



TÜRK KALİTE VE SERTİFİKASYON AKADEMİSİ

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ
DENETÇİ EĞİTİM KURSU ÇİN TQNet KRTEKLERİ

ISO 27001 B LG GÜVENL İ YÖNET M S STEM DENETÇ E T M KURSU Ç N TQNet KR TERLER

SAYFA 2/11 TQNet.LT.033/REV00

1. Genel

1.1 Bilgi Güvenli i Yönetim Sistemleri Denetçi E itim Kursu için TQNet Kriterleri, Bilgi Güvenli i Yönetim Sistemi denetçi e itim kursu düzenlemek isteyen TQNet onaylı e itim kurulu ları için hazırlanmı tır. TQNet onaylı e itim kurulu ları kurs içeri inin gereksinimlerini ve Bilgi Güvenli i Yönetim Sistemi 27001 serisi denetçi e itim kursunun yapısını belirler. TQNet; bu kriterlere kar ı uyumlu bir e itim kursunu de erlendirerek onaylamaktadır. Onaylanan her farklı yönetim sistemi kursu için e itim kurulu una kurs numarası verilir.

2. TANITIM

2.1 TQNet, ISO 27001 Serisi denetçi e itim kurslarını onaylamaktadır.

2.2 E itim kursunun öncelikli hedefi ö rencilere, ISO 27001 standardını ve Bilgi Güvenli i Yönetim Sistemlerini ulusal ve uluslararası normlarda ö retmektir.

3. Ö RENME HEDEFLER

3.1 Kursu ba arılı bir biçimde tamamlayan bir ö renci, bu bölüm içinde geçen ö renme hedeflerinin kar ılandı nını gösterebilir.

3.2 Genel

3.2.1 Kursun amacı, ö rencileri ISO 27001 standardına dayalı ISO 19011 ile uyumlu Bilgi Güvenli i Yönetim Sistemlerini gerçeğe tirmek için gerekli bilgi ve beceriler ile donatmaktır.

3.3 Standartlar

3.3.1 Kursu ba arılı ile tamamlayan bir ö renci:

- Bir bilgi güvenlik yönetim sisteminin amacını ve ISO 27001' de tanımlanan Bilgi Güvenlik Yönetim Sistemi süreçlerini (kurulum, uygulama, i letme, gözleme, tekrarlama ve geli tirme) açıklayabilecek
- ISO 17799, ISO 13335-1:2004, ISO 13335-3:1998, ISO 13335-4:2000, ISO 18044:2004 ve ISO 19001 standartlarının amacını, içeri ini, kendi aralarındaki ili kileri ve bir Bilgi Güvenlik Yönetim Sistemi ile uyumlu olan denetim kapsamını açıklayabilecek
- Bilgi Güvenlik Yönetim Sistemlerinin amacını ve ticari yararlarını açıklayabilecek
- Bilgi Güvenlik Yönetim Sisteminde süreç yakla ımını tanımlayabilecek
- Risk de erlendirmesini, risk kar ısında izlenebilecek süreçleri ve bu süreçlere nelerin dahil oldu unu ayrıntılı olarak tanımlayabilecek. Bu süreçler içerisindeki;



ISO 27001 B LG GÜVENL İ YÖNET M S STEM DENETÇ E T M KURSU Ç N TQNet KR TERLER

SAYFA 3/11 TQNet.LT.033/REV00

- Bilgi Güvenli i Yönetim Sistemi kapsamını ve prosedürleri
- Risk de erlendirme sürecini
- Risk kar ısındaki tutumun planı ve seçenekleri
- Kontrol sisteminin seçimi ve uygulama yollarıyla riskin azaltılmasını
- Bir kurumun ticari faaliyetleri ve buna ba lı olan riskler ile ili kili uygulanabilirlik ifadesini

açıklayabilecek.

