, denetçi hukuk danışmanından ve gerektiğinde başka uzmanlardan görüş ve tavsiye almalıdır. Bu tartışmalar, mevcut koşullar hakkında farklı bir bakış açısı edinmesinde ve çeşitli muhtemel eylemlerin potansiyel etki ve sonuçları hakkında farklı görüşlerin alınmasında faydalı olabilir. İç denetçinin bu tür karmaşık ve hassas durumları çözmek için uyguladığı yöntem, misillemelere ve potansiyel sorumluluklara yol açabilir.

Son olarak, iç denetçi kişisel bir karar almalıdır. Bilgilerin normal hiyerarşi dışındaki kişilere bildirilmesi kararı, ilgili yasa dışı hareket veya suç hakkında önemli ve güvenilir delillerin bulunduğu ve hukukî veya düzenleyici âmir hükümlerin veya meslekî veya etik yükümlülüklerin tedbir almayı gerektirdiği konusunda sağlam bilgilere dayanmalıdır. Denetçinin bu konudaki eylem dürtüsü, her türlü yasa dışı, usulsüz veya zararlı faaliyeti durdurma isteği olmalıdır.

# Uygulama Önerisi 2500-1: İlerlemenin Gözlenmesi

Uluslararası İç Denetim Standartlarından
Standart 2500'in Yorumu

## İlgili Standart

**2500 İlerlemenin Gözlenmesi**
İç Denetim Yöneticisi, yönetime rapor edilen sonuçların akıbetinin gözlenmesi için bir sistem kurmalı ve uygulamalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, yönetime rapor edilen sonuçları izlerken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. İç Denetim Yöneticisi, aşağıdakileri içerecek şekilde prosedürler oluşturmalıdır:
   - Yönetimin rapordaki sonuçlara, tespitlere ve tavsiyelere cevap vermesi için tanınan süre,
   - Yönetimin verdiği cevabın değerlendirilmesi,
   - Cevabın doğrulanması (gerekiyorsa),
   - Bir takip görevlendirmesi (gerekiyorsa)
   - Risklerin üstlenilmesi de dahil, tatmin edici olmayan cevapların/eylemlerin uygun seviyedeki yöneticilere iletilmesine yönelik bir raporlama prosedürü.

2. Rapordaki bazı tespitler ve tavsiyeler, yönetimin derhal tedbir almasını gerektirecek kadar önemli olabilir. Ortadan kalkana kadar, bu durum, kurum üzerindeki muhtemel etkileri dikkate alınarak, iç denetim faaliyeti tarafından gözlenmelidir.

3. İlerlemenin etkili bir şekilde gözlenmesi için kullanılan teknikler şunlardır:

   - Tespit ve tavsiyelerin, düzeltici tedbirleri almaktan sorumlu olan yönetim kademelerine iletilmesi.
   - Yönetimin tespit ve tavsiyelerle ilgili cevaplarının, görev süresinde veya görev sonuçlarının rapor edilmesinden sonra, makul bir süre içinde, alınması ve değerlendirilmesi. Yönetimin cevapları, İç Denetim Yöneticisinin düzeltici tedbirlerin zamanlamasını ve uygunluğunu değerlendirmesi için *yeterli bilgi* içeriyorsa, daha faydalı olur.
   - Yönetimin, raporlanan durumları düzeltmeye yönelik çabalarını değerlendirmek için yönetimden düzenli olarak güncel bilgi alınması.
   - İzleme veya düzeltme prosedürlerinden sorumlu diğer birimlerden bilgi alınması ve bu bilgilerin değerlendirilmesi.
   - Tespit ve tavsiyelerine alınan cevapların durumu hakkında üst yönetime veya denetim veya yönetim kuruluna rapor verilmesi.

# Uygulama Önerisi 2500.A1-1: Takip Süreci

Uluslararası İç Denetim Standartlarından
Standart 2500'ün Yorumu

## İlgili Standart

**2500.A1** İç Denetim Yöneticisi, yönetimin aldığı tedbirlerin etkili bir şekilde uygulanmasını veya üst yönetimin, gerekli tedbiri almamasının riskini üstlenmeyi kabul etmesini sağlamak ve gelişmeleri gözlemek amacına yönelik bir takip süreci kurmalıdır.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, takip süreci kurar ve uygularken aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

1. İç denetçiler, düzeltici tedbirlerin uygulanmasını ve istenen sonuçları vermesini sağlamalı ya da üst yönetim, denetim komitesi veya yönetim kurulunun, rapor edilen tespitlerin gerekli kıldığı tedbirleri almamasının riskini üstlenmesini sağlamalıdır.

2. *Takip*, dış denetçilerin ve diğerlerininkiler de dahil, rapor edilen tespit ve tavsiyeler üzerine yönetimin aldığı tedbirlerin yeterliliği, etkinliği ve zamanlamasının iç denetçiler tarafından belirlenip değerlendirildiği bir süreç olarak tanımlanır.

3. Takip sorumluluğu iç denetim faaliyetinin yazılı yönetmeliğinde tanımlanmalıdır. Takibin niteliği, zamanlaması ve kapsamı İç Denetim Yöneticisi tarafından tespit edilmelidir. Uygun takip prosedürlerinin tespitinde dikkate alınması gereken hususlar şunlardır:

- Rapor edilen tespit veya tavsiyenin önemi,
- Rapor edilen sorunun düzeltilmesi için gereken çaba ve maliyet miktarı,
- Düzeltici tedbirin yetersiz kalmasının muhtemel etkileri,
- Düzeltici tedbirin karmaşıklıklığı,
- Gereken süre.

