KAMU İÇ DENETİMİNDE RİSK DEĞERLENDİRME REHBERİ

I. GİRİŞ

Bu rehber, iç denetim birimlerince hazırlanacak risk değerlendirme çalışmalarının temel esaslarını belirlemek üzere, İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmeliğin 36 ncı maddesi uyarınca İç Denetim Koordinasyon Kurulunca hazırlanmıştır.

İç denetim birimleri, risk değerlendirme çalışmalarına ilişkin hususları bu rehbere uygun olarak kendi iç denetim birim yönergelerinde düzenlerler.

Risk, idarelerin kuruluş amaçları ile stratejik hedeflerine ulaşmasına ve görevlerin ifasına engel olabilecek veya beklenmeyen zararlara yol açabilecek durum ya da olaylardır.

İdareler, faaliyetlerini yürütürken bir çok risk ve belirsizlikle karşı karşıya kalabilir. İdareler, maruz kaldıkları bu riskleri risk yönetimi kapsamında; üstlenerek, kaçınarak, transfer ederek veya kontrol ederek yönetebilir. Risk ve belirsizliklerin olumsuz etkilerinin azaltılmasında, oluşturulacak iç kontrol süreçleri en etkili çözümdür.

Risk esaslı denetim; idarelerin faaliyet alanlarına ilişkin risk faktörlerinin tanımlanmasını, risk seviyelerinin ölçülmesini, bu riskler için uygulanan kontrollerin etkinlik ve yeterliliğinin değerlendirilmesini ve yüksek risk içeren alanlara denetim önceliğinin verilmesini öngören bir denetim yaklaşımıdır. Risk esaslı denetimde amaç; denetim kaynaklarının etkin kullanımının sağlanması ve riskli alanlara yoğunlaşarak yönetim, kontrol ve risk yönetimi süreçlerinin etkinlik düzeylerinin arttırılmasında yönetime yapılan katkının en üst seviyeye çıkartılmasıdır.

Risklerin tanımlanması ve kontrolü için gerekli stratejilerin geliştirilmesinden ve uygulanmasından yönetim sorumludur.

Yönetim tarafından tanımlanan riskler çerçevesinde idarelerin tüm faaliyetleri iç denetim birimlerince kapsamlı bir risk analizine tabi tutulur. Risklerin tanımlanması ve kontrolü için yönetimce bir risk yönetimi sürecinin oluşturulmaması veya oluşturulan sürecin etkin olmadığının daha önceki denetimlerde tespit edilmesi halinde risk tanımlaması çalışmaları iç denetim birimlerince yapılabilir.

Belirlenen riskler üzerinde yapılan analiz sonuçları değerlendirilerek, kamu idarelerinin hizmetlerini etkileyebilecek riskler, risklilik oranı ve önemine göre ağırlık verilerek derecelendirilir. Bu değerlendirme sonuçlarına göre en yüksek risk içeren alan ve konulardan başlanarak iç denetim planı ve programları hazırlanır.

II. RİSK DEĞERLENDİRMESİ

İç denetim birimince yapılacak risk değerlendirmesi dört aşamadan oluşur:

- Denetim evreninin tanımlanması
- Denetim alanlarının belirlenmesi
- Yapısal risk düzeylerinin belirlenmesi
- Denetim alanlarının önceliklendirilmesi

Risk değerlendirmesi çalışmalarında tartışma ortamları oluşturulmak suretiyle geniş katılım sağlanmalı, denetim alanları ayrı ayrı ele alınmalı ve risklerin ölçülmesinde kullanılan kriterlere bağlı kalınmalıdır. Risk değerlendirmesi sonuçları sürekli olarak gözden geçirilmeli, zaman içerisinde ortaya çıkacak yeni riskler ve belirsizlikler karşısında güncellenmelidir.

1. Denetim evreninin tanımlanması ve denetim alanlarının belirlenmesi

Denetim evreninin tanımlanması ve denetim alanlarının belirlenmesi çalışmaları Kurulca çıkarılan iç denetim planı ve programı hazırlama rehberi uyarınca yapılır.

