BİLGİ GÜVENLİĞİ DANIŞMANLIĞI REHBERİ

1. KAPSAM VE AMAÇ

1.1. Bilgi Güvenliği Danışmalığı nedir?

ISO 27001 BGYS kurulum çalışmalarının yapılması veya mevcut süreçlerin iyileştirilmesi, Fark Analizi, Belgelendirme denetimi hazırlığı, Sızma Testi, Sosyal Mühendislik Testi, Sistem Sıkılaştırma, Siber Güvenlik, vb. konularına ilişkin danışmanlık hizmetinin alınmasını kapsamaktadır.

1.2. ISO 27001 BGYS danışmanlık hizmeti alınması planlanıyor ise;

1.2.1. ISO 27001 BGYS'nin kapsamı belirlendi mi?

BGYS kapsamının belirlenmesi, kurum ihtiyaç duyduğu danışmanlık hizmetinin çerçevesinin çizilmesi ve maliyetlerin doğru belirlenmesi açısından önemlidir. Alınacak danışmanlık hizmetinin kapsamı, danışmanlık hizmetinin kaç adam/gün süreceğinin belirlenmesinde de önem arz etmektedir. Bu yüzden danışmanlık hizmeti öncesinde, işin ilk adımı olarak kapsamın belirlenmesi gerekir.

Danışmanlık hizmetinin mevcut süreçlerin iyileştirilmesi için mi yoksa yeni bir sertifika alımı için mi istendiği net olarak belirlenmelidir. Hangi organizasyonel birimlerin BGYS'ne dahil edilip edilmeyeceği, mevcut servis ve hizmetlerden hangilerinin yönetim sisteminin konusu olacağı, çalışmanın başından belirlenmelidir. Gerekli olmayan organizasyonların, personellerin, envanter ve süreçlerin bu çalışmaya dahil edilmesi ek maliyetlere sebep olacaktır. Bunun yanı sıra, çalışma kapsamına dahil edilecek kişilerin mesai saatlerinden bu çalışmaya zaman ayırması gerektiği unutulmamalıdır.

Kapsam belirlenirken aşağıdaki hususlara dikkat edilmelidir:

- Kapsama dâhil edilecek organizasyonel birimlerin lokasyon bilgileri
- Kapsama dâhil edilecek organizasyonel birimler
- Kapsama dâhil edilecek personel sayısı
- İç ve dış tarafların listesi
- BT envanter bilgileri
- Yasal zorunluluklar ve sözleşmeden doğan gereksinimler

1.2.2. BGYS kapsamlı fark analizi çalışması talep ediliyor mu?

Fark analizi, BGYS için danışmanlık hizmeti alacak kuruluşun hedeflediği konum ile şu an bulunduğu durum arasındaki farkın ne olduğunun detaylı olarak çıkarıldığı bir analizdir. Fark analizi yapılırken önce kurumun standardın ana maddelerini (4. Madde ile 10. Madde arasındaki maddeler) ne derecede sağlandığı ile ilgili bir değerlendirme yapılır. Daha detaylı bir fark analizi için bu uygunluk kontrollü standardın Ek-A'sı içerisinde bulunan 114 kontrol maddesi için de yapılır. Bu tip detaylı bir fark analizi adam/gün maliyetlerinin artmasına sebep olabilir.

Yapılan fark analizinin en büyük avantajı belirlenen kapsamdaki birimlerin standardın hangi maddesi karşısında ne kadar uygun olduğu ve standarda yüzde (%) olarak ne kadar uyum sağladığın görülebilmesidir.

1.2.3. BGYS kapsamlı sızma testi talep ediliyor mu?

BGYS çalışması neticesinde ISO 27001 sertifikası alınması gibi bir hedef var ise yılda en az 1 kez kurumun kapsam içinde kalan envanterler için bağımsız bir firma tarafından sızma testlerini yaptırması gerekmektedir. Bu sızma testleri kapsamında sosyal mühendislik testleri de dahil edilmesi kurum Bilgi Güvenliği farkındalığının ölçülmesi açısından faydalı olacaktır. Sosyal Mühendislik çalışması kapsama ek olarak eklenen bir çalışmadır.