- f. süreklili i ve güvenli i sa lamada kullanılan metotları ve önlemlerini açıklayabilecek
- g. ISO 17799 standardının amacı ve içeri ini ve bu standardın ISO 27001 ili kisini açıklayabilecek
- h. ISO 17799 standardına ba lı olan ISO 27001' in EK A' da tanımlanan kontrol hedeflerini açıklayabilecek
- i. ISO 13335 bölüm 1-2'in ISO 27001' de oynadı ı rolün amacını ve içeri ini açıklayabilecek
- j. Bilgi Güvenli i Yönetim Sistemi terminolojisine ve tanımlarına ba lı olan ISO 27001 ile ilgili Kalite Yönetim Sistemleri içeriklerini ve terminolojisini açıklayabilecek
- k. Bilgi Güvenli i Yönetim Sistemi proseslerine uygulanan PUKÖ modelini açıklayabilecek
- l. ISO 27001 gereksinimlerinin ortaya konulması için gerekli olan denetçi yeterlili ini tanımlayabilecek
- m. Kural, bilgi güvenli i risk de erlendirmesinin sonuçları, hedef ve amaçlar, sorumluluklar, programlar, prosedürler, performans bilgileri ve güvenlik tekrarları arasındaki ba lantıları açıklayabilecek
- n. Güvenlik ile alakalı tehditlerin analiz edilmesini ve bu analizlerin uygunlu u ile kurum/kurulu un çalı masına uygunlu unu tanımlayabilecek
- o. Bilgi tabanlı bir tehdit ya da darbenin önemli olarak tanımlanmasını ve bu tehdidin Bilgi Güvenli i Yönetim Sistemi içerisinde nasıl ele alınaca ını tanımlayabilecek
- h. Yasal uyumluluk ve ISO standartlarındaki uyumluluk arasındaki farkı, denetimin yürütülmesi esnasındaki önemini belirleyebilecek
- j. Girdiler, çıktılar, kontroller ve kaynaklar ile ilgili süreç bazlı aktiviteler kavramını açıklayabilecektir.

3.4 Denetim Süreci ve Sorumluluklar

3.4.1 Kursu ba arı ile tamamlayan bir ö renci:

- a. Denetçi sertifika kurumlarını, e itim kursu belgelendirme kurumlarını ve TQNet fonksiyonlarını tanımlayabilecek
- b. Bilgi Güvenli i Yönetim Sistemi organizasyonun sertifikalandırma sürecini belirleyecek
- c. Denetleme süreçlerine uygulanabilir olan u anki ISO 19011 versiyonunun ihtiyaçlarını belirleyebilecek
- d. 1., 2. ve 3. taraf denetim grupların fonksiyonlarını, benzerliklerini ve farklarını, denetçinin, denetlenenin ve bu aktivitedeki denetçi mü terilerin sorumluluklarını ve de i en rollerini tasvir edebilecek
- e. Denetim sürecinin tüm safhaları esnasındaki güvenilirlik ihtiyacını açıklayabilecek
- f. Denetçilerin yerel mü terilere duyarlı olmaları için gerekli ihtiyaçları, sa lık ve güvenlik söz konusu oldu unda denetlenenin tüzük ve kuralına uyaca ı ihtiyacını açıklayabilecek
- g. Denetim süreci esnasındaki denetçi ve denetim grup lideri sorumluluk ve rollerini alabilecek ve açıklayabilecek

3.5 Denetim Planlama

3.5.1 Kursu ba arı ile tamamlayan bir ö renci:

- a. Denetimin tüm yönlerini, belge gözden geçirmesi dahil, ISO 19011 ile uyumlu bir biçimde planlayabilecek ve organize edebilecek
- b. Ön denetim ziyaretlerinin amacını ve bu gibi ziyaretlerin ihtiyacını nasıl de erlendirece ini açıklayabilecek
- c. Süreyi yararlı bir biçimde planlama için gerekli ön denetim bilgilerine ve bir denetim için gerekli kaynaklara karar verebilecek
- d. Süreç analizine dayalı kontrol listeleri ve Bilgi Güvenli i Yönetim Sistemi' nin denetlenmesi ve bir denetim esnasında ISO 27001 için gerekli ihtiyaçlar için kontrol listelerini yapabilecek
- e. Denetleme anında kullanılan kontrol listelerinin yararları ve risklerini tanımlayabilecektir.

