Yönetim Beyanına İlişkin Esaslar

1) Amaç

Yönetim beyanının amacı, Kurum, Kuruluş ve Ortaklıkların yönetim kurulunun, bilgi sistemlerine ilişkin iç kontrollerinin bilgi sistemleri bağımsız denetim dönemi açısından etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, bu çerçevedeki mevcut durum ve yürütülen çalışmalara ilişkin güvence sunmasıdır.

2) Kapsam

Kurum, Kuruluş ve Ortaklar, yönetim beyanı çerçevesinde bilgi sistemlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin kanaat oluştururken, Tebliğin 5 inci maddesinde yer verilen bilgi sistemleri bağımsız denetim kapsamını dikkate alır.

Bilgi sistemleri dâhilinde değerlendirilecek alanlar, risk odaklı bir bakış açısıyla ve önemlilik kriteri esas alınarak belirlenir. Bu değerlendirme kapsamı, yönetim beyanında bilgi sistemlerinin bütünü için verilecek görüşe makul güvence sunacak ölçüde yeterli denetim kanıtının temin edilmesine imkân sağlayacak şekilde belirlenir.

Yönetim beyanı sadece bilgi sistemlerine ilişkin iç kontroller hakkında düzenlenir. Yönetim beyanı oluşturulurken alınan destek hizmetleri de göz önünde bulundurulur.

3) Dönem

Kurum, Kuruluş ve Ortaklıkların yönetim kurulu, yönetim beyanını, cari bilgi sistemleri denetim dönemine ilişkin yürütülen çalışmalar ve değerlendirmeler neticesinde oluşturur. Bu bağlamda esas alınacak dönem 1 Ocak -31 Aralık dönemi olup, yönetim kurulu bu dönemin sonu itibariyle, bilgi sistemleri bağımsız denetim raporu tarihi ile uyumlu olarak beyanda bulunur.

4) İçerik

Yönetim beyanında açık ve kesin ifadelerle, asgari olarak:

a) Kurum, Kuruluş ve Ortaklıkların VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'ne istinaden etkin, yeterli ve uyumlu bir iç kontrol sistemi kurma ve işletme yükümlülüğünün bulunduğu,

b) İlgili birimlerce, iç kontrol sisteminin incelenmiş ve bu sistem hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılmış olduğu,

c) İlgili birimlerce iç kontrol sistemi hakkında yapılan değerlendirmede bağımsız denetim kuruluşu tarafından gerçekleştirilen çalışmaların kullanılmadığının taahhüt edildiği,

ç) İç kontrol sistemi üzerinde -varsa- tespit edilen önemli kontrol eksiklikleri,

d) İç kontrol sisteminin, Tebliğ'in 10'uncu ve VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslar açısından etkinliği, yeterliliği veya uyumluluğuna engel teşkil edecek ve beyan edilenlerin haricinde herhangi bir önemli kontrol eksikliğinin olmadığı,

e) İç kontrol sistemi üzerinde yapılan değerlendirmelerde -dönem sonu itibariyle düzeltilmiş olsa dahi- tespit edilen iç kontrol sistemine ilişkin tüm kontrol zayıflıklarının, kayda değer ve önemli kontrol eksikliklerinin sınıflandırılarak bilgi sistemleri bağımsız denetçisine sunulduğu,

f) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere Kurum, Kuruluş ve Ortaklıklar açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen ya da önemli seviyede olmasa da yöneticilerin veya iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu tüm suiistimal veya yolsuzluklar,

g) Daha önceki bilgi sistemleri bağımsız denetimlerinde tespit edilip Kurum, Kuruluş ve Ortaklıklara sunulmuş ve yetkili kuruluş tarafından çözüldüğü onaylanmamış olan bulguların çözülüp çözülmediğine ilişkin mevcut durumuna yönetim beyanı ekinde yer verildiği,

h) İç kontrol sisteminde gerçekleştirilen incelemeleri takiben, önemli ve kayda değer kontrol eksiklikleri konularında Kurum, Kuruluş ve Ortaklıklar tarafından alınmış olan düzeltici önlemleri de içerecek şekilde, iç kontrol sisteminde veya iç kontrol sistemini önemli derecede etkileyebilecek diğer hususlarda meydana gelmiş olan değişiklikler,

beyan edilir.

Bilgi Sistemleri Denetimlerinde Tespit Edilen Bulguların Kodlanması

Bağımsız denetim kuruluşlarınca bilgi sistemleri denetimlerinde tespit edilen bulgular aşağıda açıklanan şekilde kodlanır.

Kodlamadaki alanlara ilişkin açıklamalar aşağıdadır.