4. İç Denetim Yöneticisinin, yönetimin yazılı veya sözlü cevabının -kendi gözlem veya tavsiyesinin nisbî önemiyle karşılaştırıldığında- alınan tedbirin yeterli olduğunu gösterdiği hükmüne vardığı durumlar da olabilir. Bu durumlarda, takip görevi, bir sonraki denetim görevinin bir parçası olarak da yapılabilir.

5. İç denetçiler, görev gözlemleri ve tavsiyeleri üzerine alınan tedbirlerin, ilgili sorunları çözüp çözmediğini araştırmalıdır.

6. Görev iş programlarının bir parçası olarak, takip görev ve faaliyetlerini programlamaktan da İç Denetim Yöneticisi sorumludur. Takip programı, düzeltici tedbirlerin uygulanma zorluğu ve zamanlaması yanında risk ve riske maruz kalma seviyesi dikkate alınarak yapılmalıdır.

# Uygulama Önerisi 2600-1: Yönetimin Artık (Bakiye) Riskleri Üstlenmesi

Uluslararası İç Denetim Standartlarından
Standart 2600'ün Yorumu

## İlgili Standart

**2600 Yönetimin Artık (Bakiye) Riskleri Üstlenmesinin Çözümü**
İç Denetim Yöneticisi, üst yönetimin kurum için kabul edilemeyebilecek bir artık (bakiye) risk düzeyini üstlenmeyi kabul ettiğine inandığı takdirde, konuyu üst yönetimle tartışmalıdır. Artık riskle ilgili bir karara varılamazsa, İç Denetim Yöneticisi ve üst yönetim, konuyu çözümlenmesi için denetim komitesi ve yönetim kuruluna rapor etmelidir.

**Bu Uygulama Önerisinin Niteliği:** *İç denetçiler, yönetimin riskleri üstlenmeyi kabul etmesi konusunda aşağıdaki önerileri dikkate almalıdır. Bu kılavuzun bu konuda dikkate alınması gereken bütün hususları kapsamak gibi bir amacı yoktur; kılavuz, sadece, dikkate alınması gereken bir tavsiyeler demetinden ibarettir.* ***Uygulama Önerilerine uymak isteğe bağlıdır.***

Rapor edilen tesbit ve tavsiyelere cevap olarak alınması gereken uygun tedbirlere karar vermekten yönetim sorumludur. Tespit ve tavsiyeler şeklinde rapor edilen sorunların zamanında çözümlenmesi için yönetimin aldığı tedbirlerin değerlendirilmesi, İç Denetim Yöneticisinin sorumluluğundadır. Takipin kapsamına karar verirken, iç denetçiler, kurum içinde başka kişilerin yapması gereken takip görevlerinin niteliğini ve prosedürlerini de dikkate almalıdır.

Standart 2060 ile ilgili 2060-1 sayılı Uygulama Önerisinin 3. maddesinde belirtildiği gibi, üst yönetim, maliyet veya başka düşüncelerle, rapor edilen bir sorunu *düzeltmeme riskini* üstlenmeye

karar verebilir. Bütün önemli tespit ve tavsiyeler hakkında üst yönetimin aldığı kararlar hakkında, denetim komitesi ve yönetim kurulu bilgilendirilmelidir.

1. Bu ilke, birçok kural koyucu kuruluş tarafından dile getirilmiştir. Bunlara, IAASB/IFAC'nin hazırladığı Meslekî Etik Yönetmeliği'nde ve ABD Yönetim Güvenirlik Bürosu'nun Genel Kabul Görmüş Yönetim Denetleme Standartları da dahildir.

2. Bu risk, Mali Raporlandırma Konseyi'nce atanan ve ICAEW (İngiltere ve Galler İmtiyazlı Muhasebeciler Enstitüsü) tarafından yayınlanan Denetim Komiteleri ve Birleşik Yönetmelik Kılavuzu ile ilgili Aralık 2003 Smith Raporu'nda ortaya çıkmıştır.

3. Özel sınırlandırmalara verilebilecek örnekler arasında, İngiliz Kamu İç Denetim Standartları 2.4.2 de vardır. Şuna değinmektedir: Objektifliğin, bireysel denetçiler, daha önceden yönetim sorumluluğu taşıdıkları veya danışmanlık görevi yaptıkları bir faaliyeti gözden geçirdiklerinde bozulduğuna inanılmaktadır. Bu standart, 'Danışmanlığa Dair Örnek Uygulama Kılavuzu'nda ek olarak verilmekte ve şu belirtilmektedir: Bu rolde, iç denetçinin yönetime önerilerde bulunması ve yönetim adına bir görev üstlenmemesi önemlidir. İç denetçi tarafından yapılan önerinin yönetim tarafından kabul edilmesi, kendi sorumluluk alanlarında yönetimin güvenirliğini azaltmayacaktır. (3.5.3)

4. Bağımsızlık, denetçinin ilgili uygulama sisteminin geliştirilmesi, edinilmesi, uygulanması veya sürdürülmesi gibi işlerde görev almamış olmasıdır.

5. Bağımsızlık: Denetçinin dışarıya yaptırılan BS faaliyetlerinin planlanması, seçilmesi veya sözleşmesinin yapılması işlerinde görev almamış olması.


Türkiye İç Denetim Enstitüsü

The IIA Research Foundation

Deloitte.

Uluslararası İç Denetim Standartları -
Mesleki Uygulama Çerçevesi kitabı
Deloitte sponsorluğunda yayımlanmıştır.

***Türkiye İç Denetim Enstitüsü Yayınları No: 4***