1. **DANIŞMANLIK HİZMETİNİN AŞAMALARI**
   1. **Açılış ve Proje Ekibinin Belirlenmesi**

ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) danışmanlık hizmeti proje ekibinin ve üst yönetimin katılacağı proje açılış toplantı ile başlayacaktır. Proje açılış toplantısında firmanızın Üst Yönetimi, Proje Ekibi ile Danışman bir araya gelecektir. Danışman tarafından ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) projesini ana hatları ile anlatacak, organizasyonel görev tanımları ile projenin uygulama yol haritası hakkında karşılıklı görüş alış-verişi gerçekleştirilecektir. Açış toplantısınde proje süreç sahiplerinin görev ve sorumlulukları netleşmiş olacaktır. **I**SO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) sürecini yönetecek, firmada uyarlanması için gerekli araştırma ve çalışmaları yürütecek bir ekibin görevlendirilmesi gereklidir. Kurumunuzda ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS)’ni yürütmekle sorumlu Bilgi Güvenliği Ekibi belirlenerek ataması yapılacaktır. Açılış toplantısında karşılıklı olarak proje planı belirlenecektir.

* 1. **GAP Analizi**

İkinci adımda mevcut bilgi güvenliği sisteminiz ile ilgili mevcut durum tespiti ve boşluk analizi gerçekleştirilecektir. Kurumunuzun mevcut uygulamaları, dokümantasyon altyapı, IT organizasyonel yapılanması, IT süreçleri ve polikaları analiz edilmesidir. Bu çalışmada mevcut bilgi güvenliği yönetim sisteminin altyapısı ve dokümantasyonu ele alınarak ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) gereksinimlerinin ve rehber standartların süzgecinden geçirilecek, boşluklar belirlenecektir. Bu aşama bir bakıma yönetim sisteminin tasarım aşaması olup, gerekli altyapı ve dokümantasyon gerçeksinimi belirlecektir. ENDERUN AKADEMİtarafından geliştirilen ISO/IEC 27001:2022 BGYS dokumantasyon boşluk analiz kontrol listesi kullanılarak firmanın mevcut durumu resimlenmiş olacaktır. Boşluk analizi sonrası tespit edilen fiziksel ve teknik boşluklar ile altyapı gereksinimleri firmanız tarafından gerçekleştirilecektir.

* 1. **Sistem Tasarımı**

ÜçüncüAdım, sistem tasarımı ve dokümanların geliştirilmesi aşamasıdır. Döküman geliştirme süreci üç adımda gerçekleşecektir. İlk adım ham dökümanların hazırlanması. İkinci adımda hazırlanan ham dökümanların gözden geçirilerek formatlanması, üçüncü aşamada üst yönetimin onayına sunulup dökümanın geçerli ve kontrollü kılınması. Sürecin en fazla zaman alan aşaması döküman geliştirme aşamasıdır.

**Döküman Modellemesi**

Danışman ve proje ekibi taraından ISO/IEC 27001:2022 BGYS ile ilgili döküman modeli belirlenecektir. Belirlenen doküman modeline göre öncelikle ham dökümanlar; danışman rehberliğinde Proje Ekibi, ilgili süreci gerçekleştiren kişilerce kaleme alınacaktır. Ham halde hazırlanacak dökümantasyon, danışman ve Proje Ekibi tarafından gözden geçirilerek formatlanacak veISO/IEC 27001:2022 BGYS standardının temel ilkelerine göre nihai metin olarak hazırlanacaktır. Gerekli prosedür ve talimatların hazırlanarak yayınlanacaktır. ISO 27001 BGYS standart gerekleri ile ilgili aşağıdakilerle sınırlı olmamak üzere asgari aşağıdaki dokümanlar hazırlanacaktır.