3.6 Denetlemeyi Gerçekle tirme

3.6.1 Kursu ba arı ile tamamlayan bir ö renci:

- a. ISO 19011 ile uyumlu bir denetleme sürecinin tüm yönlerini i letebilecek
- b. Denetlemenin açılı ve kapanı toplantılarını yönetebilecek ve ISO 19011 ile uyumlu olan bir denetleme esnasındaki denetlenen ki i için yapılan toplantıların amacını anlayabilecek
- c. Etkili ki iler arası becerileri gösterebilecek ve dinleme ve sorma kabiliyetinin dahil oldu u teknikleri görü ebilecek
- d. Süreç esnasında denetim kriterlerine uygun olan ve olmayan kanıtları sa layabilmek için yeterli notları alabilecekler
- e. Denetleme anında yapılan örneklendirmenin risklerini ve yararlarını açıklayabilecek; ve denetleme anındaki kanıtları toplayabilecek ve analiz edebilecek, belirli standarttaki uygun denetleme kanıtlarını, Bilgi Güvenli i Yönetim Sistemini anlatabilecek ve toplanılan kanıtı objektif bir biçimde gözden geçirebilecektir.

3.7 Raporlama ve Denetleme Takibi

3.7.1 Kursu ba arı ile tamamlayan bir ö renci:

- a. Bir denetlemenin sonucunu özetleyecek, kaydedecek, sunacak ve elde edilen denetleme kanıtlarına dayanan açık, az ve öz raporlar üretebilme kabiliyetini gösterebilecek
- b. Bir denetleme esnasında elde edilen bulguları de erlendirebilecek ve denetleme kriterlerine uygun raporlar hazırlayabilecek
- c. Denetleme anındaki bulguları de erlendirebilecek ve onları denetleme programına (örne in: minör, majör, gözlem) uygun bir biçimde derecelendirebilecek
- d. Denetleme esnasındaki gereksiz kayıtlara kar ılıklı olması için denetlenen tarafından hazırlanan do ru ve önleyici önerileri de erlendirebilecek
- e. Yapılan do ru hareketlerin etkisini ve uygulanmasını de erlendirebilecek
- f. Yapılan önleyici hareketlerin etkisini ve uygulanmasını de erlendirebilecek; ve do ru önleyici hareketleri ayırt edebilecek



ISO 27001 B LG GÜVENL YÖNET M S STEM DENETÇ E T M KURSU Ç N TQNet KR TERLER

SAYFA 6/11 TQNet.LT.033/REV00

- g. Denetleme esnasında elde edilen denetleme kanıtlarına dayanan, sertifikalandırma yönetim sisteminin kabul edilebilirliği üzerine tavsiyeler yapabilecek
- h. Denetçi ve denetlenenin, doğrulama sürecinde tüm safhalarındaki sorumluluklarını ve rollerini tasvir edebilecek
- i. Devam eden denetimlerin amacını açıklayabilecektir.

4. KURS ÇER

4.1 Kursun başında, kurs sağlayıcısı öğrencilere kurs formatı, öğrenci sorumlulukları, öğrencilerin nasıl değerlendirileceği ve temel değerlendirme çitleri hakkında bir bilgi vermelidir.

4.2 Kurs:

- a. Öğrenme hedefleri altındaki tüm unsurları
- b. Gereksinimler, denetleme alımları veya yaklaşımları ve uygun ISO 27001 uygulamasını kapsamalıdır.

5. KURSUN YAPISI ve E T M YÖNTEMLER

5.1 Süre

5.1.1 Direk etime, grup ve birey aktivitelerine ayrılan toplam kurs süresi en az (40) saat olmalıdır.

5.1.2 TQNet ve/veya başka bir onay kurulu u tarafından da onaylanmış; kurs sağlayıcısı kurs için en az 36 saatlik bir kurs süresi sağlamalıdır.

5.1.2.1 (36) saatlik kursa devam eden bir öğrenci aşağıda belirtilenleri uygulayarak ilk bilgilerini gösterebilir.

- a. ISO 27001:2006 u anki versiyonunun belirli gereksinimlerini.
- b. ISO 17799, ISO 13335-1:2004, ISO 13335-3:1998, ISO 13335-4:2000, ISO 18044:2004 ve ISO 19011 kar ıla tırılması.
- c. ISO 27001' de kullanılan terimlerin tanımı (Örne in: bütünlük, risk, varlık, kullanılabilirlik ...)

