Meslek	**BİLGİ GÜVENLİK DENETMENİ**
Seviye	**7**[I]
Referans Kodu	**13UMS0292-7**
Standardı Hazırlayan Kuruluş	**İstanbul Ticaret Odası Koordinasyonunda BGD Bilgi Güvenliği Derneği ve TBGD Türkiye Bilişim Güvenliği Derneği**
Standardı Doğrulayan Sektör Komitesi	**MYK Bilişim Teknolojileri Sektör Komitesi**
MYK Yönetim Kurulu Onay Tarih / Sayı	**30.01.2013 Tarih ve 2013/08 Sayılı Karar**
Resmî Gazete Tarih/Sayı	**26/2/2013 - 28571 (Mükerrer)**
Revizyon No	**00**

[I] Mesleğin yeterlilik seviyesi, sekizli (8) seviye matrisinde seviye yedi (7) olarak belirlenmiştir.

TERİMLER, SİMGELER VE KISALTMALAR

ACİL DURUM: Hemen eylem veya önlem gerektiren, daha önceden kestirilemeyen koşullar ya da bu koşulların yarattıkları durumu,

BİLGİ GÜVENLİĞİ: Bilginin yetki dışı bir başka kişiye aktarılması, değiştirilmesi, tahrif edilmesi, kurcalanması ya da açığa vurulması tehlikelerine karşı korunmasını, bilginin kime ait olduğunun belirlenmesi, bütünlüğünün korunması ve kullanılabilirliğinin sağlanması aşamalarını,

BİLGİ VARLIĞI DÖKÜMÜ: Sistemde muhafaza edilen, işlenen ve iletişime konu olan, önem derecesine göre sınıflandırılmış ve sorumlusu belirtilmiş sayısal varlıkları,

BİLGİYE ERİŞİM SÜRECİ: Kullanıcıların ihtiyaçları olduğu anda güvenlik sistemdeki bilgilerini edinme süresini,

BİLİŞİM GÜVENLİĞİ YÖNETİCİSİ: Bilişim güvenliğine ilişkin bütün önlemleri yöneten ve/veya gerçekleştiren kişiyi,

BİLİŞİM GÜVENLİĞİ: Bilgi ve iletişim sistemlerinin bilgi güvenliğine yönelik tehlikelerine karşı korunması yöntemlerini ve disiplinini,

DONANIM: Ağ, bilgisayar veya çevre birimlerinin elektronik, elektromekanik ve mekanik aksamlardan oluşan tüm aktif cihazları,

ERİŞİM YETKİSİ: Daha önce kendisi için tanımlanmış erişim yetkileri dâhilinde kimliğini tanıtan kişiye verilere erişme ve üzerinde işlemler yapma yetkisinin sistem tarafından verilmesini,

FELAKET: Kurumun bilgi işlem yapısının iş göremez hale gelmesini,

GÜNLÜK HAREKET (İZ, LOG): Bilgisayar ya da başka bir cihaz üzerinde daha sonra irdeleme ve yorumlar yapabilmek için olaylar hakkında zamandizinsel veriler toplamayı,

GÜRÜLTÜ: İşitme kaybına yol açan veya sağlığa zararlı olan veya başka tehlikeleri ortaya çıkaran bütün sesleri,

GÜVENLİ ERİŞİM: Bir kullanıcının bilişim kaynaklarına erişiminin güvenlik kontrolünden geçerek sağlanabilmesini,

GÜVENLİK NOKTALARI: Kurum içerisinde korunması gerekli gizlik niteliğine sahip önem ihtiva eden bölgeleri,

GÜVENLİK UNSURLARI: Sistem içerisinde ve dolaşımda bulunan bilginin güvenliğini sağlamak için konumlandırılacak dâhili ve harici tüm mekanizmalar, önlemler, insan faktörünü,

GÜVENLİK YAZILIMI: Bilgisayar veya diğer ağ ve iletişim donanımlarının güvenliğini sağlamak amacıyla geliştirilmiş koruma ve anlık denetleme, izleme, yetkilendirme, raporlama yazılımlarını,

ISCO: Uluslararası Standart Meslek Sınıflamasını,

IT: Bilgi teknolojilerini,

İSG: İş Sağlığı ve Güvenliğini,

İŞ SÜREÇLERİ YÖNETİMİ: Bir kuruluştaki bütün iş süreçlerinin, bir iş ya da bilginin evriminin otomasyona dayalı olarak gerçek zamanda izlenmesini,

KONFİGÜRASYON: Güvenlik sisteminin kurum ihtiyaçlarına yönelik düzenlenmesi ve kullanıma hazır hale getirilmesini,

OFİS ERGONOMİSİ: Ofis ekipmanları ve genel ofis çalışma ortamının çalışanların fiziksel ve zihinsel olarak rahat çalışmasına ve verimliliklerinin arttırılmasına yönelik olarak düzenlenmesini,

RİSK: Bir tehdit kaynağının, bir sistemdeki güvenlik boşluğundan yararlanarak bilişim güvenliğini sekteye uğratma olasılığını ve olası tehdidin gerçekleşmesi anında kurumun görebileceği zararları,