2. Yapısal risk düzeylerinin belirlenmesi

Riski bir olay veya faaliyetin kurumu olumsuz olarak etkileme olasılığı olarak tanımladığımızda, yapısal risk; mevcut kontroller ve tedbirler dışarda tutulduğunda kamu idarelerinin mevcut yapısından veya faaliyetin doğasından kaynaklanan risktir. İdarelerin yapısal risk düzeylerinin belirlenmesi çalışmaları, yapısal risk kriterlerinin (unsurlarının) tanımlanması ve ölçülmesi aşamalarından oluşur.

2.1 Yapısal risk kriterlerinin tanımlanması

Denetim alanları, belli risk kriterleri çerçevesinde değerlendirilir. Risk kriterleri tanımlanırken kullanılacak model mümkün olduğunca basit seçilmeli ve kullanılan risk kriterlerinin tanımlarını içermelidir. Üst yönetici ile iç denetim biriminin riskli alanların belirlenmesinde kullanılan kriterleri anlaması ve bu kriterler üzerinde görüş birliği içinde olması önemlidir.

Yapısal risk düzeyinin belirlenmesinde kullanılabilecek örnek risk kriterleri modeli aşağıda yer almaktadır. İdareler, kendi faaliyet alanlarına uygun risk kriterleri modelini oluşturmalıdır. Ancak, oluşturulacak modelde yapısal risk kriterlerinin sayısının fazla olmamasına özen gösterilmelidir.

Örnek risk kriterleri;

- Bütçe büyüklüğü

Kamu idaresine bütçeyle verilen kaynakların büyüklüğü kayıp ve zararların gerçekleşme olasılığını arttırır.

- İşlem hacmi ve personel sayısı

İşlem hacminin büyüklüğü karşısında personel sayısının yetersizliği hata yapılma olasılığını artırarak idareyi riskli bir konuma getirebilir.

- Faaliyetlerin karmaşıklığı

İdarenin faaliyetlerinin karmaşıklığı, kontrollerin uygulanmasını zorlaştırarak hata yapılma ihtimalini artırabilir.

- Mevzuatın yoğunluğu

Kamu idaresinin faaliyet alanını ilgilendiren çok sayıda yasal düzenlemenin olması mevzuatın doğru bir şekilde anlaşılmasını güçleştirebileceğinden faaliyetlerin düzenlemelere uygun yapılamama riskini arttırabilir.

- Yapısal, işlevsel ve teknik değişiklikler

Yeni birim ve faaliyetler, yeniden yapılandırma projeleri, organizasyon ve insan kaynaklarındaki önemli değişiklikler yüksek risk içerdiğinden öncelikli olarak denetim kapsamına alınması gereken alanlardır.

- Bilgi teknolojileri sisteminin yapısı

Kullanılan bilgi teknolojilerinin çeşitliliği ve veri tabanının genişliği, varlıkların kontrolünü güçleştirebilecek ve önemli bilgilerin kaybına neden olabileceğinden riskliliği artırabilecek bir unsurdur.

2.2 Yapısal risk düzeyinin ölçülmesi

Denetim alanlarına yönelik yapısal risk kriterleri tanımlandıktan sonra, denetim alanlarının bu risk kriterleri karşısındaki durumu değerlendirilmek suretiyle yapısal risk düzeyleri belirlenir. Bu değerlendirme aşağıdaki iki yönteme göre yapılabilir.

a. Kümülatif yöntem

Her risk kriterine idare faaliyetlerine etkisi ve önemi göz önünde bulundurularak bir ağırlık verilir. Aynı şekilde, her risk kriterine risk seviyesini gösteren 1'den 5'e kadar bir değer verilir. En düşük risk seviyesi için 1 ve en yüksek risk

seviyesi için ise 5 değeri kullanılır. Daha sonra, verilen bu değer ağırlığıyla çarpılarak her bir kriter için risk puanı bulunur. Son olarak her kriter için elde edilen risk puanları toplanarak denetim alanının yapısal risk düzeyi belirlenir. Kümülatif yöntemin uygulanmasıyla ilgili örnek Ek:1'de yer almaktadır.

b. Göreceli yöntem

Her risk kriterine bu kriterle ilgili ortaya çıkması muhtemel riskin idare faaliyetlerine etkisi ve önemi göz önünde bulundurularak 1'den 5' e kadar bir etki değeri verilir. En düşük etki seviyesi için 1 ve en yüksek etki seviyesi için 5 değeri kullanılır. Aynı şekilde, her risk kriteriyle ilgili riskin gerçekleşme olasılığı göz önünde bulundurularak 1'den 5' e kadar bir olasılık değeri verilir. En düşük olasılık seviyesi için 1 ve en yüksek olasılık seviyesi için ise 5 değeri kullanılır. Daha sonra, verilen bu olasılık değeri etki değeriyle çarpılarak her bir kriter için risk puanı bulunur. Son olarak her kriter için elde edilen risk puanları toplanarak denetim alanının yapısal risk düzeyi belirlenir. Göreceli yöntemin uygulanmasıyla ilgili örnek Ek:2'de yer almaktadır.

