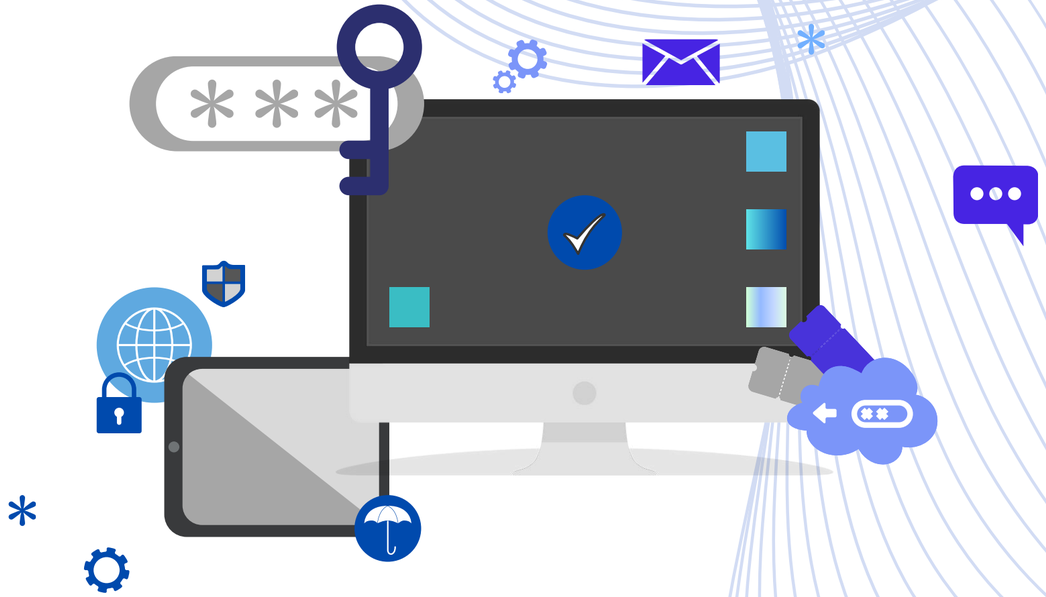
NESİL

ISO 27001
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ
TANITIM SUNUMU

www.nesilteknoloji.com

NESİL



ISO 27001 BGYS NEDİR?

ISO 27001 BGYS, Uluslararası Standart organizasyonu tarafından (ISO) yayınlanan yaklaşık 54 standarttan oluşan ISO 27000 ailesinin denetlemeye tabi olan ISO 27006'dan sonraki tek standarttır.

ISO 27001 BGYS, finansal verilerin, bilgi varlığının ve müşterilere ait özel ve kişisel bilgilerin saklanması ve korunmasına yardımcı, başta insanlar olmak üzere süreçler ve bilgi sistemlerini kapsayan ve de sürekli iyileştirmeyi ilke edinen bir yönetim sistemidir.

ISO 27001 BGYS'NİN AVANTAJLARI NELERDİR?

Kuruluşunuzun tümüne ya da seçilmiş bölgelerine kontrol uygulama esnekliği sağlar.

Tedarikçi ilişkilerinizin gelişmesini, bunları performans takip ve yönetimini sağlar.

Bilgilerinizdeki riskleri tanımlamanızı bunları yönetmek veya azaltmak için güvenlik önlemleri almanızı sağlar.

Verilerinizin güvenliğini en üst seviyeye getirme yolunda sizi yönlendirip müşteri ve kurumsal memnuniyeti sağlar.

Hazırlanacak prosedürlerle güvenlik ihlallerinin tespiti hızlıca yapabilecek ve raporlayabilecek siniz.

Yasal şartlara uygunluk konusunda sizi yönlendirir ve uygunluğunuzu arttırır.

ISO 27001 BGYS'NİN AVANTAJLARI NELERDİR?

Sürekli iyileştirme temeline dayandığından kurumu sürekli geliştirir.