SIZMA (PENETRASYON) TESTİ: Sistem güvenliği mekanizmalarını sağladıktan sonra, sistem görevlileri dışındaki kişiler tarafından yapılan sistem açıklarını bularak, sisteme sızma testini,

SIZMA: Bilişim sistemine, güvenlik önlemlerini aşarak yetkisi olmadan girmeyi,

SİSTEM GÜVENLİĞİ: Kurum IT altyapısının topyekûn korunmasını,

TEHDİT: Bilginin bozulması, bilginin ifşa edilmesi, hizmet kesintisi gibi istenmeyen durumlara neden olma potansiyeli bulunan ortamları ve olayları,

TEHLİKE: İşyerinde var olan ya da dışarıdan gelebilecek, çalışanı veya işyerini etkileyebilecek, zarar veya hasar verme potansiyelini,

TERMAL KONFOR: Çalışma ortamında çalışanların büyük çoğunluğunun ısı, nem, hava akım hızı ve termal radyasyon gibi iklim şartları açısından, bedensel ve zihinsel faaliyetlerini sürdürürken belli bir rahatlık içinde bulunmasını,

TERMAL RADYASYON: İletimi için maddesel bir ortama gerek olmayan ısı türünü,

ULUSAL GÜVENLİK NORMLARI: Kurumun konumlandığı bölge ve kurumun faaliyet konusu açısından tanımlanmış en az güvenlik gerekliliklerinin tanımlarını,

ULUSAL GÜVENLİK STRATEJİLERİ: Ulusal güvenlik beklentilerine ulaşabilmek için belirlenmiş eylem planlarını,

VERİ YEDEKLEME: Donanım yapılandırma değerlerinin veya diğer veri yedeklerinin, herhangi bir sorun durumunda tekrar yüklenebilmesi için başka bir konuma kopyalanması işlemlerini,

YAZILIM ENTEGRASYONU: Kullanılmasına ihtiyaç olan programların sistem içerisinde uyumu ve gerekiyorsa iletişimini,

YAZILIM: Bilgisayar ve ağ donanımsal yapısının amaca uygun şekilde kullanılmasını sağlayan komutlar topluluğunu,

YETKİ SEVİYELENDİRİLMESİ: Sisteme dâhil olacak kullanıcıların hangi bilgiyi nereye kadar görebileceği, kullanabileceği, değiştirebileceği ve silebileceği haklarının tümünü

ifade eder.

1. GİRİŞ

Bilgi Güvenlik Denetmeni (Seviye 7) ulusal meslek standardı 5544 sayılı Mesleki Yeterlilik Kurumu (MYK) Kanunu ile anılan Kanun uyarınca çıkartılan "Ulusal Meslek Standartlarının Hazırlanması Hakkında Yönetmelik" ve "Mesleki Yeterlilik Kurumu Sektör Komitelerinin Kuruluş, Görev, Çalışma Usul ve Esasları Hakkında Yönetmelik" hükümlerine göre MYK'nın görevlendirdiği İstanbul Ticaret Odası (İTO) koordinasyonunda BGD Bilgi Güvenliği Derneği ve TBGD Türkiye Bilişim Güvenliği Derneği tarafından hazırlanmıştır.

Bilgi Güvenlik Denetmeni (Seviye 7) ulusal meslek standardı, sektördeki ilgili kurum ve kuruluşların görüşleri alınarak değerlendirilmiş, MYK Bilişim Teknolojileri Sektör Komitesi tarafından incelendikten sonra MYK Yönetim Kurulunca onaylanmıştır.

2. MESLEK TANITIMI

2.1. Meslek Tanımı

Bilgi Güvenlik Denetmeni (Seviye 7), İSG, çevre koruma, kalite kural ve yöntemleri çerçevesinde; yetkisi dâhilinde ve tanımlanmış görev talimatlarına göre; farklı sektörlerdeki işletmelerin bilgi işlem biriminde çalışan ve/veya bu hizmeti dışarıdan profesyonel olarak sağlamak üzere uzmanlaşmış; denetim planı hazırlayan, denetim faaliyetlerini gerçekleştiren, gerçekleştirdiği denetim sonuçlarını raporlayan ve bulgu takibini gerçekleştiren nitelikli kişidir.

2.2. Mesleğin Uluslararası Sınıflandırma Sistemlerindeki Yeri

ISCO 08: 2529 (Başka yerde sınıflandırılmamış veri tabanı ve bilgisayar ağları ile ilgili profesyonel meslek mensupları)

2.3. Sağlık, Güvenlik ve Çevre ile ilgili Düzenlemeler

4857 sayılı İş Kanunu
5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
6331 sayılı İş Sağlığı ve Güvenliği Kanunu
Ambalaj Atıklarının Kontrolü Yönetmeliği
Atık Yönetimi Genel Esaslarına İlişkin Yönetmelik
Binaların Yangından Korunması Hakkında Yönetmelik
Çalışanların İş Sağlığı ve Güvenliği Eğitimlerinin Usul ve Esasları Hakkında Yönetmelik
Ekranlı Araçlarla Çalışmalarda Sağlık ve Güvenlik Önlemleri Hakkında Yönetmelik
Elle Taşıma İşleri Yönetmeliği
Hazırlama, Tamamlama ve Temizleme İşleri Yönetmeliği
İşçi Sağlığı ve İş Güvenliği Tüzüğü
İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik
Tehlikeli Atıkların Kontrolü Yönetmeliği

Ayrıca; iş sağlığı ve güvenliği ve çevre ile ilgili yürürlükte olan, kanun, tüzük ve yönetmeliklere uyulması ve konu ile ilgili risk değerlendirmesi yapılması esastır.