3. Denetim alanlarının önceliklendirilmesi

Risk değerlendirmesinde son aşama, her bir denetim alanına ait risklerin mukayese edilerek denetim alanlarının sıralanmasıdır.

Her denetlenebilir alan, yukarıda açıklanan risk kriterleri esas alınarak derecelendirilir. Derecelendirmede elde edilen sonuçlara göre, denetim alanları mümkün olduğunca basit bir ölçeğe göre ifade edilir.

Örnek derecelendirme ölçeği aşağıda yer almaktadır:

1: Yüksek riskli alan

2: Orta riskli alan

3: Düşük riskli alan

EK- 1/A

(X) İDARESİ "KÜMÜLATİF RİSK DEĞERLENDİRMESİ" ÖRNEĞİ

1) Denetim evreninin tanımlanması ve denetim alanlarının belirlenmesi

(X) idaresiyle ilgili olarak; denetim evreni idarenin tüm faaliyetleri olarak tanımlanmış, denetim alanları olarak da A-J alanları belirlenmiştir.

2) Yapısal risk düzeylerinin belirlenmesi

2.1) Yapısal risk kriterlerinin tanımlanması

İdarenin faaliyetlerine etki eden dört risk kriteri tanımlanmıştır. Bunlar; bütçe büyüklüğü, işlem hacmi ve personel sayısı, faaliyetlerin karmaşıklığı ile yapısal, işlevsel ve teknik değişikliklerdir.

2.2) Yapısal risk düzeyinin ölçülmesi

Denetim alanlarının risk kriterleri karşısındaki durumu değerlendirilmek suretiyle yapısal risk düzeyleri aşağıdaki şekilde belirlenmiştir.

(X) İDARESİ RİSK KRİTERLERİNİN VE DEĞERLENDİRME ÖLÇEĞİNİN TANIMLANMASI

RİSK KRİTERLERİ	KATSAYILAR		AĞIRLIK (%)
Bütçe Büyüklükleri (Milyon YTL)	100'den fazla	5	40
	60-100	4	
	20-60	3	
	5-20	2	
	5'den az	1	
İşlem Hacmi Ve Personel Sayısı	İşlem Hacmi Yüksek-Personel Sayısı Çok Yetersiz	5	30
		4	
		3	
		2	
	İşlem Hacmi ve Personel Sayısı Dengeli	1	
Faaliyetlerin Karmaşıklığı	Çok Karışık Faaliyetler	5	15
		4	
		3	
		2	
	Karışık Olmayan Faaliyetler	1	
Yapısal, İşlevsel Ve Teknik Değişiklikler	Çok Sık Değişiklik Var	5	15
		4	
		3	
		2	
	Nadiren Değişiklik Var	1	