Eğer sertifika hedefi yok ise sızma testleri bir zorunluluk değildir, fakat günümüzde yaşanan siber saldırıların gerçekleşmeden önlenebilmesi için söz konusu sistemlere yılda en az 1 kez sızma testlerinin uygulanarak çıkan açıkların en kısa sürede kapatılması önerilmektedir.

1.2.4. ISO 27001 BGYS iç ve dış denetimi talep ediliyor mu?

Kurumun geçerliliği devam eden ISO 27001 BGYS sertifikası varsa veya danışmanlık hizmetinin sonunda sertifika hedefleniyorsa hizmet kapsamına iç denetimde dâhil edilebilir. İç denetimin danışmanlık hizmeti veren danışman dışında ki başka bir kişi veya kişiler tarafından yapılmasına dikkat edilmelidir. ISO 27001 BGYS kapsamının içeriğine göre iç denetim yapılacak gün ve danışman sayısı değişiklik gösterebilir.

Anahtar teslim projelerde danışmanlık hizmetine dış denetim firmasıyla koordinasyonun sağlanması, dış denetim hizmetin maliyetinin karşılanması gibi konularda dahil edilebilmektedir. Bu ihtiyaçlar önceden belirlenerek danışmanlık hizmeti kapsamında değerlendirilebilir.

1.3. Sızma testi hizmeti alınması planlıyor ise;

1.3.1. Sızma testi yapılması gereken sistemler belirlendi mi?

Sızma testi çalışması öncesinde testin kapsamı net olarak belirlenmelidir. Etkilenecek iç ve dış tarafların gereklilikler listesinin çıkarılması, etkilenecek altyapıların kritiklik seviyelerinin tespit edilmesi gerekmektedir. Kapsam belirlenirken aşağıdaki sayılar netleştirilmeli ve danışman ile sızma testinin sistemleri etkilemeyeceği bir zaman diliminde proje takvimi için anlaşılmalıdır.

- Kurumun ağ yapısı (İntranet/internet/DMZ) ve bileşenleri;
- Son kullanıcı cihazı sayısı
- Sunucu sayısı
- Ağ cihazı sayısı
- Veri tabanı sayısı ve çeşitleri
- Kablosuz ağ sayısı (SSID)

1.3.2. Sızma testi yapılması gereken kurumsal uygulamalar belirlendi mi?

Sızma testi kapsam çalışmaları sırasında dikkate alınması gereken bir diğer konu da kurum web sitelerinin, kuruma özel geliştirilmiş ya da satın alınmış uygulamaların sızma testine dâhil edilip edilmeyeceğine karar verilmesidir. Bu uygulamaların sızma testlerinin internet üzerinden mi yoksa intranet üzerinden mi yapılacağı testin planlama aşamasında belirlenmelidir.

1.3.3. Kaynak kod analizi talep ediliyor mu?

Kod güvenliğine yönelik testler ayrı bir kapsam oluşturmakta ve bu testler için ayrıca maliyet çalışması yapılmaktadır. Kod zafiyetlerinin tespit edilmesi siber saldırıların hayata geçmeden önlenebilmesi açısından faydalıdır. Analizin planlama aşamasında kaynak kodun hangi dilde geliştirildi ve kod satır sayısı bilgileri belirlenmelidir.

1.3.4. Sosyal Mühendislik testi talep ediliyor mu?

Sosyal mühendislik testlerinde kurum personeline çeşitli iletişim yollarıyla (telefon, e-posta vb.) erişilerek, ikna ve kandırma yöntemleriyle personelden kritik ve kurumsal bilgiler elde edilmeye çalışılır. Sosyal Mühendislik testleri öncesinde hangi iletişim kanalı (telefon, e-posta vb.) kullanılacağı, olası senaryoların neler olacağı ve hangi kullanıcı profiline uygulanacağı kurum ile danışman ortak karar verilmelidir. Gerçek kişi ve kurum isimleri kontrollü ve izin alarak kullanılmalıdır.