2.4. Meslek ile İlgili Diğer Mevzuat

5070 sayılı Elektronik İmza Kanunu
5237 sayılı Türk Ceza Kanunu
5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
5809 sayılı Elektronik Haberleşme Kanunu
Elektronik Haberleşme Güvenliği Yönetmeliği
TSE/ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

Ayrıca, meslek ile ilgili yürürlükte olan kanun, tüzük, yönetmelik ve diğer mevzuata uyulması esastır.

2.5. Çalışma Ortamı ve Koşulları

Bilgi Güvenlik Denetmeni (Seviye 7), genelde kapalı alanlarda, iyi aydınlatılmış, havalandırılmış, termal konfor koşulları ve uygun gürültü düzeyinde, ofis ergonomisine uygun hazırlanmış ortamlarda ayakta veya oturarak çalışır.

2.6. Mesleğe İlişkin Diğer Gereklilikler

Mesleğe ilişkin diğer gereklilikler bulunmamaktadır.

3. MESLEK PROFİLİ

3.1. Görevler, İşlemler ve Başarım Ölçütleri

Görevler		İşlemler		Başarım Ölçütleri	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
A	İSG önlemleri almak (devamı var)	**A.1**	Risk etmenlerini azaltmak	**A.1.1**	Çalışma ortamındaki tehlikelerin belirlenmesi, risklerin değerlendirilmesi çalışmalarına katkıda bulunur.
				A.1.2	Varsa talimatlarda yer almayan, bildirilen ve belirlenen tehlike ve riskleri İSG birimine/görevlisine veya amire, önlem önerisiyle birlikte iletir.
				A.1.3	Çalışma ortamında belirlenen tehlike kaynaklarının ve risk etmenlerinin ortadan kaldırılması çalışmalarını yürütür.
		A.2	Çalışma esnasında kişisel İSG önlemleri almak	**A.2.1**	İlk yardım ve acil müdahale araçlarını gerektiğinde uygun şekilde kullanır.
				A.2.2	Bilgisayar ekranının yüksekliğini ve uzaklığını boyun ve göz sağlığına uygun şekilde konumlandırır.
				A.2.3	Ekran çözünürlüğünü, donanımsal olarak önerilen sınırlar içerisinde, rahat okunabilirliği sağlayacak şekilde ayarlar.
				A.2.4	Masa başında beden sağlığını korumaya yönelik belirtilen kurallara uygun şekilde oturur.
				A.2.5	Masa başında aralıksız oturma süresini ve mola verme aralıklarını kurallara uygun şekilde ayarlar.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
A	İSG önlemleri almak	**A.3**	Çalışılan alanlarda İSG önlemlerini almak	**A.3.1**	İSG araç ve donanımlarını, talimatlar doğrultusunda çalışmanın yapılacağı alanda konumlandırır.
				A.3.2	İşe özgü olarak talimatlarda belirtilen havalandırma, ısıtma-soğutma, aydınlatma gibi önlemlerin çalışma öncesinde uygulanmasını sağlar.
				A.3.3	Çalışma ortamındaki güvenlik ve sağlık işaret ve levhalarına uygun davranır.
				A.3.4	İşe özgü olarak varsa talimatlarda belirtilen güvenli çalışma sürelerine uyar.
		A.4	İşletmenin acil durum önlemlerini uygulamak	**A.4.1**	Acil durum ve acil tahliye tatbikatlarında yapılan plana göre, verilen görevleri uygun yöntemler kullanarak gerçekleştirir.
				A.4.2	Uygulanan işleme özel acil durum kural ve yöntemlerini uygular.
				A.4.3	Acil durumlarda çıkış veya kaçış kural ve yöntemlerini uygular.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
B	Çevre koruma önlemleri alınmasını sağlamak	**B.1**	Çevresel tehlikeleri değerlendirmek	**B.1.1**	İşlemlerin gerçekleştirileceği ortamlar ve yapılacak işlerle ilgili çevresel etkileri ve olası tehlikeleri belirler.
				B.1.2	Varsa talimatlarda yer almayan, bildirilen ve belirlenen tehlike ve riskleri ilgili birime/ görevliye veya amire, önlem önerisiyle birlikte iletir.
				B.1.3	Çalışma ortamında belirlenen çevresel tehlike kaynaklarının ve risk faktörlerinin azaltılmasına yönelik yapılan çalışmalara verilen görevlere göre katılır.
		B.2	Çevre koruma önlemlerini uygulatmak	**B.2.1**	İş süreçlerinin uygulanması sırasında oluşabilecek çevresel etkilere ve olası tehlikelere ilişkin belirlemelerine göre, işletme talimatlarına uygun şekilde önlemler alınmasını sağlar.