Bilgi erişimini yalnız yetkili kişilere sağlayacak kontroller kurar.

Sadece Yetkili kişilerin bilgilere erişimini sağlayacak kontroller kurar.

Bilgi güvenliğinizin etkinliğini düzenli olarak gözden geçirmeyi ve ortaya çıkan yeni riskleri görüp müdahale etmeyi sağlar.

Bilgi güvenliğin bir öncelik olduğunu gösterir. Böylece en iyi uygulama sisteminin yürürlükte olduğu konusunda paydaşlara ve 3. taraflara güvence verir.

Bilgi güvenliği risklerini tanımlamak için bir çerçeve sunar. Böylece riskler için uygun metotlar, yönetim ve teknik uygulama kontrolleri sağlar.

ISO 27001 BGYS'NİN AVANTAJLARI NELERDİR?

Bilgi güvenliğine yönelik riskleri yönetmek için ortak bir dizi politika, prosedür ve kontrolün yapılmasını sağlamanın bir yolunu sağlar.

Bilgi güvenliğiyle ilgili olarak artan müşteri beklentilerine cevap vermeyi kolaylaştırır.

Bilgi güvenliği yönetimi için bir çerçeve sunar ve yasal düzenlemeleri dikkate almanızı ve böylece yasal cezalardan kurtulmanızı sağlar.

Organizasyona, bilgi yönetimi ile ilgili ihale şartlarına cevap vermek için kolay bir yol sağlar.

Kuruluşunuz genelinde bilgi güvenliği farkındalığının oluşmasını sağlar

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 1

EĞİTİM VE FARKINDALIK FAALİYETLERİ (BİLGİ GÜVENLİĞİ VE KANUN)	7.3 FARKINDALIK
KURUMSAL POLİTİKALAR (ERİŞİM, BİLGİ GÜVENLİĞİ, KULLANIM, SAKLAMA VE İMHA) VB.	EK A 7.2.2 BİLGİ GÜVENLİĞİ FARKINDALIĞI, EĞİTİM VE ÖĞRETİMİ

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 1

İDARİ TEDBİRLER	ISO 27001:2013 BGYS İLİŞKİSİ
KURUMSAL POLİTİKALAR (ERİŞİM, BİLGİ GÜVENLİĞİ, KULLANIM, SAKLAMA VE İMHA VB.	5.2 POLİTİKA
SÖZLEŞMELER (VERİ SORUMLUSU- VERİ İŞLEYEN)	EK A 7.1.2 İSTİHDAM HÜKÜM VE KOŞULLARI

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 1

GİZLİLİK TAAHHÜTNAMELERİ	EK A 13.2.4 GİZLİLİK YA DA İFŞA ETMEME ANLAŞMALARI EK A 15.1.2 TEDARİKÇİ ANLAŞMALARINDA GÜVENLİĞİ İFADE ETME
KURUM İÇİ PERİYODİK VE/VEYA RASTGELE DENETİMLER	9.2 İÇ TETKİK
RİSK ANALİZLERİ	6.1.2 BİLGİ GÜVENLİĞİ RİSK DEĞERLENDİRME 6.1.3 BİLGİ GÜVENLİĞİ RİSK İŞLEME

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 1

İŞ SÖZLEŞMESİ, DİSİPLİN YÖNETMELİĞİ	EK A 7.2.3 DİSİPLİN PROSESİ
KURUMSAL İLETİŞİM (KRİZ YÖNETİMİ, İTİBAR YÖNETİMİ)	EK A 17 İŞ SÜREKLİLİĞİ YÖNETİMİNİN BİLGİ GÜVENLİĞİ HUSUSLARI

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 2

TEKNİK TEDBİRLER	ISO 27001:2013 BGYS İLİŞKİSİ
YETKİ KONTROL	Ek A 9.2.5 Kullanıcı Erişim Haklarının Gözden Geçirilmesi
ERİŞİM LOGLARI	Ek A 9.1.2 Ağlara ve Ağ Hizmetlerine Erişim

