ETİK HACKER

SEVİYE 5

REVİZYON NO: 00

22UY0515-5

GİRİŞ

Etik Hacker (Seviye 5) Ulusal Yeterliliği 19/10/2015 tarihli ve 29507 sayılı Resmi Gazete'de yayımlanan Ulusal Meslek Standartlarının ve Ulusal Yeterliliklerin Hazırlanması Hakkında Yönetmelik ve 27/11/2007 tarihli ve 26713 sayılı Resmi Gazete'de yayımlanan Mesleki Yeterlilik Kurumu Sektör Komitelerinin Kuruluş, Görev, Çalışma Usul ve Esasları Hakkında Yönetmelik hükümlerine göre MYK'nın görevlendirdiği Türkiye Bilişim Vakfı tarafından hazırlanmış, sektördeki ilgili kurum ve kuruluşların görüşleri alınarak değerlendirilmiş ve MYK Bilişim Teknolojileri Sektör Komitesi tarafından incelendikten sonra MYK Yönetim Kurulunca onaylanmıştır.

TERİMLER, SİMGELER VE KISALTMALAR

ACİL DURUM: İş yerinin tamamında veya bir kısmında meydana gelebilecek yangın, patlama, tehlikeli kimyasal maddelerden kaynaklanan yayılım, doğal afet gibi acil müdahale, mücadele, ilkyardım veya tahliye gerektiren olayları,

ACİL DURUM PLANI: İşyerlerinde meydana gelebilecek acil durumlarda yapılacak iş ve işlemler dahil bilgilerin ve uygulamaya yönelik eylemlerin yer aldığı planı,

AÇIK KAYNAK KODLU YAZILIM: Herkesin inceleyebileceği, değiştirebileceği ve geliştirebileceği kaynak kodlu yazılımı,

BULUT SİSTEMİ: Bilgisayar, telefon, tablet ve sunucu gibi tüm cihazlar arasında zaman ve mekan kısıtlaması olmadan veri paylaşımına olanak sağlayan, internet tabanlı bir veri depolama hizmeti,

DONANIM: Ağ, bilgisayar veya çevre birimlerinin elektronik, elektromekanik ve mekanik aksamını,

ISCO: Uluslararası Standart Meslek Sınıflandırmasını,

İSG: İş Sağlığı ve Güvenliğini

İŞ KAZASI: Kişinin çalışma hayatında 5510 sayılı kanunda, sayılı hallerden birinde meydana gelen ve sigortalıyı bedenen ya da ruhen engelli hale getiren olay,

KİŞİSEL KORUYUCU DONANIM (KKD): Çalışanı, yürütülen işten kaynaklanan, sağlık ve güvenliği etkileyen bir veya birden fazla riske karşı koruyan, çalışan tarafından giyilen, takılan veya tutulan tüm alet, araç, gereç ve cihazları,

KVKK: Kişisel Verilerin Korunması Kanununu,

RAMAK KALA OLAY: İş yerinde meydana gelen; çalışan, işyeri ya da iş ekipmanını zarara uğratma potansiyeli olduğu halde zarara uğratmayan olayı,

RİSK: Tehlikeden kaynaklanacak kayıp, yaralanma ya da başka zararlı sonuç meydana gelme ihtimalini,

RİSK DEĞERLENDİRMESİ: İş yerinde var olan ya da dışarıdan gelebilecek tehlikelerin belirlenmesi, bu tehlikelerin riske dönüşmesine yol açan faktörler ile tehlikelerden kaynaklanan risklerin analiz edilerek derecelendirilmesi ve kontrol tedbirlerinin kararlaştırılması amacıyla yapılması gereken çalışmaları,

SCADA: Endüstriyel tesise veya işletmeye ait üretim planlaması, çevre kontrol üniteleri, yardımcı işletmeler dahil tüm birimlerin otomatik kumanda ve kontrolü, izleme, veri toplama, verilerin kaydı ve saklanması işlevlerini gerçekleştirmesi için kullanılan yazılımı,

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

TELNET: Internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan genel programları,

VERİTABANI: Bir uygulama yazılımının ihtiyaç duyduğu ve / veya yazılım kullanılarak oluşturulan verilerin tümünün işlenmesi, saklanması ve raporlanmak amacı ile erişilmesi için tasarlanan birbirleri ile ilişkili tablo, indeks, kural ve betikler topluluğunu,

VoIP: Analog ses sinyalini dijital bir sinyale dönüştüren, doğrudan bir bilgisayardan, VoIP telefonundan veya diğer veri odaklı cihazlardan arama yapmanıza olanak tanıyan teknolojiyi,

YAZILIM: Bilgisayar sistemini oluşturan harici ve dâhili donanım birimlerinin yönetimini ve kullanıcıların işlerini yapmak için gerekli olan programları

ifade eder.