				B.2.2	Tedbirlere rağmen gerçekleşen zararlı sonuçların giderilmesine ilişkin acil önlemleri, işletme kural ve yöntemlerine uygun olarak uygulatır.
				B.2.3	İş süreçlerinin uygulanması sırasında oluşan atıkların, işletme talimatlarına göre bertaraf edilmesini sağlar.
				B.2.4	Çevresel olarak olumsuz etki yaratabilecek fonksiyonlarına karşı, kullanılan cihaz, donanım ve araçların güvenli ve sağlıklı çalışma tedbirlerini alır.
				B.2.5	Çalışanların iş süreçlerinde; ilgili talimatlara göre çevre koruma önlemlerine uygun davranma durumunu planlı ve plansız olarak denetler.
		B.3	İşletme kaynaklarının verimliliğini sağlamak	**B.3.1**	Kullanılan enerji, sarf malzemeleri, zaman, gibi işletme kaynaklarını, iş süreçlerinde tasarruflu ve verimli bir şekilde kullanır.
				B.3.2	İş süreçlerinde kullanılmak üzere talep edilecek elektronik malzeme, donanım ve araçların, enerji tasarrufu ve verimlilik sağlayan özelliklerde olmasını önerir.
				B.3.3	Sistem ve cihazların asgari enerji ile azami verimde çalışması amacıyla; cihaz ve sistemlerin talimatlarda belirlenen çalışma önlemlerini uygular.
				B.3.4	Çalışanların iş süreçlerinde; ilgili talimatlara göre işletme kaynaklarının verimli kullanılmasına uygun davranma durumunu planlı ve plansız olarak denetler.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
C	Kalite uygulamalarını yürütmek	**C.1**	Yapılan çalışmaların kalitesini denetim altında tutmak	**C.1.1**	İşletmenin kalite güvence kural ve yöntemlerini, işlem formlarında yer alan talimatlara göre uygular.
				C.1.2	İş süreçlerinde kullanılan cihaz ve aletleri kalite güvence kural ve yöntemlerinde tanımlanan koşullarına uygun olarak kullanır.
				C.1.3	Yapılan işlemlerin ilişkili olduğu standartlara uygunluğunu denetler.
				C.1.4	Çalışmayla alakalı kalite yönetim sistemi formlarını doldurur.
		C.2	Süreçlerin iyileştirilmesi çalışmalarını yürütmek	**C.2.1**	Çalışmalar sırasında saptadığı hata ve arızaları nedenini belirler.
				C.2.2	İşletmenin hata ve arıza gidermeyle ilgili kural ve yöntemlerinin uygulanmasını sağlar.
				C.2.3	İş süreçlerinin iyileştirilmesi ve hataları gidermeye yönelik işletme kural ve yöntemlerine uygun öneriler geliştirir.
				C.2.4	İş süreçlerinin iyileştirilmesine ve hataları gidermeye yönelik ekiplerinin yaptığı gözlemleri, geliştirdiği görüş ve önerilerini işletme kural ve yöntemlerine göre ilgili yetkiliye iletir.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
D	İş organizasyonu yapmak (devamı var)	**D.1**	İş emirlerini almak	**D.1.1**	Kendi birimi ile ilgili iş taleplerini sistemden/ilgili birimden/müşteriden alır.
				D.1.2	Eldeki araç-gereç, malzeme, iş gücü gibi kaynakları kontrol ederek talepleri değerlendirir.
				D.1.3	Tahmini iş sürelerini belirleyerek günlük, aylık, dönemsel ve yıllık olarak talepleri takvime bağlar.
				D.1.4	İş bazında takip edilebilirliği sağlamak için planlanan her iş için tanımlama ve kodlama yapar.
				D.1.5	Yapılacak işin niteliğine göre çalışma ekipleri oluşturarak sorumlu personel atamaları yapar.
				D.1.6	İş emirlerini sistem üzerinden veya bizzat sorumlu personele iletir.
				D.1.7	İhtiyaç halinde sorumlu personel ile iş emirlerine dair değerlendirmeler yapar.
		D.2	İş planlaması yapmak	**D.2.1**	Dönemlik iş takvimlerinden günü gelmiş işlemleri belirler.
				D.2.2	Kendi sorumluluğunda olan iş emirlerini tespit ederek bireysel iş planını yapar.
				D.2.3	Sorumlu çalışanlar tarafından oluşturulan iş planlarını inceleyerek onaylar.
				D.2.4	İş planlarını gerektiğinde, çalışanlarını yönlendirerek değişen koşullara göre revize eder.