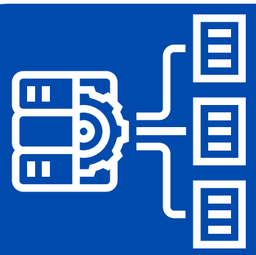
KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 2

KULLANICI HESAP YÖNETİMİ	Ek A 9.4.2 Güvenli Oturum Açma Prosedürleri
AĞ GÜVENLİĞİ	Ek A 13.1.2 Ağ Hizmetlerinin Güvenliği
UYGULAMA GÜVENLİĞİ	Ek A 14.2.6 Güvenli Geliştirme Ortamı

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 2

SIZMA TESTİ	Ek A 12.6.1 Teknik Açıklıkların Yönetimi
SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ	Ek A 12.6.1 Teknik Açıklıkların Yönetimi
LOG KAYITLARI	Ek A 12.4.1 Olay Kaydetme

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 2

 VERİ KAYBI ÖNLEME YAZILIMLARI	Ek A 12.6.1 Teknik Açıklıkların Yönetimi
 YEDEKLEME	Ek A 12.3.1 Bilgi Yedekleme
 GÜVENLİK DUVARLARI	Ek A 14.1.2 Halka Açık Ağlardaki Uygulama Hizmetlerinin Güvenliğinin Sağlanması

KVKK – ISO 27001 BGYS İLİŞKİ TABLOSU 1

 ANTİ-VİRÜS SİSTEMLERİ	Ek A 12.2.1 Kötücül Yazılımlara Karşı Kontroller
 SİLME, YOK ETME/ANONİM HALE GETİRME	Ek A 8.3.2 Ortamın Yok Edilmesi
 KEY MANAGEMENT	Ek A 10.1.2 Anahtar Yönetimi

ISO 27001 BGYS PROJE YOL HARİTASI

1. AÇILIŞ (KICKOFF) TOPLANTISI VE BGYS EKİBİNİN ATANMASI
2. GAP ANALİZİ
3. ISO 27001, FARKINDALIK VE STANDART EĞİTİMİ
4. BGYS BAĞLAM, KAPSAM, AMAÇLARIN BELİRLENMESİ
5. LİDERLİK FAALİYETLERİNİN YERİNE GETİRİLMESİ
6. PLANLAMA FAALİYETLERİNİN YAPILMASI
7. DOKÜMAN VE KAYITLARIN OLUŞTURULMASI
8. RİSK ANALİZİ EĞİTİM VE UYGULAMASI
9. 1. PERFORMANS DEĞERLENDİRME 2. İÇ TETKİK EĞİTİMİ VE UYGULANMASI 3. YÖNETİM GÖZDEN GEÇİRME TOPLANTISI (YGG)
10. DÜZELTİCİ VE İYİLEŞTİRİCİ FAALİYETLER
11. SOA VE EK-A KONTROLLERİNİN SAĞLANMASI
12. BELGELENDİRME BAŞVURUSUNUN YAPILMASI

1. AÇILIŞ (KICKOFF) TOPLANTISI VE BGYS EKİBİNİN ATANMASI

Kıdemli danışman, eğitmen ve müşteri firma yetkililerinin katılımı ile gerçekleştirilen bu toplantıda;