* BGYS Politikaları
* BGYS Organizasyon Yapısı, Rol ve Sorumluluklar,
* İnsan Kaynakları Yönetimi ve Güvenliği
* Varlık Yönetimi ve Risk Analizi
* Erişim Yönetimi
* Fiziksel ve Çevresel Kontroller, İzleme
* Kriptografi
* İşletim ve Haberleşme
* Sistem Temini, Edinim ve Bakım
* Tedarikçi İlişkileri
* Olay ve İhlal Yönetimi
* İş Süreklilği Yönetimi
* Bilgi Silme ve Maskeleme
* Güvenli Kodlama
* Bulut Hizmetleri
* Tehdit ve Veris Sızıntısı
* Web Filitreleme
* Uyum
* İzleme Faaliyetleri
* İç denetimler,
* Dokümantasyon ve Kayıtları tutma,
* Yönetimin gözden geçirilmesi,
* Uygulanabilirlik bildirgesinin deklerasyonu,

**Varlık Envanterinin Hazırlanması**

Danışman ve proje ekibi tarafından kapsam dahilinde yer alan lokasyon ve birimlerde bilgi güvenliğine etki eden varlıklar belirlenerek varlık envanter listesi hazırlanacaktır. Belirlen varlıkların Adı, Varlık Grubu, Alt Grup, Sorumlu Departman, Varlık Sorumlusu, Yedek Durumu ve Bulunduğu Yer tepit edilerek Varlık Değeri (Gizlilik, Bütünlük ve Erişebilirlik) belirlenecektir.

**Risk Yönetimi ve Değerlendirmesi**

Varlık envanteri hazırlandıktan sonra ve ISO/IEC 27001:2022 BGYS nin kapsamına giren hizmetlerin uygulanması sırasında kullanılan ve kazanılan bilgilerin gizliliğine, doğruluğuna ve erişilebilirliğine yönelik risklerin değerlendirilmesi, uygulanması, yönetilmesi, kullanılan metodoloji, bilgi varlıklarına ve kaynaklarına etki eden tüm olayların raporlanması ve sorumluluklar tanımlanacaktır. Bu süreç aynı zamanda ISO/IEC 27001:2022 BGYS’nin alt yapı gereksinimlerini belirleyecektir. Bu kapsamda belirlenen varlıklarla ilgili açıklık ve zayıflık listeleri belirlenecektir. Varlıkların karşılaşabileceği risklerin belirlenmesi ve uygun düzenlemelerin yapılabilmesi için, kurum, tehdit ve zayıflıkları, gerçekleşme ihtimali ve gerçekleşmesi durumundaki etkilerini göz önünde tutarak değerlendirilecektir. Risk Yönetimi ve Değerlendirmesinde Risk kabulü, Riskten kaçınma, Riski azaltma ve kontrol etme, Riski yok etme, Riskin transferi edilme yöntemleri ile KABUL EDİLEBİLİR RİSK SEVİYESİ belirlenecektir.

**İş Sürekliliği Planın Hazırlanması**

Kurumunuz bünyesinde Bilgi Güvenliği iş sürekliliğini kesintiye uğratacak durumların tanımlanması ve durumların oluşması sırasında yapılacak faaliyetler belirlenecektir. Bu kapsamda felaket durumları, alt yapı ve donanınım arızaları, sistem, network ve destek birimleri arızaları, yazılımsal felaketler vs. ilgili BGYS iş sürekliliğini etkileyen acil durumlar belirlenerek bu durumların oluşmaması, oluşması durumunda ve oluştuktan sonra alınacak önlemler ve sorumluluklar belirlenecektir. İş Sürekliliğinin sağlanması için BG Acil Durum ekipleri ve Tahammül Ve Yeniden Devreye Alma Süreleri belirlenecektir.

* 1. **Uygulama**

Bu aşamada geliştirilen dökümanlar süreç sahipleri tarafından uygulamaya alınacaktır. Hazırlanan dokümanlar süreç sahipleri tarafından uygulanarak dokümanların etkinliği kontrol edilecektir. Uygulamaların geliştirilen dokümantasyona uygun olarak yapılması, kayıt altına alınarak sürdürülmesi için gerekli önlemler alınacaktır. Bu aşamada, eski dokümantasyonlar toplanacak, uygulamaya konan yeni dokümantasyona etkinlik kazandırılacaktır.