GÖREVLER		İŞLEMLER		BAŞARIM ÖLÇÜTLERİ	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
D	İş organizasyonu yapmak	**D.3**	Personel yönlendirmesi yapmak	**D.3.1**	Onaylanmış iş planlamasına göre ekipler/personel arasında iş dağılımı yapar.
				D.3.2	Ekibinin gerçekleştirdiği işleri denetler.
				D.3.3	İşlerin özelliklerine göre gerekli durumlarda işlere nezaret eder.
		D.4	Çalışılan alanı işe uygun olarak düzenletmek	**D.4.1**	Çalışmaların kesintisiz ve uygun şekilde sürdürülmesi için, çalışma alanını inceleyerek özelliklerini ve çalışma noktalarının kapsamını belirler.
				D.4.2	Çalışma alanının, kapsamına ve belirlenen özelliklerine göre, emniyet ve teknik olarak yapılacak işe uygun ortam koşullarına getirilmesini sağlar.
				D.4.3	Çalışanlarını da sürece dâhil ederek, iş alanının olumsuz özelliklerinin iyileştirilmesi ve standartlaştırılması faaliyetlerini yürütür.
		D.5	Yapılan çalışmaların form ve kayıtlarının tutulmasını sağlamak	**D.5.1**	İş emri, süreç, fire/hata, ölçüm gibi formların işletme formatlarına uygun olarak doldurulmasını sağlar.
				D.5.2	Kendisine bağlı ekiplerin doldurduğu formları kontrol ederek onaylar.
				D.5.3	Kontrol ve onay işlemi sonrasında formların varsa ilgili birimlere iletilmesini sağlar.
		D.6	Raporlama yapmak	**D.6.1**	Yapılan işlemlerin sonuçları hakkında işletme formatlarına uygun şekilde raporlar hazırlar.
				D.6.2	Gerçekleştirilemeyen işlemleri, nedenleri ve önerilerini işletme formatına uygun olarak bağlı olduğu yöneticiye raporlar.
				D.6.3	Tamamlanmış işlemler hakkında talep sahibi birime yazılı ve/veya sözlü bilgi verir.
				D.6.4	İşyeri çalışma kural ve yöntemlerine göre aksaklıkları varsa bağlı olduğu yöneticiye sözlü ve/veya yazılı olarak bildirir.
		D.7	Dijital arşivleme yapmak	**D.7.1**	İş süreçleri sonunda oluşan rapor, form vb. kaynak materyallerin sonraki düzeylerde teknik aktarım amacıyla işletme kural ve yöntemlerine uygun olarak arşivlenmesini sağlar.
				D.7.2	Dijital arşivin güvenlik ve koruma önlemlerinin işletme kural ve yöntemlerine göre uygulanmasını sağlar.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
E	Denetim planını hazırlamak (devamı var)	**E.1**	Denetimin kapsamını oluşturmak	**E.1.1**	Denetim ihtiyacı denetim organizasyonu tarafından belirleniyorsa denetimi planlanan sistemin risk analizini yapar.
				E.1.2	Denetim ihtiyacı denetlenen veya denetleten tarafından belirleniyorsa ihtiyacı karşılayacak denetim hedeflerini belirler.
				E.1.3	Denetim hedeflerini denetim prosedürlerine uygun şekilde dokümante eder.
				E.1.4	Denetim hedeflerine uygun denetim kapsamını altyapı, süreç ve organizasyon bazında belirleyerek dokümante eder.
				E.1.5	Denetim hedef ve kapsamını denetim hizmetini talep eden organizasyon yönetimine onaylatır.
				E.1.6	Denetim bir soruşturma niteliği içermiyorsa denetim hedef ve kapsamını denetlenecek organizasyon yönetimi ile paylaşır.
		E.2	Denetim prosedürlerini tanımlamak	**E.2.1**	Denetim hedefleri ve kapsamı ile genel kabul görmüş BT ve bilgi güvenliği kontrol çerçeve ve standartlarını (ör: CobiT, ISO27002) ilişkilendirir.
				E.2.2	Denetim hedeflerine uygun denetlenecek kontrol faaliyetlerini belirler.
				E.2.3	Belirlenen kontrol faaliyetlerine uygun denetim tekniklerini içeren mülakat, doküman inceleme, teknik testler, gözlem gibi denetim prosedürlerini hazırlar.
				E.2.4	Denetim prosedürlerini yerine getirmek için gerekli olacak yatırım veya harcama ihtiyacını belirler.
				E.2.5	Denetim prosedürlerini yerine getirmek için belirlediği yatırım veya harcama ihtiyacını bütçelendirir.
				E.2.6	Denetim prosedürlerinin denetim hedeflerine uygunluğunu kontrol eder.
				E.2.7	Denetim için gerekli araç tedariği için denetim organizasyon yönetiminin onayını alır.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
E	Denetim planını hazırlamak	**E.3**	Denetim planını oluşturmak	**E.3.1**	Denetim planını denetim prosedürlerinin gerçekleştirilebilmesi için yeterli süreyi içerecek biçimde takvimlendirir.
				E.3.2	Denetim planını denetçi ve kapsam/hedef /denetim prosedürü alanı başlıklarında hazırlar.
				E.3.3	Denetim sırasında katılımı gereken denetlenecek organizasyon birimleri ve diğer teknik denetim gereksinimleri hakkında planlama yapar.