22UY0515-5 ETİK HACKER ULUSAL YETERLİLİĞİ

1	**YETERLİLİĞİN ADI**	Etik Hacker
2	**REFERANS KODU**	22UY0515-5
3	**SEVİYE**	5
4	**ULUSLARARASI SINIFLANDIRMADAKİ YERİ**	ISCO 08: 2519 (Başka yerde sınıflandırılmamış yazılım ve uygulama geliştiricileri ve analistleri)
5	**TÜR**	
6	**KREDİ DEĞERİ**	
7	**A) YAYIN TARİHİ**	22/06/2022
	B) REVİZYON NO	00
	C) REVİZYON TARİHİ	
8	**AMAÇ**	Bu yeterlilik Etik Hacker (Seviye 5) mesleğinin nitelikli kişiler tarafından yürütülmesi ve çalışmalarda kalitenin artırılması için; • Adayların sahip olması gereken nitelikleri, bilgi, beceri ve yetkinlikleri tanımlamak, • Adayların, geçerli ve güvenilir bir belge ile mesleki yeterliliğini kanıtlamasına olanak vermek, • Eğitim sistemine, sınav ve belgelendirme kuruluşlarına referans ve kaynak oluşturmak amacıyla hazırlanmıştır.
9	**YETERLİLİĞE KAYNAK TEŞKİL EDEN MESLEK STANDART(LAR)I**	
Etik Hacker (Seviye 5) Ulusal Meslek Standardı-22UMS0788-5		
10	**YETERLİLİK SINAVINA GİRİŞ ŞART(LAR)I**	
-		
11	**YETERLİLİĞİN YAPISI**	
11-a) Zorunlu Birimler		
22UY0515-5/A1 İş Sağlığı Güvenliği, Çevre Koruma ve Kalite Gereklilikleri 22UY0515-5/A2 Siber Güvenlik Araştırmalarını Yaparak Sızma Testleri Yürütme		
11-b) Seçmeli Birimler		
-		
11-c) Birimlerin Gruplandırılma Alternatifleri		
Yeterliliğin elde edilebilmesi için adayın birimlerin tümünden başarılı olması gerekir.		
12	**ÖLÇME VE DEĞERLENDİRME**	
Mesleki Yeterlilik Belgesini elde etmek isteyen adaylar yeterlilik birimlerinde tanımlanan teorik ve performansa dayalı sınavlara tabi tutulur. Adayların yeterlilik belgesini alabilmeleri için, yeterlilik birimlerinde tanımlanan sınavlardan başarılı olmaları gerekir. Yeterlilik birimlerindeki teorik sınavlar, her bir birim için ayrı ayrı yapılabileceği gibi birlikte de yapılabilir. Ancak her birimin değerlendirmesi bağımsız yapılmalıdır. Yeterlilik birimlerinin geçerlilik süresi birimin başarıldığı tarihten itibaren 2 yıldır. Yeterliliğin elde edilebilmesi için tüm birimlerin geçerliliğini koruyor olması gerekmektedir.		