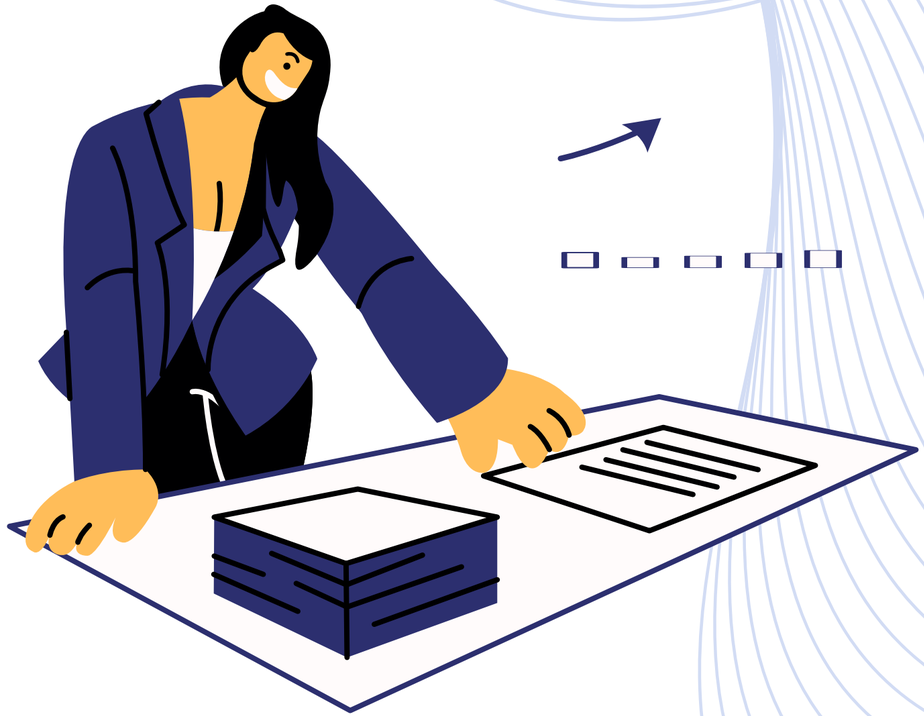
- *Proje Basamakları,*
- *Görev Dağılımları,*
- *Eğitim Tarihleri,*
- *Varlık Envanteri Hazırlığı,*
- *BGYS Ekibi Atanması*

gerçekleşmektedir.

➢ **Ayrıca BGYS ekibi oluşturulması bu toplantıda gerçekleştirileceğinden kuruluşunuzun yöneticilerin geniş katılım göstermesi önemlidir.**

2. GAP ANALİZİ

Kuruluşunuzun ISO 27001 BGYS standardına uygunluk durumunun belirlenmesi, gerekmesi halinde ne gibi çözümlerin konumlandırılması hakkında detaylı bir çalışma yapılmaktadır.



➢ **Bu çalışma sonunda Teknik Ekibimiz kuruluşunuza bir İyileştirme Raporu sunacak ve çözüm önerilerinde bulunacaktır.**

3. FARKINDALIK VE STANDART EĞİTİMİ

Nesil Teknoloji'nin alanında uzman kıdemli danışman ve eğitmenleri tarafından BGYS kapsamında tüm personelinize bilgi güvenliği farkındalık eğitimleri düzenlenmektedir.

Ayrıca BGYS Ekibine ISO 27001 Standart eğitimi de verilmektedir.

➢ **Bu sayede kurum içerisinde ISO 27001 BGYS hakkında Bilgi Teknolojileri üzerine düşen yükü hafifletmekte ve İNSAN faktöründen kaynaklanan açıklıkları en aza indirmeyi amaçlamaktadır.**

4. BAĞLAM, İLGİLİ TARAFLAR, KAPSAM VE SINIRLAR

Standardın 4. Maddesi gereği firmanın İç ve Dış Bağlamının, İlgili taraflar ve beklentilerinin tanımlanması, BGYS kapsamının belirlenmesi ve sınırlarının çizilmesi sağlanarak dokümante edilir.

5. LİDERLİK

Üst Yönetimin BGYS Sistemi için gerekli liderlik görevini yerine getirebilmesi sağlanır

Bu görevler içerisinde,

- *BGYS Ekibinin atamasının yapılması,*
- *Gerekli Kaynakların ayrılması,*
- *Rol ve sorumlulukların belirlenmesi vb.*

bulunabilir.

6. PLANLAMA

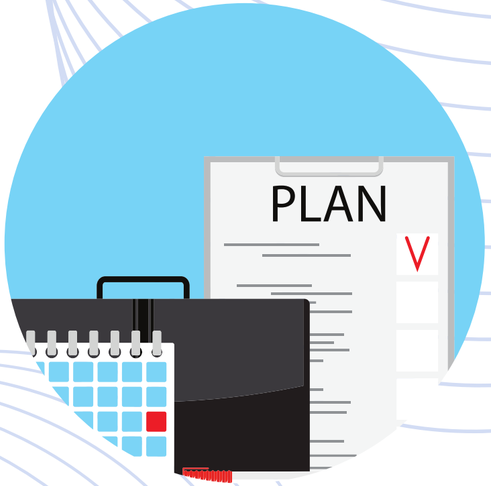
Her işte olduğu gibi yönetim sistemlerinde de planlama önemli bir süreçtir

Üst Yönetimin görevlendirdiği BGYS ekibiyle beraber PUKÖ döngüsü mantığında BGYS sisteminin planlanması sağlanır.

P	U	K	Ö
Planla	Uygula	Kontrol Et	Önlem Al

6. PLANLAMA

- *Risk ve fırsatları ele alan faaliyetler*
- *Genel (Risk ve fırsatlar için planlama)*
- *Bilgi güvenliği risk değerlendirmesi, (analizi)*
- *Bilgi güvenliği risk işleme, (SoA: Statement of Applicability) Uygulanabilirlik Bildirgesi oluşturma, uygulanabilir olmayan maddelerin gerekçelendirilmesi,*
- *Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama,*



7. DOKÜMAN VE KAYITLARIN OLUŞTURULMASI

DESTEK

- *Kaynaklar, bilgi güvenliği için gerekli kaynaklar (insan kaynağı, altyapı, donanım, yazılım vs.),*

- *Yeterlilik, bilgi güvenliği için gerekli yetkinlik ve yeterlilik kayıtları (personel geçmiş deneyim ve eğitim kayıtları),*

- *Farkındalık, bilgi güvenliği farkındalık eğitimleri (BGYS Ekibi temel standart eğitimi ve personel farkındalık eğitimi),*

- *İletişim, bilgi güvenliği için gerekli otorite ve ilgi grupları iletişimi ve yönetimi*

7. DOKÜMAN VE KAYITLARIN OLUŞTURULMASI

HAZIRLANACAK TEKNİK POLİTİKA VE PROSEDÜRLER VE DİĞER DOKÜMANLARDAN BAZILARI

POLİTİKALAR

- BGYS Politikası
- Parola Yönetimi Politikası
- Network Politikası
- Kabul Edilebilir Kullanım Politikası
- Kriptografik kontroller Anahtar Yönetimi Politikası
- Güvenli Yazılım Geliştirme Politikası
- Temiz Masa Temiz Ekran Politikası vb.

PROSEDÜRLER

- Doküman Kayıtlarının Kontrolü Prosedürü
- Varlık Yönetimi Prosedürü
- Riskler Analizi ve Değerlendirme Prosedürü
- Yönetim Gözden Geçirme Prosedürü
- İç Tetkik Prosedürü
- Mobil Cihaz Yönetim Prosedürü
- Olay İhlal Yönetimi Prosedürü vb.

UYGULANABİLİRLİK BİLDİRGESİ (SOA)

7. DOKÜMAN VE KAYITLARIN OLUŞTURULMASI

HAZIRLANACAK TEKNİK POLİTİKA VE PROSEDÜRLER VE DİĞER DOKÜMANLARDAN BAZILARI

SÜREÇLER

- Süreç Haritası
- Hukuk Süreci
- BGYS Süreci vb.

TALİMATLAR

- Bilgi Sınıflandırma ve Etiketleme Talimatı
- Kurumsal İletişim Talimatı
- Arşivleme Talimatı vb.