				E.3.4	Denetim planını denetim organizasyonu yönetimine onaylatır.
				E.3.5	Denetim bir soruşturma niteliği içermiyorsa denetim planını denetlenecek organizasyon yönetimi ile paylaşarak görüş ve önerilerini alır.
				E.3.6	Denetlenecek organizasyonun önerilerini denetim açısından değerlendirerek uygun bulduklarını içerecek şekilde denetim planında değişiklikler yapar.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
F	Denetim faaliyetini gerçekleştirmek (devamı var)	**F.1**	Açılış toplantısını gerçekleştirmek	**F.1.1**	Açılış toplantısını denetlenecek organizasyon yönetimi yardımıyla tertipler.
				F.1.2	Denetim hedefleri ve kapsamını denetlenecek organizasyon yönetimi ile paylaşır.
				F.1.3	Denetim sırasında katılımı gereken denetlenecek organizasyon birimleri ve diğer teknik denetim gereksinimleri hakkında bilgilendirme yapar.
		F.2	Denetim prosedürlerini uygulamak (devamı var)	**F.2.1**	Gerçekleştirdiği denetim prosedürlerini ilgili denetim kapsamı, hedefi, faaliyetleri, denetime katılan kişi, denetim yeri ve zamanı bilgileri ile denetim kanıt referans ve bilgilerini içerecek biçimde dokümante ederek çalışma kağıtlarını oluşturur.
				F.2.2	Denetim planında belirlenen prosedürü uygulayarak bilgi güvenliği yönetim sistemi süreçlerini denetler.
				F.2.3	Denetim planında belirlenen prosedürü uygulayarak organizasyonel bilgi güvenliğini denetler.
				F.2.4	Denetim planında belirlenen prosedürü uygulayarak fiziksel ve çevresel denetimi yapar.
				F.2.5	Denetim planında belirlenen prosedürü uygulayarak ağ erişimini denetler.
				F.2.6	Denetim planında belirlenen prosedürü uygulayarak uygulama erişimini denetler.
				F.2.7	Denetim planında belirlenen prosedürü uygulayarak veri güvenliğini denetler.
				F.2.8	Denetim planında belirlenen prosedürü uygulayarak ağ cihazları yapılandırmalarını denetler.
				F.2.9	Denetim planında belirlenen prosedürü uygulayarak sistem yapılandırmalarını denetler.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
F	Denetim faaliyetini gerçekleştirmek	**F.2**	Denetim prosedürlerini uygulamak	**F.2.10**	Denetim planında belirlenen prosedürü uygulayarak bilgi teknolojileri ve bilgi güvenliği sürecini denetler.
				F.2.11	Ağ sızma testlerinin yapıldığını doğrular.
				F.2.12	Yapılan sızma testleri sonucu oluşan açıkların giderilip giderilmediğini denetler.
				F.2.13	Denetim bir soruşturma niteliğinde ise veya kontrol faaliyetine denetimi desteklemek amacıyla ihtiyaç duyuluyorsa iz kayıtlarını güvenlik olaylarının tespiti amacıyla inceler.
				F.2.14	Denetim bir soruşturma niteliğinde ise veya kontrol faaliyetlerinin denetimi desteklemek amacıyla ağ trafiğini güvenlik olaylarının tespiti amacıyla izleyerek kaydeder.
				F.2.15	Denetim bir soruşturma niteliğinde ise veya kontrol faaliyetleri denetimini desteklemek amacıyla kapsam içindeki sistem ve bilgisayarlar için adli bilişim teknikleri uygulayarak disk üzerindeki verileri inceler.
				F.2.16	Denetim kapsamı ile ilgili bilgi teknolojileri ve bilgi güvenliği sektörel ve ulusal düzenlemelerinin uygunluğunu denetler.
				F.2.17	Belirlenen diğer denetim prosedürlerini uygulayarak denetim kapsamındaki kontrol faaliyetlerini denetler.
				F.2.18	Gerçekleştirdiği tüm denetim işlemlerini ilgili çalışma kağıtları üzerine raporlar.
		F.3	Kapanış toplantısını gerçekleştirmek	**F.3.1**	Kapanış toplantısını denetlenen organizasyon yönetimi yardımıyla tertipler.
				F.3.2	Denetim bulgularını hatalı bulgu olma ihtimaline karşı denetlenen organizasyon yönetimi ile paylaşır.
				F.3.3	Varsa denetlenen organizasyon yönetimi tarafından, eksik denetim prosedürü uygulanması veya denetlenen organizasyon yönetiminin yanlış bilgilendirmesi nedeniyle, hatalı olarak belirlendiği iddia edilen bulgulara dair ek denetim prosedürü uygulayarak bulgu varlığını netleştirir.
		F.4	Denetim belgelerini arşivlemek	**F.4.1**	Gerçekleştirdiği denetime ait denetim belgelerini denetim organizasyon kurallarına uygun biçimde saklar.
				F.4.2	Denetim belgelerini denetim organizasyon kurallarına uygun güvenliklerini sağlayarak arşivler.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