1.3.5. Tespit edilen açıklıkların kapatılması için ek bir hizmet alınması planlanıyor mu?

Sızma testinin sonuç raporu bu hizmetin kapsamını belirlemekte yardımcı olacaktır. Test sonrası raporda yazılacak olan teknik açıkların detayları, açıkları kapatacak personeller tarafından net anlaşılamayabilir. Bu yüzden testi yapan kişilerin açıkları kapatacak kişilere birebir eğitim vermeleri ya da teknik destek almaları ihtiyacı doğabilir.

1.3.6. Doğrulama testi talep ediliyor mu?

Sızma testi sonucunda bulunan açıklıklar kurum tarafından kapatıldıktan sonra bu açıklıkların ne oranda kapatıldığına dair bir doğrulama testi yapılabilir. Doğrulama testi ile kurumun sızma testi sonrasında bulunana açıklıkları ne oranda kapattığı analiz edilir. Açıklıkları kapatan taraf ile doğruluma testini yapan tarafın farklı olması önerilir.

1.4. Danışmanlık hizmeti kapsamında eğitim talep ediliyor mu?

Danışmanlık hizmetinin içeriğine göre ihtiyaç duyulan eğitim konularının ve eğitim alacak personel sayılarının belirlenmesi bütçenin doğru planlanması açısından önemlidir. Eğitimin doğru planlanması için;

- Eğitim talep edilen konular
- Eğitim sonunda sertifika hedefi
- Personel sayısı
- Eğitim yöntemi (sınıf eğitimi, e-eğitim vb.)

- Eğitim gün sayısı
- Eğitim lokasyonu (kurum, eğitim merkezi vb.)

gibi kriterler göz önünde bulundurulmalıdır.

2. YAPILACAK İŞİN TANIMI

2.1. ISO 27001 BGYS'nin yönetimi için bir ürün / yazılım kullanılması planlanıyor mu?

ISO 27001 BGYS gereği yapılması gereken risk analizinin bir uygulama aracılığı ile yapılması kurumun risklerinin sağlıklı bir şekilde yönetilebilmesi için faydalıdır. Microsoft Office uygulamaları üzerinden yapılacak risk analizinin versiyon takibinin zor olması ve risk sayısına göre çok uzun dokümanların bir süre sonra anlaşılamaz olması durumu söz konusudur. Yönetim sistemi içerisinde ürün kullanımı gerektiren temel konu risk analizidir, bu kapsamda ürün/yazılım satın alımı yapılacaksa kullanıcı sayısına göre lisans ücretleri, bakım anlaşmalarının ücretleri öğrenilmelidir. Lisans ücretlerine karar verilirken bu sistemi kaç kullanıcının kullanacağı dikkate alınmalıdır. Paket bir ürün alınacak ise bu ürün hayata geçirileceği zaman bir hizmet kesintisi yaşanmaması için gerekli takvim planlaması yapılmalı, sistem kaynağı ihtiyaçları (cpu, ram, harddisk) ve bu ihtiyaçları kurumun nasıl karşılayacağı belirlenmelidir.

2.2. BGYS'nin sürekliliğinin sağlanması çalışmalarının kurum personeli tarafından yapılması planlandı mı?

Kurumun kapsam dâhilindeki tüm süreçlerinde BGYS gereksinimlerinin uygulayabilmesi, sürekliliğinin sağlayabilmesi ve sürekli olarak iyileştirebilmesi için bu süreçlerin kurum personeli tarafından yürütülmesi önemlidir. Bu sebeple danışmanlık hizmeti alınmadan önce kurum içerisindeki BGYS'den sorumlu olacak kişilerin belirlenmesi ve bu kişiler için gerekli eğitimlerin planlanması faydalı olacaktır. BGYS sorumluları için öncelikli olarak ISO 27001 Baş Denetçi sertifika eğitimleri planlanması tavsiye edilir. Eğitimlerin BGYS kurulumu öncesinde alınması, personelin hem danışman tecrübesinden yararlanması hem de pratik edinmesi açısından yarar sağlayacaktır.