PLANLAR

- İş Sürekliliği Planı
- İç Tetkik Planı
- Eğitim Planı vb.

7. DOKÜMAN VE KAYITLARIN OLUŞTURULMASI

HAZIRLANACAK TEKNİK POLİTİKA VE PROSEDÜRLER VE DİĞER DOKÜMANLARDAN BAZILARI

TABLOLAR

- Varlık Envanteri Tablosu
- Risk Değerlendirme ve Risk İşleme Tablosu
- Bağımlılıklar Tablosu vb.

GÖREV TANIMLARI

- Görev Tanımları ve Sorumlulukların Tahsisi
- Proje Yöneticisi
- Bilgi İşlem Müdürü vb

LİSTELER

- Ana Doküman Listesi
- Erişim Yetki Matrisi
- Dış Kaynaklı Doküman Listesi vb.

7. DOKÜMAN VE KAYITLARIN OLUŞTURULMASI

HAZIRLANACAK TEKNİK POLİTİKA VE PROSEDÜRLER VE DİĞER DOKÜMANLARDAN BAZILARI

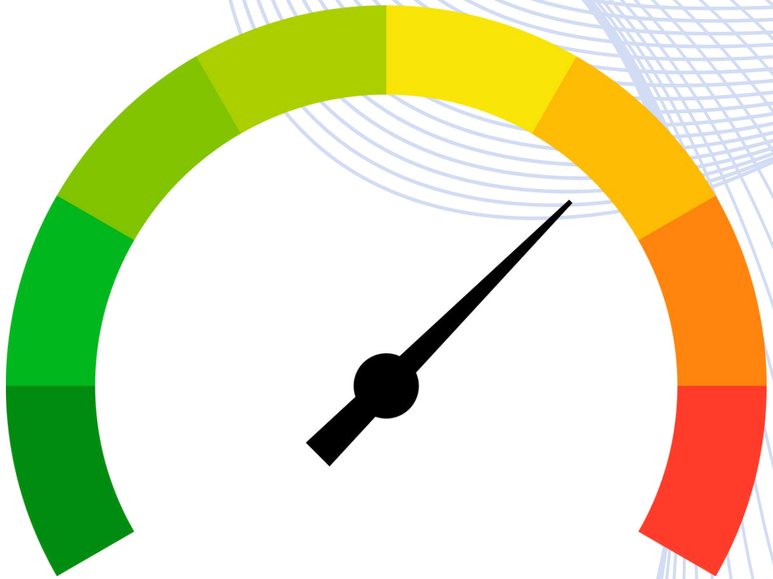
FORMLAR

- Oryantasyon Formu
- Eğitim Katılım Formu
- Eğitim Etkinlik Değerlendirme Formu vb.

8. RİSK ANALİZİ

ISO 27001 BGYS Baş Denetçi sertifikasına sahip Kıdemli Danışmanlarımız kurumunuzun ISO 27001 kapsamında Risk Analizi oluşturmak için;

- *Öncesinde BGYS Ekibine ve ilgili personellere Risk Analizi Eğitimi verirler.*
- *Sonrasında Risk Analizi uygulamasına geçilir.*
- *Risk Analizi varlık bazlı veya süreç bazlı yapılabilir.*



9-1: PERFORMANS DEĞERLENDİRME

Firmada kurulan BGYS ve ilgili süreçlerin belirlenen KPI'lar (Key Performance İnticator - Anahtar Performans Göstergesi) doğrultusunda performans değerlendirmesi yapılmaktadır

9-2: İÇ DENETİM

- *BGYS Sisteminin tam olarak kurulup işletildiğini anlaşılabilmesi için firmanın kendini öz değerlendirme yapabilmesini sağlayan İç Denetim yapılır.*

- *İç Denetim başlanmadan firma tarafından seçilecek ve danışmanlarımız tarafından onaylanan kişilere 2 Gün İç Denetçi Eğitimi verilir.*