G	Denetim raporlamasını yapmak	**G.1**	Denetim raporunu hazırlamak	**G.1.1**	Denetim raporunda yönetici özeti bölümünü hazırlar.
				G.1.2	Denetim raporunda denetim hedef(ler)i ve kapsamını belirtir.
				G.1.3	Denetim bulgularını raporu okuyacak hedef kitleye uygun teknik seviye ve detayda raporlar.
				G.1.4	Her bulgu için bulguya ilişkin açıklama ve ilgili riski belirtir.
				G.1.5	Denetçi bulguların önceliklerinin daha iyi anlaşılabilmesi için kritiklik seviyesini belirtir.
				G.1.6	Denetçi bulguların ortadan kaldırılabilmesi için öneride bulunur.
				G.1.7	Bulgu açıklamasında gerek duyuluyorsa çalışma kağıtlarında bulunan referanslar veya kanıtları kanıt referansları olarak verir.
		G.2	Denetim raporundaki düzeltici faaliyetler için taahhüt almak	**G.2.1**	Denetim raporunu dağıtım listesine ve bilmesi gereken prensibine uygun olarak güvenli biçimde ilgili görevlilere iletir.
				G.2.2	Denetim raporunu ihtiyaç duyuluyorsa denetlenen ve/veya denetleten organizasyon yönetimine bir toplantı ile sunar.
				G.2.3	Denetlenen ve/veya denetleten organizasyon yönetiminden her bulgu için sorumlu, düzeltici faaliyet planı ve hedeflenen tarih taahhütlerini alır.
				G.2.4	Denetlenen ve/veya denetleten organizasyon yönetiminden aldığı her bulgu için sorumlu, düzeltici faaliyet planı ve hedeflenen tarih taahhütlerini rapora veya takip listesine not eder.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
H	Bulgu takibini gerçekleştirmek	**H.1**	Bulguları izlemek	**H.1.1**	Bulgulara ilişkin denetlenen ve/veya denetleten organizasyonun verdiği taahhütler doğrultusunda takip listesi hazırlar.
				H.1.2	Bulguları hazırladığı takip listesi aracılığı ile bulgu kapatma taahhüdüne göre izler.
		H.2	İzlediği bulguların denetimini gerçekleştirmek	**H.2.1**	Denetlenen ve/veya denetleten organizasyondan takip listesindeki bulguların kapatılma durumu hakkında bilgi alır.
				H.2.2	Kapatıldığı belirtilen bulguların kritikliğine uygun olarak takip denetimi yapar.
				H.2.3	Kapatıldığı belirtilen bulguların kritikliğine uygun olarak sonraki olağan denetim kapsamında kapatılıp kapatılmadığını denetler.
				H.2.4	Takip denetim sonuçlarını denetim organizasyon yönetimine ve denetlenen organizasyon yönetimine raporlar.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
I	Mesleki gelişim faaliyetlerini yürütmek	**I.1**	Mesleki eğitimlere katılmak	**I.1.1**	Günlük deneyim ve gözlemler çerçevesinde kendisinin eğitim ihtiyaçlarını tespit eder.
				I.1.2	Tespit ettiği ihtiyaçlar çerçevesinde işverenden/ilgili birimden eğitim talebinde bulunur.
				I.1.3	Mesleki kuruluşlar tarafından ilgili konulara ilişkin düzenlenen eğitim programlarını izler.
				I.1.4	Katıldığı mesleki eğitimler hakkında ilgili birimlere geri bildirimde ve önerilerde bulunur.
		I.2	Mesleki ve teknolojik yenilikleri takip etmek	**I.2.1**	Meslek ve sektördeki yeni araç-gereç, donanım, yeni yöntem, yeni sistem gibi teknolojik gelişmeleri süreli yayınlar, internet, dergi gibi kaynaklardan güncel olarak izler.
				I.2.2	Görevleriyle ilgili mevzuat ve norm değişikliklerini işletmenin ilgili birimleri veya dış kaynakların yayınlarından izler.
				I.2.3	Edinilen bilgileri ve dokümanları elemanları ve üst yönetim ile paylaşır.
				I.2.4	Değişim ve yenilikleri iş planlamalarına ve süreçlerine yansıtır.
		I.3	Denetime yönelik teknik yetkinliğini geliştirmek	**I.3.1**	Gerçekleştireceği denetim prosedürlerinin gerektirdiği teknik yetkinliğe ilişkin eksikliklerini belirler.
				I.3.2	Belirlediği teknik yetkinlik eksikliğini teknik referansları okuyarak veya gerekli teknik eğitimleri alarak giderir.
		I.4	Personelin eğitim almasını sağlamak	**I.4.1**	Birim personelinin bilgi, beceri, mesleki tutum ve iş alışkanlıkları konularındaki eğitim ihtiyaçlarının belirlenmesini sağlar.
				I.4.2	Belirlenen eğitim ihtiyaçlarını ilgili birime iletir.
				I.4.3	Personelinin planlanan eğitimlere katılımını sağlar.
		I.5	Personelin işbaşı eğitimine iştirak etmek	**I.5.1**	Birim personeline yapılacak işlere ilişkin iş talimatlarını, bilgi ve deneyimlerini aktarır.
				I.5.2	Gerektiğinde işi uygulamalı olarak gösterir.
				I.5.3	Personeli iş sırasında gözleyerek olumsuzlukları düzeltir.