Denetim Yılı	.	K/S	.	Kontrol Alanı	.	Bulgu Sıra No	.	Önemlilik Derecesi	.	Önemlilik Derecesi 2

Kodlamadaki alanlara ilişkin açıklamalar aşağıdadır.

Denetim Yılı: Bu alana bulgunun tespit edildiği denetim yılı dört hane olarak (2016, 2017, ...) yazılır.

K/S: Konsolide bilgi sistemleri denetimi bulguları için "K", solo bilgi sistemleri denetimi bulguları için "S" harfi kullanılır.

Kontrol Alanı: Bu alana bulgunun tespit edildiği kontrol alanının kısaltması yazılır.

Kontrol Alanı	Kısaltma
Bilgi Sistemlerinin Yönetilmesi	**BSY**
Bilgi sistemleri yönetiminin oluşturulması ve hayata geçirilmesi	BSY-1
Bilgi güvenliği politikası	BSY-2
Üst yönetimin gözetimi ve sorumluluğu	BSY-3
Bilgi sistemleri risk yönetimi	BSY-4
Güvenlik testi	BSY-5
Diğer	BSY-DGR
Bilgi Sistemleri Kontrollerine İlişkin Esaslar	**BSK**
Bilgi sistemleri kontrollerinin tesisi ve yönetilmesi	BSK-1
Varlık yönetimi	BSK-2
Görevler ayrılığı prensibi	BSK-3
Fiziksel ve çevresel güvenlik	BSK-4
Ağ güvenliği	BSK-5
Kimlik doğrulama	BSK-6
Yetkilendirme	BSK-7
İşlemlerin, kayıtların ve verilerin bütünlüğü	BSK-8
Veri gizliliği	BSK-9
Bilgi sistemlerine ilişkin dış kaynak yoluyla alınan hizmetlerin yönetimi	BSK-10
Müşteri bilgilerinin gizliliği	BSK-11
Müşterilerin bilgilendirilmesi	BSK-12
Üçüncü taraflarla bilgi değişimi	BSK-13
Denetim izlerinin oluşturulması	BSK-14
Zaman Senkronizasyonu	BSK-15
Bilgi Güvenliği İhlali	BSK-16
Bilgi sistemleri edinimi, geliştirilmesi ve idamesi	BSK-17
Bilgi sistemleri sürekliliği	BSK-18
Değişiklik yönetimi	BSK-19
Diğer	BSK-DGR

Bulgu Sıra No: Bu alana solo bilgi sistemleri denetimi raporunda yer alan tüm bulgular, tespit edildiği süreç ve denetim alanından bağımsız olarak, **her yıl için 1**'den başlayacak şekilde numaralandırılır. Konsolide bilgi sistemleri denetimi raporundaki bulgular da, tespit edildiği ortaklık, süreç ve denetim alanından bağımsız olarak, **her yıl için 1**'den başlayacak şekilde numaralandırılır. Numaralandırma sonrasında bulguya ait sıra no bilgisi üç haneli olarak girilir (001, 162, ... gibi).

Önemlilik Derecesi: Bu alana bulgu ilk tespit edildiğinde, bulguya verilen önemlilik derecesi girilir. Bu bilgi takip eden dönemlerde değiştirilmez. Kontrol zayıflığı olarak sınıflandırılan bulgular için "KZ", kayda değer kontrol eksikliği olarak sınıflandırılan bulgular için "KD", önemli kontrol eksikliği olarak sınıflandırılan bulgular için "ÖK" kısaltmaları kullanılır.

Önemlilik Derecesi 2: Bu alana önceki dönemlerde tespit edilen bulguların önemlilik derecesinde, cari dönem itibariyle değişiklik oluştuğu durumlarda, bulgunun yeni önemlilik derecesi girilir. Bulgunun önemlilik derecesinin birden fazla değiştirildiği durumlarda, bulguya son durum itibariyle verilen önemlilik derecesi bu alana girilir. **Bulgunun önemlilik derecesinde bir değişiklik yoksa bu bölüm boş bırakılır.**

Örnek Kodlamalar:
2016.S.BSY-1.003.ÖK.KD
2014.S.BSK-2:152.ÖK
2015.K.BSY-3.045.KD

EK-3

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Olumlu Görüş)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Denetçi Görüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-4

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Şartlı Görüş)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleriyle ilgili tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemleri bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

Görüşümüze göre, yukarıda (....ncı paragrafta) açıklanan husus(lar) nedeniyle, denetlenenin bilgi sistemleri üzerinde bu hususun/hususların muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-5

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Olumsuz Görüş)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu bulunmama sebepleri)

[Denetçi Görüşü]

Görüşümüze göre, yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Görüşten Kaçınma)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ..... A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

(Denetçinin görüş bildirmemesinin nedenleri)

[Denetçi Görüşü]

Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleriyle ilgili tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı