STEP YAZILIM TEKNOLOJİ
FİNANSAL DANIŞMANLIK
LİMİTED ŞİRKETİ

SPK VII - 128.10

Bir IT Projesi Değildir

Bir Yönetim ve Denetim Modelidir

Değerleme Şirketleri için Yol Haritası

Step Veri Güvenliği

Biz Kimiz?

- 150+ KVKK ve bilgi güvenliği projesi
- Finans, sağlık, üretim sektör deneyimi
- Değerleme sektörü ile doğrudan çalışma
- Regülasyon odaklı danışmanlık yaklaşımı
- Denetim hazırlık süreçlerinde aktif rol almış deneyim

SPK Tebliği Ne Getiriyor?

- Yönetim sorumluluğu zorunluluğu
- Bilgi güvenliği organizasyonu kurulması
- Risk yönetimi yaklaşımı
- Dokümante edilmiş süreçler
- Denetime hazır yapı

“Bu bir teknoloji yatırımı değil, yönetim modelidir”

Tebliğ Aslında Ne İstiyor?

- Bu tebliğ bir “IT yatırımı” değildir
- Bu tebliğ bir “yönetim sistemi”dir
- Denetim bakış açısıyla yazılmıştır

“Firewall alarak uyum sağlanmaz”

Step Veri Güvenliği

Tebliğ Maddelerini Nasıl Okumak Gerekir?

- Tebliğ teknik değil, yönetsel bir dokümandır
- Her madde 3 soruya cevap verir:

  Ne kurulmalı
  Nasıl işletilmeli
  Kim sorumlu

Tebliği Nasıl Yorumlamalı?

Tebliğ Başlığı	Ne Kurulmalı	Nasıl İşletilmeli	Kim Sorumlu
Bilgi Sistemleri Yönetimi (Md.5)	Bilgi sistemleri yönetim yapısı, strateji	İş hedefleri ile uyumlu sürekli gözden geçirme	Üst Yönetim
Bilgi Güvenliği Politikası (Md.6)	Yazılı politika ve doküman seti	Yıllık gözden geçirme ve güncelleme	Üst Yönetim
Yönetim Gözetimi (Md.7)	Gözetim mekanizması, raporlama yapısı	Düzenli izleme, onay ve kaynak tahsisi	Yönetim Kurulu / Üst Yönetim
BG Sorumlusu (Md.7/5)	Bağımsız BG sorumlusu rolü	Riskleri izleme, raporlama	Üst Yönetim'e bağlı BG Sorumlusu
Risk Yönetimi (Md.8)	Risk analizi ve yönetim süreci	Yılda en az 1 kez analiz ve aksiyon takibi	BG Sorumlusu + Yönetim
Kontroller (Md.9)	Süreç ve kontrol yapısı	Sürekli izleme ve raporlama	Süreç sahipleri + Yönetim
Varlık Yönetimi (Md.10)	Varlık envanteri	Güncel tutma ve sınıflandırma	Varlık sahipleri
Görevler Ayrılığı (Md.11)	Rol ayrımı	Düzenli gözden geçirme	Üst Yönetim
Ağ & Sistem Güvenliği (Md.13-14)	Teknik güvenlik kontrolleri	Sürekli izleme ve güncelleme	IT + BG Sorumlusu
Kimlik & Erişim (Md.15-16)	Kimlik doğrulama ve yetki yapısı	Periyodik kontrol ve loglama	IT + Süreç sahipleri
Veri Güvenliği (Md.17-18)	Veri koruma ve sınıflandırma	Şifreleme, erişim kontrolü	IT + Yönetim
Dış Hizmet (Md.19)	Outsource yönetim modeli	Performans ve güvenlik takibi	Üst Yönetim
Kayıt & Log (Md.22)	Log ve denetim izi mekanizması	5 yıl saklama ve izleme	IT + BG Sorumlusu
İhlal Yönetimi (Md.24)	Olay müdahale planı	Olay kaydı, raporlama	BG Sorumlusu
Süreklilik (Md.27)	İş sürekliliği ve DR planı	Test, yedekleme ve geri dönüş	Üst Yönetim + IT
İç Denetim (Md.29)	İç denetim mekanizması	Yıllık denetim ve aksiyon takibi	İç Denetim

"Firmaların en çok zorlandığı yer 'ne kurulmalı' değil, 'nasıl işletilmeli' kısmıdır."

Zorunlu Başlıklar

Bilgi Güvenliği Organizasyonu
BG Sorumlusu Ataması
Risk Analizi ve Takibi
Politika ve Prosedür Seti
Olay Yönetimi
İş Sürekliliği
Yönetim Raporlaması

“Denetim bu başlıkların tamamının çalıştığını görmek ister”

Madde Bazlı Uygulama Yönetim Katmanı

Kapsam : Madde 5-6-7

Başlık	Açıklama
Politika	Yazılı olmalı, yönetim onaylı
Strateji	İş hedefleri ile uyumlu
Sorumluluk	Üst yönetimde

“Denetimde ilk bakılan yer burası.
Bu yapı kurulmadan diğer maddeler sağlıklı ilerlemez”

BG Sorumlusu – En Kritik Gereklilik

- En az 5 yıl tecrübeli
- IT’den bağımsız
- Üst yönetime raporlar

“Denetimde en kritik kontrol noktasıdır.
Yanlış atanırsa tüm yapı geçersiz sayılabilir”

Step Veri Güvenliği

Risk Yönetimi – Madde 8

- Yılda en az 1 risk analizi
- Tüm varlıklar kapsanır
- Aksiyon planı oluşturulur

“Excel doldurmak değil, risk yönetmek”

Varlık Yönetimi – Madde 10

- Tüm bilgi varlıkları envantere alınır
- Sahibi belirlenir
- Sınıflandırılır

Teknik Kontroller – Ama Ne Kadar?

Kapsam : Madde 12-18

- Ağ güvenliği
- Kimlik yönetimi
- Erişim kontrolü
- Veri gizliliği

Ama önemli olan:

Ölçeğe uygunluk

Risk bazlı yaklaşım

“Tüm teknik kontroller, risk seviyesine göre belirlenir”

“Her firma için aynı seviyede uygulanmaz”

Dış Hizmet - En Yanlış Anlaşılan Konu

- IT dışarıdan olabilir
- Sorumluluk içeride kalır

“Outsource = sorumluluktan kurtulmak değildir”

Olay ve Süreklilik Yönetimi

Kapsam : Madde 24-27

- İhlal yönetimi
- Müdahale planı
- Yedekleme
- Felaket senaryosu

Step Veri Güvenliği

Aynı Tebliğ – Farklı Uygulama

Başlık	Küçük Ölçek (10–20 kişi)	Orta Ölçek (20–50 kişi)	Büyük Ölçek (50+ / şubeli)
Yönetim Yapısı	Basit sorumluluk tanımı	Yazılı rol ve sorumluluklar	Komite / düzenli yönetim toplantısı
BG Sorumlusu	Dış hizmet olabilir	Dış + iç koordinasyon	İç + dış birlikte
Risk Yönetimi	Yıllık basit analiz	Detaylı analiz + aksiyon takibi	Sürekli izleme + raporlama
Dokümantasyon	Temel politika seti	Genişletilmiş prosedür seti	Tam kapsamlı doküman yapısı
Teknik Kontroller	Temel güvenlik önlemleri	Orta seviye kontroller	Gelişmiş katmanlı güvenlik
Erişim & Yetki	Basit yetkilendirme	Rol bazlı erişim	Detaylı RBAC + log analizi
Log & İzleme	Temel kayıt	Merkezi loglama	SIEM / ileri analiz
İhlal Yönetimi	Basit müdahale planı	Yazılı süreç + kayıt	Gelişmiş olay yönetimi
Süreklilik (DR)	Temel yedekleme	DR planı + test	Tam DR + senaryo testleri
Denetim Hazırlık	Doküman + temel yapı	Süreç + raporlama	Yönetim dashboard + KPI

“Önemli olan büyük sistem kurmak değil, doğru sistemi kurmaktır.”

Step Veri Güvenliği

Muafiyet Ne Anlama Gelir?

Alan	Muaf Olan Firmalar (Değerleme dahil)	Ne Yapmak Zorunda Değil	Ne Yapmak Zorunda
Sızma Testi	Evet (bazı fıkralar)	Her durumda zorunlu değil	Risk varsa yaptırmalı
İleri Teknik Kontroller	Kısmen	Tüm ileri seviye sistemler	Temel güvenlik şart
SIEM / ileri log	Kısmen	Büyük sistem zorunlu değil	Log tutulmalı
İç Denetim (tam kapsam)	Kısmen	Büyük yapı zorunlu değil	Denetim mantığı kurulmalı
DR ileri seviye	Kısmen	Full yedek veri merkezi değil	Yedekleme şart
Uygulama güvenliği detayları	Evet	Tüm teknik maddeler değil	Risk bazlı önlem

Muafiyet = daha basit uygulama

Muafiyet ≠ yapmamak

Denetimde Ne Sorulur?

- BG sorumlusu kim?
- Politika var mı?
- Risk analizi güncel mi?
- İhlaller nasıl yönetiliyor?
- Yönetim rapor alıyor mu?

“Bu soruların tamamı denetimde doğrudan sorulmaktadır
Bu soruların cevabı yoksa, yapı eksik kabul edilir”

Sahada Karşılaşılan Temel Problemler

- Doküman var, uygulama yok
- BG sorumlusu yanlış konumda
- Risk analizi güncel değil
- Tüm IT dışarıda ama sorumluluk içeride

Doğru Yaklaşım vs Yanlış Yaklaşım

Ürün satın almak
Copy-paste doküman
Formalite risk analizi

Yönetim modeli kurmak
Süreçleri işletmek
Denetime hazır olmak

Firmalar Aslında Şunu Soruyor

- Minimum ne yapmalıyım?
- Denetimde ne sorulacak?
- IT firmam yeterli mi?
- Dışarıdan alınabilir mi?

“Şimdi bunu netleştirelim”

Step Veri Güvenliği

Nasıl İlerleyebilirsiniz?

- Mevcut durum analizi
- Yol haritası oluşturma
- Doküman seti
- Süreç kurulumu
- Denetim hazırlığı

“Bu süreç tek seferlik değil, sürdürülebilir yapı gerektirir”

Bu Süreci Nasıl Yönetiyoruz?

Mevcut Durum Analizi
Uyum Yol Haritası
Doküman Seti Oluşturma
Süreç Kurulumu
Denetim Hazırlığı

“Adım Adım Yaklaşım”

Bu Süreçte En Kritik Başarı Faktörü

- Yönetimin süreci sahiplenmesi
- BG sorumlusunun doğru konumlanması
- Sürecin IT değil yönetim tarafından yönetilmesi

“Bu 3 başlık doğru kurulmazsa, diğer tüm çalışmalar yetersiz kalır”

Kapanış

- Bu bir IT projesi değildir
- Bu bir yönetim modelidir
- Denetim hazırlığı esastır

Teşekkürler

+90(542) 604 01 29
eozurun@stepveriguvenligi.com
https://www.stepveriguvenligi.com