3. İŞ MODELİ

3.1. Danışman firmanın kurumsallığı ve sektördeki itibarı değerlendirildi mi?

Danışman firmaya karar verilirken aşağıdaki maddeler göz önüne alınarak bir değerlendirme formu hazırlanabilir.

Danışman Firmanın;

- Sektördeki tanınırlığı
- Akreditasyonları
- Kalite belgeleri ve hangi standartlarla uyumlu oldukları
- Sertifikalı personel sayısı ve personelin nitelikleri

- Yerleşik ofisi bulunup bulunmadığı ve yakın konumda çalıştırdığı personel sayısı
- Faaliyete başladığı yıl
- Daha önce yapmış olduğu benzer danışmanlık projelerindeki referansları
  - Referans projenin büyüklüğü, karmaşıklığı, hangi noktalarda dış kaynak kullandığı/kullanacağı
  - Referans listesinde yer alan kurumlardan görüş alınması

3.2. Danışmanların proje referansları ve mesleki tecrübeleri değerlendirildi mi?

Danışmanın tecrübesini incelemek için aşağıdaki konular hakkında firmadan bilgi istenmelidir.

Danışmanın:

- Pratik iş tecrübesi
- Yönetim tecrübesi
- Kalite yönetim tecrübesi
- Kalite yönetim sistemi tetkik tecrübesi

Danışman ISO 27001 Baş Uygulayıcı (Lead Implementer), ISO 27001 Baş Denetçi (Lead Auditor) vb. sertifikalara sahip olması tercih sebebi olmalıdır. Yönetim sisteminin uygulanacağı organizasyonda her seviyedeki ilgili kişiler ile iletişim kurabilecek, onların aktif olarak kalite yönetim sisteminin gerçekleştirilmesine katılmalarını sağlayacak iletişime sahip bir danışman profili tercih edilmelidir. Danışmanın referans olarak sunduğu firmalar ile görüşülerek fikir alınmalıdır.

4. ÇIKTILAR

4.1. BGYS kapsamında yapılan fark analizi sonuçları talep edildi mi?

Bu raporda BGYS kurulum çalışmasından önce yapılan ve standarda uyumluluk düzeyini gösteren fark analizi sonuçları talep edilmelidir. Böylelikle kurum, yapılacak BGYS çalışmalarıyla standardın hangi maddelerine uyumluluk sağladığını bu rapor sonuçlarıyla karşılaştırarak takip edebilir.

4.2. BGYS kapsamında hazırlanan dokümanlar listesi talep edildi mi?

BGYS çalışmaları kapsamında hazırlanan tüm dokümanların listesi talep edilmelidir. Böylelikle kurumun mevcut dokümantasyonu haricinde oluşturulan dokümanlar bu listeden izlenebilir. Bu dokümanlar;

- Varlık listesi
- Risk değerlendirme ve işleme planı
- Bilgi güvenliği politikası ve diğer alt politikalar
- Prosedürler
- Formlar
- Talimatlar

4.3. Sızma Testi / Sosyal Mühendislik testi raporu talep edildi mi?

Bu raporda, sızma testi çalışması kapsamında gerçekleştirilen tüm faaliyet ve sonuçları, tespit ettiği bulguları, bu bulguların risk seviyeleri, bulgu kanıtları ve çözüm önerileri bulunmalıdır. Rapor iki farklı format olacak şekilde hazırlanmalıdır, bir tanesi yöneticilere yönelik olarak hazırlanmış olan özet rapor olmalıdır, diğeri de teknik tüm detayları içeren teknik çalışanlara özel okunabilir ve anlaşılır bir rapor olmalıdır. Kurumun güveliği açısından raporların kuruma şifreli bir şekilde iletilmesi gereklidir.