5.1.2.2 Kurs sağlayıcısı sınav ve değerlendirme sürecine sahip olmalıdır.

5.1.2.3 (36) saatlik eğitim kurslarında, öğrenme hedefleri kurstan kaldırılmamalıdır.

5.1.3 E er kurs tercümanlar tarafından verilirse; öğrenme hedeflerini kar ılamak amacıyla zaman arttırılabilir.

5.1.4 Sınava, yeme e, aralara ve diğer boş zamana ayrılan süre hesaplanmış kurs süresine dahil değildir.



ISO 27001 B LG GÜVENL İ YÖNET M S STEM DENETÇ E T M KURSU Ç N TQNet KR TERLER

SAYFA 7/11 TQNet.LT.033/REV00

5.1.5 Belgelendirme kurumu aksinin yapılmasını istemedikçe, kurs birbirini takip eden (5) gün süresince yapılmalıdır.

5.2 E itim Yöntemleri

5.2.1 E itim kursları ö renciler ile e itmenlerin fazla etkile imde bulunması amacı ile dizayn edilmelidir. E itim yöntemleri, kurs esnasında ö rencileri derse ba layıcı bir biçimde olmalıdır.

5.2.2 E itim kursu hem bilgi bazlı bölümlerden hem de beceri bazlı bölümlerden olu malı ve her ö renciye kalite sistem denetleme alı tırmaları uygulanmalıdır.

5.2.3 Bilgi bazlı oturumlar e itmen merkezli olabilir, fakat ö rencilerle bazen etkile imde bulunulmalı ve gerekti inde ö rencilerin anlamasını test etmelidir.

5.2.4 E itmenler, beceri bazlı oturumları senaryo denetimler ile destekleyebilir.

5.2.5 Ö rencinin ö renme hedeflerindeki ba arısını uzatmak ve yeterli geri bildirim sa lamak için gerekli olan yöntemler kursa dahil edilebilir.

5.2.6 Her ö rencinin beceri bazlı aktivite alı tırmalarına katılması gerekir: seminer, durum çalı maları, denetçi rolü oynama veya gerçek kalite sistem denetim durumları. En azından kursun (%50)' si bu gibi bu gibi aktiviteler için kullanılmalıdır.

5.2.7 Ö renciler gerçek Bilgi Güvenli i Yönetim Sistemi denetim durumlarına katıldıklarında, Bilgi Güvenli i Yönetim Sistemi denetimlerinde geçen zamanın üçte ikisi toplam kurs süresi üstüne sayılır. Denetim safhasındaki geçi ve gecikme zamanı sayılmaz.

5.2.8 E itmenler zamana, kursun içeri ine, standart ihtiyaçlara, e itmen yönetimine ve di er gereksinimlere dikkat ederek, kursu etkili bir biçimde yönetebildiklerini göstermelilerdir.

5.2.9 E itimle direk ilgili video gibi araçlar e itmenler tarafından ilave olarak kullanılabilirler. Bunlar ticari e itim videoları veya ö rencilerin kurs anındaki performanslarını gösteren ve kaydeden videolar olabilir.

Toplam kurs süresinin (3) saatten fazlası bu gibi pasif, etkile imde bulunulmayan e itim araçlarına ayrılmamalıdır.

5.3 Sınıf Ölçüsü ve Devamlılık

5.3.1 Bir sınıftaki öğrenci sayısı (20)' den fazla, (4)' ten az olmamalıdır.

5.3.2 Nadir ve harici durumlarda; (4)' ten az ve (20)' den fazla olan sınıflar, bölüm 7 ile uygun olarak düzenlenebilir.

5.3.3 Öğrencilerin tüm kurs süresince devamlılıkları zorunludur.

5.4 E itmen Sayısı

5.4.1 (11) veya daha fazla öğrenci bulunan her sınıf (2) e itmen tarafından yönetilmelidir. Belirli konular veya aktiviteler için ilave insan kaynakları ve e itmenler kullanılabilir.

5.4.2 Öğrenci sayısı (4) ile (10) arası ise kurs (1) e itmen tarafından yönetilebilir.

5.4.3 Belirli aktiviteler (örneğin: yazılı sınavlar) ne e itim ne de de erlendirme gerektirirler ve açıklama tavsiye veya izah için e itmenler gerektirmezler. Sadece (1) e itmenin olması yeterlidir.