13	DEĞERLENDİRİCİ ÖLÇÜTLERİ	
Değerlendiricilerin aşağıdaki şartlardan en az birini sağlaması gerekmektedir: • Siber güvenlik alanında öğretmen/öğretim görevlisi/eğitmen olarak en az üç (3) yıl eğitim vermiş olmak, • Lisans mezunu olmak ve siber güvenlik alanında en az üç (3) yıl deneyime sahip olmak, • Meslek yüksekokullarından mezun olmak ve siber güvenlik alanında en az beş (5) yıl deneyime sahip olmak. Yukarıdaki özelliklere sahip olan ve ölçme ve değerlendirme sürecinde görev alacak değerlendiricilere; ilgili alanda yetkilendirilmiş kuruluşlar tarafından mesleki yeterlilik sistemi, kişinin görev alacağı ulusal yeterlilik(ler), ilgili ulusal meslek standart(lar)ı, ölçme-değerlendirme ve ölçme-değerlendirmede kalite güvencesi konularında eğitim sağlanmalıdır.		
14	**BELGE GEÇERLİLİK SÜRESİ**	Belgenin geçerlilik süresi beş (5) yıldır.
15	**GÖZETİM SIKLIĞI**	-
16	**BELGE YENİLEMEDE UYGULANACAK ÖLÇME-DEĞERLENDİRME YÖNTEMİ**	Beş (5) yıllık geçerlilik süresinin sonunda belge sahibinin performansı aşağıda tanımlanan yöntemlerden en az biri kullanılarak değerlendirmeye tabi tutulur; a) 5 yıl belge geçerlilik süresi içerisinde toplamda en az bir yıl veya son altı ay boyunca ilgili alanda çalıştığını gösteren kayıtları (hizmet dökümü, referans yazısı/mektubu, sözleşme, fatura, portfolyo vb.) sunmak, b) Yeterlilik kapsamında yer alan yeterlilik birimleri için tanımlanan uygulama sınavlarına katılmak. Değerlendirme sonucu olumlu olan adayların belge geçerlilik süreleri 5 yıl daha uzatılır.
17	**MESLEKTE YATAY ve DİKEY İLERLEME YOLLARI**	Yatay İlerleme: Bulut Bilişim Analisti (Seviye 5)
18	**YETERLİLİĞİ GELİŞTİREN KURULUŞ(LAR)**	Türkiye Bilişim Vakfı
19	**YETERLİLİĞİ DOĞRULAYAN SEKTÖR KOMİTESİ**	MYK Bilişim Teknolojileri Sektör Komitesi

22UY0515-5/A1 İŞ SAĞLIĞI GÜVENLİĞİ, ÇEVRE KORUMA VE KALİTE GEREKLİLİKLERİ YETERLİLİK BİRİMİ

1	**YETERLİLİK BİRİMİ ADI**	İş Sağlığı Güvenliği, Çevre Koruma ve Kalite Gereklilikleri
2	**REFERANS KODU**	22UY0515-5/A1
3	**SEVİYE**	5
4	**KREDİ DEĞERİ**	
5	**A) YAYIN TARİHİ**	22/06/2022
	B) REVİZYON NO	00
	C) REVİZYON TARİHİ	
6	**YETERLİLİK BİRİMİNE KAYNAK TEŞKİL EDEN MESLEK STANDARDI**	
Etik Hacker (Seviye 5) Ulusal Meslek Standardı-22UMS0788-5		
7	**ÖĞRENME KAZANIMLARI**	

Öğrenme Kazanımı 1: İş sağlığı ve güvenliği önlemlerini açıklar.

Alt Öğrenme Kazanımları:
1.1: İş sağlığı ve güvenliği ile ilgili uygulaması gereken önlemleri açıklar.
1.2: Acil durum prosedürlerini açıklar.

Öğrenme Kazanımı 2: Çevre koruma, kalite ve veri güvenliği gerekliliklerini açıklar.

Alt Öğrenme Kazanımları:
2.1: Çevre koruma ile ilgili uygulaması gereken önlemleri açıklar.
2.2: İş süreçlerinde uygulaması gereken kalite gerekliliklerini açıklar.
2.3: Kişisel verilerin korunması mevzuatı gerekliliklerini açıklar.

8	**ÖLÇME VE DEĞERLENDİRME**

8 a) Teorik Sınav

Çoktan Seçmeli Sınav (T1): A1 birimine yönelik teorik sınav Ek A1-2'de yer alan "Bilgiler" kontrol listesine göre gerçekleştirilir. Teorik sınavda adaylara en az yirmi (20) soruluk 4 seçenekli çoktan seçmeli ve her biri eşit puan değerinde yazılı sınav (T1) uygulanmalıdır. Çoktan seçmeli sorularla düzenlenmiş sınavda yanlış cevaplandırılan sorulardan herhangi bir puan indirimi yapılmaz. Sınavda adaylara her soru için ortalama bir buçuk (1,5) dakika zaman verilir. Yazılı sınavda soruların en az %70'ine doğru yanıt veren aday başarılı sayılır. Sınav soruları, bu birimde teorik sınav ile ölçülmesi öngörülen tüm bilgi ifadelerini (Ek A1-2) ölçmelidir.

8 b) Performansa Dayalı Sınav

Bu birime yönelik beceri ve yetkinlik ifadeleri diğer birimin beceri ve yetkinlik kontrol listesinde tanımlanmış olup, bu kapsamda söz konusu beceri ve yetkinlik ifadelerinin ölçme ve değerlendirmesi yapılacaktır.