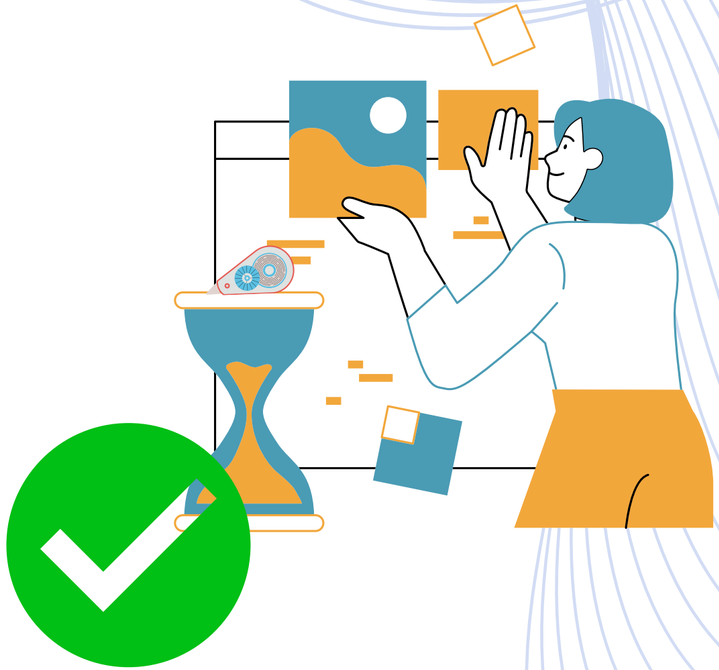
- *İlk gün ISO 19011 standart eğitimi ve ikinci günde ise Rol Play ve uygulama eğitimi sağlanır.*

9-3: YÖNETİM GÖZDEN GEÇİRME TOPLANTISI

İç Tetkik çalışması yapıldıktan Üst yönetimin, BGYS ekibi ve diğer departman yöneticilerinin katılımının olduğu ve BGYS için önemli tüm kararların alındığı toplantıdır.

**Yılda en az 1 defa yapılmalıdır.*

10: DÜZELTİCİ VE İYİLEŞTİRİCİ FAALİYETLER



İç Tetkik, Risk Analizi, ihlal olayı gibi nedenlerden veya denetimlerde görülen uygunsuzlukların kapatılması için gerekli görülen ve kayıt altına alınan faaliyetlerdir.

NESİL

ISO 27001 BGYS EK A MADDELERİ

- *ISO 27001:2013 BGYS Standart maddelerinin yanında sistem için önemli çok olan Ek-A kılavuzu bulunmaktadır.*

- *Bu kılavuzun teknik detayları ISO 27002 kılavuz standardında detaylandırılmıştır.*

- *Hem Ek-A hem de ISO 27002 ile ilgili gerekli dokümantasyon ve uygulamalar sürecinize tarafımızca destek verilmektedir.*

11. BELGELENDİRME BAŞVURUSU

Kuruluş içinde BGYS yapısının tam olarak kurulup işletildiğine sağlandıktan sonra (sistem kurulduktan en az 2 ay sonra) Belgelendirme sürecine girmek için alternatif firmalara Belgelendirme Başvurusu yapılabilir.

Bu belge "NESİL GRUP" kurumuna ait"GİZLİ" gizlilik derecesine sahip bilgiler içermektedir. Dökümanı hazırlayan kurum ve "NESİL GRUP TEKNOLOJİ TİC.A.Ş." yetkilileri dışında bu belgenin üçüncü kişilerce depolanması, kopyalanması ve dağıtımı kesinlikle YASAKTIR. Bahse konu ihlalleri gerçekleştirdiği tespit edilen yetkisiz kişi ve kurumlar hakkında yasal işlem başlatılacağını önemle duyururuz.

NESİL

TEŞEKKÜRLER

www.nesilteknoloji.com