5.5 Kurs Materyalleri

5.5.1 Her öğrenciye e itim programı için gerekli olan tüm kurs notları ile verilmelidir.

5.5.2 Kurs notları; organizasyon yapısı ve içeri i hakkında bilgi vermelidir.

5.5.3 Kurs notları seti, TQNet onaylı kurs sa layıcısını belirtmelidir. (Örne in: kapak sayfası)

5.5.4 Kurs notları her bir oturumu kapsamalı ve öğrenme hedeflerinin tüm önemli noktalarını kapsamalıdır.

5.5.5 Kurs notlarına; örnek belgeler, notlar ve raporlar dahil edilebilir.

5.5.6 Kurs notları kurs esnasınca ve kurstan sonra di er sınavlarda kullanılmamak üzere tipik sınav sorularından oluşmalıdır.

5.5.7 Her öğrenci uan ki ISO 27001 versiyonunun bir kopyasına sahip olmalıdır. E er standart kurs notlarının bir parçası olarak tedarik edilmediyse, her öğrencinin kursa bir kopyasını getirmeleri gerekir.

ISO 27001 B LG GÜVENL YÖNET M S STEM DENETÇ E T M KURSU Ç N TQNet KR TERLER

SAYFA 9/11 TQNet.LT.033/REV00

6. Ö RENC LER N DE ERLEND R LMES

6.1 Ö rencinin kursu ba arı ile tamamlayabilmesi için birbirini takip eden iki madde do rultusunda de erlendirilmelidir.

- a. Ö rencilerin bölüm 3'te detaylıca anlatılan ö renme hedeflerindeki ba arısının e itmenler tarafından sürekli de erlendirilmesi
- b. Ö rencilerin denetleme prensiplerini uygulayabilme yetene ini test eden yazılı sınavlar ve ISO 27001 gereksinim alı tırmaları.

6.2 Sürekli De erlendirme

6.2.1 Sürekli de erlendirme kaydedilmelidir. Bu kayıtlar;

- a. Dahil edilen ve bununla sınırlandırılmayan ö renme hedefleri ba arısını
- b. Kursa devamlılık ve dakikli ini içermelidir.

6.2.2 Her ö rencinin performansı, e itmen(ler) tarafından her günün sonunda yeniden gözlemlenmelidir. Günlük derecelendirme her ö renci için yapılmalı ve her iki e itmeninde de erlendirmesini yansıtmalıdır.

6.2.3 E itmenler ö renme hedeflerini ba armakta zorluk çeken ve kurs aktivitelerinde yeterli performans gösteremeyen ö rencileri tanımlamalıdır. Bu ö rencilerle özel olarak ve zamanında görü ülmeli, geli im için fırsat tanınmalıdır.

6.2.4 Sürekli de erlendirme de ba arısız olan ö renci ba arıyla bitirme sertifikasını almayı hak etmeden önce di er bir e itim kursunu ba arı ile bitirmelidir.

6.3 Yazılı Sınav

6.3.1 Yazılı sınav, ö rencilerin denetleme sürecini anlayabilmelerini, ISO 27001 uygulamasını ve kendi de erlendirmelerini yazılı bir ifade biçimiyle sa lama kabiliyetlerini de erlendirebilecektir.

6.3.2 Sınav ba arılı bir ö rencinin (ö renme hedefleri ba arısını gösteren) iki saat içinde en az %70' lik bir notla ba arılı olabilmesine göre dizayn edilmelidir.

6.3.3 Sınav için gerekli süre (2) saat olmalıdır. Süre limitine dikkat edilebilir.

6.3.4 Sınav farklı bir dilde yapılıyor ise ekstra 30 dakika daha verebilir. Ö renci uygun olan bir sözlük kullanabilir. Böyle bir izin kurs sınavlarının kayıtlarında belirtilmelidir.

6.3.5 E itmen(ler) veya gözetmen(ler), sınavı verilen süre içerisinde bitiremeyecek derecede belli yetersizli i olan ö rencilere ekstra 30 dakika verebilir. Böyle bir izin nedeni ile belirtilerek, kurs sınavlarının kayıtlarında belirtilmelidir.