3.2. Kullanılan Araç, Gereç ve Ekipman

1. Belgegeçer ve fotokopi makinesi
2. Bilgisayar çevre birimleri (yazıcı, barkod okuyucu, tarayıcı, vb.)
3. Bilgisayar ekranı (CRT, LCD, LED)
4. Çeşitli güvenlik tarayıcı yazılımlar ve raporlama araçları
5. Depolama ortamları (CD, DVD, disket, vb.)
6. Dijital görüntüleme donanımları (webcam, fotoğraf makinesi, kamera, vb.)
7. Dönüştürücüler (DVI, HDMI, PATA, USB)
8. Güvenlik, tanımlama, sorun giderme ve veri kurtarma araçları
9. Harici depolama birimleri (flash bellek, HDD)
10. Her türlü güvenlik duvarı, ağ aktif cihazları, ağ yönetim yazılımları
11. İnternet bağlantılı bilgisayar
12. İşletim sistemleri ve ofis yazılımları
13. Kablolu ve kablosuz iletişim araçları (telefon, cep telefonu, telsiz, ses kayıt cihazı, vb.)
14. Kesintisiz güç kaynağı (UPS)
15. Kişisel koruyucu donanım
16. Ofis ve kırtasiye malzemeleri
17. Virus, casus yazılım, solucan vb, sistemi tehdit eden tehlikeleri tespit eden virüs koruma yazılımları

3.3. Bilgi ve Beceriler

1. Analitik düşünme yeteneği
2. Basit ilkyardım bilgisi
3. Bilgi güvenliği yönetim sistemi standartları ve uygulama teknikleri bilgisi
4. Bilgisayar donanımları ve çevre birimleri bilgisi
5. Çevre koruma yöntemleri ve yasal düzenlemeler bilgisi
6. Doğal kaynakların etkin kullanımı bilgisi
7. Ekip yönetim becerisi
8. Genel iş sağlığı ve güvenliği bilgisi
9. Güncel ağ teknolojileri bilgisi (DNS, TCP/IP, Workflow,vb)
10. Güvenli ağ ve internet bağlantısı kurulum bilgisi
11. Güvenlik donanım araç ve gereçleri bilgisi
12. Güvenlik duvarı kurulum ve kullanım bilgisi
13. İnternet kullanım bilgisi
14. İş organizasyonu ve planlama becerisi
15. İşletim sistemleri ve sunucu yazılımları bilgisi
16. Kimlik ve kaynak yönetimi bilgisi
17. Mesleğe ilişkin yasal düzenlemeler bilgisi
18. Mesleki matematik, terim ve yabancı dil bilgisi
19. Öğrenme ve öğrendiğini aktarabilme yeteneği
20. Programlama bilgisi
21. Savunma algoritmaları bilgisi
22. Sektöre ait ulusal ve uluslararası standartlar bilgisi
23. Teknik dokümanları okuma ve anlama bilgi ve becerisi

24. Temel çalışma mevzuatı bilgisi
25. Veri tabanı güvenliği bilgisi
26. Veri toplama, kayıt tutma ve raporlama bilgi ve becerisi
27. Yangın önleme, yangınla mücadele, acil durum ve tahliye bilgisi
28. Yazılı ve sözlü iletişim yeteneği
29. Zaman yönetimi bilgisi

3.4. Tutum ve Davranışlar

1. Acil ve stresli durumlarda soğukkanlı ve sakin olmak
2. Astlarının iş disiplinini sağlamak
3. Beraber çalıştığı kişilerle işe göre eşgüdüm sağlamak ve uyumlu hareket etmek
4. Bilgi, tecrübe ve yetkisi dâhilinde tarafsız karar vermek
5. Çalışma zamanını etkili ve verimli kullanmak
6. Çevre, kalite ve İSG mevzuatında yer alan düzenlemelere uymak
7. Değişime açık olmak ve değişen koşullara uyum sağlamak
8. Deneyimlerini çalışma arkadaşlarına aktarmak
9. Görevi ile ilgili yenilikleri takip etmek
10. İşyeri çalışma prensiplerine uymak
11. Kurumsal ve kişisel verilerin gizliliğini korumak
12. Meslek etiği ve yasal düzenlemelere uygun davranmak
13. Mesleki gelişim için araştırmaya istekli olmak
14. Programlı ve düzenli çalışmak
15. Sahip olduğu güvenlik bilgilerini amacı dışında kullanmamak
16. Süreç kalitesine özen göstermek
17. Süreçleri iyileştirici ve geliştirici önerilerde bulunmak
18. Tehlike ve risk durumları konusunda duyarlı olmak ve ilgilileri bilgilendirmek
19. Uygun (sözlü ve sözlü olmayan) iletişim becerileri sergilemek
20. Yeniliklere açık olmak ve değişen koşullara uyum sağlamak

4. ÖLÇME, DEĞERLENDİRME VE BELGELENDİRME

Bilgi Güvenlik Denetmeni (Seviye 7) meslek standardını esas alan ulusal yeterliliklere göre belgelendirme amacıyla yapılacak ölçme ve değerlendirme, gerekli şartların sağlandığı ölçme ve değerlendirme merkezlerinde yazılı ve/veya sözlü teorik ve uygulamalı olarak gerçekleştirilecektir.

Ölçme ve değerlendirme yöntemi ile uygulama esasları bu meslek standardına göre hazırlanacak ulusal yeterliliklerde detaylandırılır. Ölçme ve değerlendirme ile belgelendirmeye ilişkin işlemler Mesleki Yeterlilik, Sınav ve Belgelendirme Yönetmeliği çerçevesinde yürütülür.