EK:1/B

(X) İDARESİ DENETİM ALANLARININ YAPISAL RİSK DÜZEYLERİNİN ÖLÇÜLMESİ

Denetim Alanları	Bütçe Büyüklüğü (1)			İşlem Hacmi Ve Personel Sayısı (2)			Faaliyetlerin Karmaşıklığı (3)			Yapısal, İşlevsel Ve Teknik Değişiklikler (4)			Denetim Önceliği Risk Puanı
	Kriter Puanı	Ağırlık	Risk Puanı	Kriter Puanı	Ağırlık	Risk Puanı	Kriter Puanı	Ağırlık	Risk Puanı	Kriter Puanı	Ağırlık	Risk Puanı	
A	5	0.40	2.00	4	0.30	1.20	5	0.15	0.75	2	0.15	0.30	4.25
B	4	0.40	1.60	5	0.30	1.50	4	0.15	0.60	3	0.15	0.45	4.15
C	4	0.40	1.60	3	0.30	0.90	3	0.15	0.45	2	0.15	0.30	3.25
D	3	0.40	1.20	4	0.30	1.20	4	0.15	0.45	1	0.15	0.15	3.00
E	2	0.40	0.80	1	0.30	0.30	2	0.15	0.30	5	0.15	0.75	2.15
F	2	0.40	0.80	2	0.30	0.60	3	0.15	0.45	1	0.15	0.15	2.00
G	3	0.40	1.20	2	0.30	0.60	2	0.15	0.30	4	0.15	0.60	2.70
H	1	0.40	0.40	3	0.30	0.90	1	0.15	0.15	2	0.15	0.30	1.75
İ	3	0.40	1.20	2	0.30	0.60	4	0.15	0.60	4	0.15	0.60	3.00
J	2	0.40	0.80	1	0.30	0.30	2	0.15	0.30	3	0.15	0.45	1.85

EK:1/C

3) Denetim alanlarının önceliklendirilmesi

Denetim alanları, risk düzeylerine göre aşağıda sıralanmıştır.

(X) İDARESİ DENETİM ALANLARININ ÖNCELİK SIRALAMASI

DENETİM ALANLARI	RİSK KRİTERİ PUANLARI	RİSK DÜZEYİ	RİSK ÖNCELİĞİ
A	4.25	YÜKSEK	1
B	4.15		
C	3.25		
D	3.00	ORTA	2
İ	3.00		
G	2.70		
E	2.15	DÜŞÜK	3
F	2.00		
J	1.85		
H	1.75		

EK:2/A

(Y) İDARESİ " GÖRECELİ RİSK DEĞERLENDİRMESİ" ÖRNEĞİ

1) Denetim evreninin tanımlanması ve denetim alanlarının belirlenmesi

(Y) idaresiyle ilgili olarak; denetim evreni idarenin tüm faaliyetleri olarak tanımlanmış, denetim alanları olarak da A-F alanları belirlenmiştir.

2) Yapısal risk düzeylerinin belirlenmesi

2.1) Yapısal risk kriterlerinin tanımlanması

İdarenin faaliyetlerine etki eden beş risk kriteri tanımlanmıştır. Bunlar; bütçe büyüklüğü, işlem hacmi ve personel sayısı, faaliyetlerin karmaşıklığı, yapısal, işlevsel ve teknik değişiklikler ile bilgi teknolojileri sisteminin yapısıdır.

2.2) Yapısal risk düzeyinin ölçülmesi

Denetim alanlarının risk kriterleri karşısındaki durumu değerlendirilmek suretiyle yapısal risk düzeyleri aşağıdaki şekilde belirlenmiştir.

(Y) İDARESİ RİSK KRİTERLERİNİN VE DEĞERLENDİRME ÖLÇEĞİNİN TANIMLANMASI

RİSK KRİTERLERİ	RİSKİN OLASILIK VE ETKİ KATSAYILARI		
		OLASILIK (0)	ETKİ (E)
Bütçe Büyüklüğü	100'den fazla	5	5
	60-100	4	4
	20-60	3	3
	5-20	2	2
	5'den az	1	1
İşlem Hacmi Ve Personel Sayısı	İşlem Hacmi Yüksek-Personel Sayısı Çok Yetersiz	5	5
		4	4
		3	3
		2	2
	İşlem Hacmi ve Personel Sayısı Dengeli	1	1
Faaliyetlerin Karmaşıklığı	Çok Karışık Faaliyetler	5	5
		4	4
		3	3
		2	2
	Karışık Olmayan Faaliyetler	1	1
Yapısal, İşlevsel Ve Teknik Değişiklikler	Çok Sık Değişiklik Var	5	5
		4	4
		3	3
		2	2
	Nadiren Değişiklik Var	1	1
Bilgi Teknolojileri Sisteminin Yapısı	Çok Geniş	5	5
		4	4
		3	3
		2	2
	Çok Geniş Değil	1	1