ISO 27001 B LG GÜVENL YÖNET M S STEM DENETÇ E T M KURSU Ç N TQNet KR TERLER

SAYFA 10/11 TQNet.LT.033/REV00

6.3.6 Sınavın en az %75' lik kısmı, ö rencilerin denetleme senaryolarını analiz edebilme yetene ini ve denetleme anında ISO 27001 standardını nasıl uygulayabilece ini anlaması kabiliyetini test eden yazılı cevaplara dayanmalıdır.

6.3.7 Geri kalan kısım çoktan seçmeli, do ru/yanlı veya kısa cevap gerektiren sorulardan oluşabilir.

6.3.8 Minimum geçme notu %70 olmalıdır.

6.3.9 Sınav esnasında izin verilen tek referans kayna ı standart 27001'in bir kopyası, kurs sa layıcısının kurs notları, kurs esnasında ö renci tarafından alınan ki sel notlardır.

6.3.10 Yetkili ki i veya sınavın kurs sa layıcısı; kurs sonunda ba arılı olamayan ö rencilere uygulayaca ı yöntemi, e itim kursu sonunda veya kursun bitiminden en fazla (6) aya kadar bildirmelidir.

6.3.11 Sınav sorularının kopyalarının (örnek sınav ka ıdı dı nda kalanlar), sınav ka ıtları, çözümler ve tamamlanmı sınav ka ıtları her hangi bir sebepten dolayı ö renciye veya ba ka bir ki iye (yetkili ki i hariç) verilmemelidir.

6.3.12 E itim programı sa layıcıları, mümkünse bu sunumların daha önceden verilmedi ini veya önceden aynı sunumda görevlendirilmı yetkilinin yine aynı sunumda kullanılacak olan sınav ka ıdından haberdar olmadı ndan emin olunmalıdır.

6.4 Derecelendirme: Geçti/Kaldı Kararları

6.4.1 Her sınav ka ıdı bir e itmen tarafından derecelendirilmelidir. Di er bir e itmen her bölümdeki not da ılımını ilave olarak kontrol edebilir ve tüm sınav ka ıtlarını % 60 ile %75 notları arasında yeniden derecelendirebilir.

6.4.2 Kurs sa layıcısı derecelendirme ve final derecesinde ortaya çıkan herhangi farklılıkları çözebilecek yetkilere sahip olmalıdır.

6.4.3 E er kurs tercümanlar tarafından verilir ise, ö rencinin yazılı sınav cevaplarını çeviren tercümanlar kurs sa layıcısı tarafından güvenilen, tarafsız ve çevirileri do ru olan ki ilerden seçilmelidir.

6.5 Tekrar Sınavı

6.5.1 Yazılı sınavda ba arısız olan fakat sürekli de erlendirmeyi geçen bir ö renci kursun son günüyle beraber (12) ay içinde tekrar sınav hakkı kazanır.

6.5.2 Tekrar sınavı ö rencinin ba arısız oldu u sınavı idare eden, aynı kurs sa layıcısı tarafından yönetilir.



ISO 27001 B LG GÜVENLİK YÖNETİM SİSTEM DENETÇİ EĞİTİM KURSU Ç N TQNet KR TERLER

SAYFA 11/11 TQNet.LT.033/REV00

6.5.3 Yetkili ki i onay verir ise, farklı bir ki i sınavı yönetebilir. Bu yetkili ki inin, sınavın yukarıdaki 6.3 bölümündeki gereksinimler do rultusunda yönetilmesini garanti etti inde gerçekleşle tirilebilir.

6.5.4 Tekrar sınavı için farklı bir sınav ka ıdı kullanılabilir.

6.5.5 Tekrar sınavı, kurs sa layıcının prosedürlerinde belirtildi i gibi yetkili bir gözetmenin e li inde gerçekleşle melidir.

6.5.6 Tekrar sınavında da ba arısız olan bir ö renci, di er sınavlara girme hakkı kazanmak için tüm e itim kursunu tekrar almalıdır.

7. DE İKENLER

7.1 Kurs sa layıcısı bu kriterlerde herhangi bir de i iklik yapmak istedi inde de i ikli i TQNet' e bildirmek zorundadır.

7.2 İlave materyaller kursa dahil edildi inde, dahil edilen ilave materyal ilave kurs zamanında sunulmalıdır .