* 1. **Eğitim**

Danışmanlık hizmeti kapsamında proje ekibinde yer alan personele ISO/IEC 27001:2022 BGYS ile ilgili aşağıdaki eğitimler verileceyektir. Bu aşamada öncelikle yönetim sistemleri ve temel gerekleri ile ilgili eğitimler verilecektir.

ISO/IEC 27001:2022 BGYS İç Denetçilik Eğitimi (ISO 19011 şartlarına göre) ise dokümantasyon ve uyarlama aşamasından sonra gerçekleştirilecektir. Eğitim sonunda katılımcılara eğitim sertifikası verilecektir. İç Denetçi eğitimi sonunda yapılacak sınavda başarı olan personele iç denetçi “Başarı Sertifikası”, diğer katılımcılara ise “Katılım Sertifikası” verilecektir. Eğitim salonu ve eğitim organizasyonu BAUHAUS tarafından gerçekleştirilecektir.

|  |  |  |  |
| --- | --- | --- | --- |
| **Eğitimin Adı** | **Birim Süre** | **Grup Sayısı** | **Eğitim**  **Verilecek Grup** |
| ISO/IEC 27001:2022 BGYS Farkındalık Eğitimi | 3 Saat | 2 | Tüm Çalışanlar |
| ISO/IEC 27001:2022 BGYS (KYS) Temel ve İç Tetkikçi Eğitimi | 2 Gün | 1  (20 Kişi) | İç Denetçiler  Proje Ekibi |
| Risk Yönetimi Eğitimi / Uygulamalı | 1 Gün | 1  (20 Kişi) | Proje Ekibi  Süreç Sahipleri |

* 1. **Kontrol ve Değerlendirme**

Sistem tasarımı, eğitim ve uygulama aşamasından sonra sistemin etkinliği ve değerlendirme amacıyla iç denetçi eğitimi almış personelle iç denetim gerçekleştirilecektir. Bu aşamada, danışman gözetiminde iç denetçi eğitimi almış personel tarafından bir tam iç denetim çevrimi yapılarak, bulgular raporlanacaktır. İç Denetim Bulguları esas alınarak, kaliteli yönetim sisteminizin, üst yönetim tarafından gözden geçirilmesi sağlanacaktır. Standartların uygulanmasında son aşama olan uyarlama aşaması ile Eğitim ve Danışmanlık hizmeti tamamlanmış olacaktır. Bu aşamadan sonra, belgelendirme kuruluşuna başvurularak denetim süreci başlatılacaktır.

* 1. **Sertifikasyon**

Dokumantasyon ve danışmanlık hizmeti sonrasında denetim süreci başlatılacaktır. Belgelendirme denetimi kurumunuz tarafından belirlenen belgelendirme kuruluşu tarafından gerekleşecektir. Danışmanlık hizmeti teklifine belgelendirme bedeli dahil olmayıp bu bedel firmanız tarafından ödenecektir. Belgelendirme süresi 3 yıl olup, belgenin devamlılığının sağlanabilmesi için 12 ayda bir yıllık gözetim denetimleri gerçekleşecektir. İlk Belgelendirme denetimi 2. Aşamalı olarak gerçekleşecektir. 3 yıllık belge geçerlilik süresi içinde 1 belgelendirme, 2 adet gözetim denetim gerçekleşecektir. Üç yıllık geçerlilik süresi sonunda, belgelendirme denetiminde olduğu gibi tekrar teklif verilecek ve denetime tabi tutulur. Başarı ile gerçekleşen denetim sonucu firmanın belge kullanım hakkı 3 sene için daha uzatılmış olur. Danışmanlık hizmet bedeli ilk yıl belgelendirme öncesi danışmanlık hizmeti gerçerlidir, başarılı bir belgelendirme sonunda Enderun Akademi’nin sorumluluğu sona erer. Firmanızın talep etmesini durumunda gözetim denetimleri öncesi yapılacak danışmanlık ve gözden geçirme için ayrıca teklif verilecektir.