EK:2/B

(Y) İDARESİ DENETİM ALANLARININ YAPISAL RİSK DÜZEYLERİNİN ÖLÇÜLMESİ

Denetim Alanları	Bütçe Büyüklüğü (1)	İşlem Hacmi Ve Personel Sayısı (2)	Faaliyetlerin Karmaşıklığı (3)	Yapısal, İşlevsel Ve Teknik Değişiklikler (4)	Bilgi Teknolojileri Sisteminin Yapısı (5)	Risk Puanı	Toplam Risk Derecesi (%)
A	O: 5 E:5 R:25	O: 4 E:4 R:16	O: 4 E:3 R:12	O: 2 E:3 R:6	O:4 E:3 R:12	71	9.46 [71/(25x30)]
B	O: 4 E:4 R:16	O:3 E:4 R:12	O:3 E:4 R:12	O:4 E:4 R:16	O:3 E:2 R:6	62	8.26
C	O: 4 E:5 R:20	O:4 E:4 R:16	O:2 E:3 R:6	O:2 E:3 R:6	O:4 E:3 R:12	60	8.00
D	O:3 E:2 R:6	O:4 E:2 R:8	O:2 E:2 R:4	O:3 E:3 R:9	O:2 E:2 R:4	31	4.13
E	O:4 E:4 R:16	O:2 E:2 R:4	O:3 E:2 R:6	O:5 E:2 R:10	O:4 E:3 R:12	48	6.40
F	O: 3 E:4 R:12	O:3 E:2 R:6	O:3 E:3 R:9	O: 4 E:3 R:12	O:4 E:4 R:16	55	7.33
Risk Puanı	95	62	49	59	62	327	
Toplam Risk Derecesi (%)	12.66	8.26	6.53	7.86	8.26		43.60

EK:2/C

3) Denetim alanlarının önceliklendirilmesi

Denetim alanları, risk düzeylerine göre aşağıda sıralanmıştır.

(Y) İDARESİ RİSK MATRİSİ

OLASILIK					
	5	10 E4	15	20	25 A1
	4	8 D2	12 A3,A5,C5,E5,F4	16 A2,B1,B4,C2,E1,F5	20 C1
	3	6 D1,E3,B5,F2	9 D4,F3	12 B2,B3,F1	15
	2	4 D3,D5,E2	6 A4,C3,C4	8	10
	1	2	3	4	5
	ETKİ				

Tabloda kırmızı işaretli alanlar, yüksek düzeyde risk içeren alanları; sarı işaretli alanlar, orta düzeyde risk içeren alanları; mavi işaretli alanlar, düşük düzeyde risk içeren alanları ve yeşil işaretli alanlar ise kabul edilebilir düzeyde risk içeren alanları göstermektedir.

Tabloda yer alan örneğin A1 ifadesi, A denetim alanının 1'inci risk kriteri olan "Bütçe Büyüklüğü"nün 25 risk kriteri puanına sahip olduğunu ve dolayısıyla denetlenebilir alan önceliklerinin belirlenmesinde A alanının tamamının değil sadece "Bütçe Büyüklüğü" risk kriterine ilişkin süreçlerinin dikkate alınması gerektiğini ifade etmektedir.

İç denetim birimi, yüksek ve orta düzeyde risk içeren alanları denetlemek için gerekli tedbirleri almak zorundadır. Düşük derecede risk içeren alanlar, eldeki kaynakların yeterliliği ölçüsünde denetlenmelidir. Kabul edilebilir düzeyde risk içeren alanlar için ise, bir eylem planına gerek yoktur.

EK:2/D

(Y) İDARESİ DENETİM ALANLARININ ÖNCELİK SIRALAMASI

DENETİM ALANLARI	RİSK KRİTERİ PUANLARI	RİSK DEĞERLEME ORANI (%)	RİSK DURUMU	RİSK ÖNCELİĞİ
A1	25	100	Kabul Edilemez	Öncelikle Denetle (1)
C1	20	80	Kabul Edilemez	Öncelikle Denetle (1)
A2,B1,B4,C2,E1,F5	16	64	Kabul Edilemez	Öncelikle Denetle (1)
A3,A5,C5,E5,B2,B3,F1,F4	12	48	Sorunlu	Denetle (2)
E4	10	40	Sorunlu	Denetle (2)
D4,F3	9	36	Sorunlu	Denetle (2)
D2	8	32	İkinci Derece Sorunlu	Kaynak Varsa Denetle (3)
A4,C3,C4,D1,E3,B5,F2	6	24	İkinci Derece Sorunlu	Kaynak Varsa Denetle (3)
D3,D5,E2	4	16	Kabul Edilebilir	Kabul Et Denetleme