8 c) Ölçme ve Değerlendirmeye İlişkin Diğer Koşullar

Adayın söz konusu birimden başarılı sayılması için T1 sınavından başarılı olması gerekir. Yeterlilik

biriminin geçerlilik süresi birimin başarıldığı tarihten itibaren 2 yıldır.		
9	**YETERLİLİK BİRİMİNİ GELİŞTİREN KURUM/KURULUŞ(LAR)**	Türkiye Bilişim Vakfı
10	**YETERLİLİK BİRİMİNİ DOĞRULAYAN SEKTÖR KOMİTESİ**	MYK Bilişim Teknolojileri Sektör Komitesi

YETERLİLİK BİRİMİ EKLERİ

EK [A1]-1: Yeterlilik Biriminin Kazandırılması için Tavsiye Edilen Eğitime İlişkin Bilgiler

1. **İş sağlığı ve güvenliğine yönelik temel düzenlemeler**
   1.1. İş sağlığı ve güvenliğinde işverenlerin ve çalışanların hukuki yükümlülükleri
   1.2. Araç, gereç ve ekipmanların güvenli kullanımı ile ilgili talimat ve prosedürler ve bunları iş süreçlerine uygulama
   1.3. Çalışma ortamındaki risk ve tehlikeler
   1.4. Risk ve tehlike kavramları, türleri ve özellikleri
   1.5. Çalışma ortamındaki risk ve tehlikeleri belirleme yöntem ve teknikleri
   1.6. Çalışma ortamında bulunabilecek sağlık ve güvenlik işaretleri
2. **Acil durumlar**
   2.1. Acil durum kapsamı ve acil durum planı
   2.2. Acil durum türleri ve acil durumlarda harekât tarzı
   2.3. Acil durumda uyulması gereken kurallar
3. **Çevre koruma uygulamaları**
   3.1. Çalışma süreçlerinde ortaya çıkan atık malzemelerin tasnif ve bertarafı
   3.2. Çalışma süreçlerinde ortaya çıkan elektronik atıkların tasnif ve bertarafı
   3.3. Temel atık yönetimi
   3.4. Çevresel risk ve tehlikeler ile bunlara karşı uygulanacak önlemler
   3.5. Enerji verimliliği ve temel tasarruf uygulamaları
4. **İş süreçlerinde kalite ve veri güvenliği gereklilikleri**
   4.1. Süreçlerle ilgili takip edilmesi gereken mevzuatlar
   4.2. Çalışma süreçlerinde kalitenin sağlanmasına yönelik izlenmesi gereken prosedürler
   4.3. Tutulması gereken kayıtlar ve raporlama
   4.4. Temel kalite yönetim süreçleri
   4.5. Çalışma süreçlerinde karşılaşılması olası hatalar ve bunların giderilmesi süreci
   4.6. Kişisel ve kurumsal bilgilerin gizliliği ve güvenliği mevzuatı

EK [A1]-2: Yeterlilik Biriminin Ölçme ve Değerlendirmesinde Kullanılacak Kontrol Listesi

a) BİLGİLER

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BG.1	İş sağlığı ve güvenliği ile ilgili terimleri (iş kazası, tehlike, risk, risk değerlendirmesi ve ramak kala olay) ayırt eder.	A.1.4	1.1	T1
BG.2	İSG önlemlerini gerektiren durumlarda uygulanacak prosedürleri açıklar.	A.1.4	1.1	T1
BG.3	Çalışma süreçlerine göre temel İSG tehlike ve risklerini açıklar.	A.1.4-6	1.1	T1

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BG.4	Çalışma süreçlerindeki olası İSG tehlike ve risklerine göre uygulaması gereken önlemleri açıklar.	A.1.6	1.1	T1
BG.5	Çalışma ortamında bulunabilecek güvenlik donanımlarını sıralar.	A.1.2	1.1	T1
BG.6	Çalışma ortamında bulunabilecek güvenlik donanımlarına ilişkin talimatları açıklar.	A.1.2	1.1	T1
BG.7	Çalışma ortamında bulunabilecek sağlık ve güvenlik işaretlerini ve bunlara ilişkin talimatları açıklar.	A.1.2	1.1	T1
BG.8	Çalışma ortamında bulunabilecek sağlık ve güvenlik işaretlerine ilişkin talimatları açıklar.	A.1.2	1.1	T1
BG.9	Acil durum kapsamını ve acil durum planını açıklar.	A.2.1	1.2	T1
BG.10	Acil durumlarda uyulması gereken kuralları ve yapılması gerekenleri açıklar.	A.2.2	1.2	T1
BG.11	Çalışma süreçlerinde ortaya çıkan atık malzemelerin (kablolar ve benzeri) tasnif ve bertarafına yönelik prosedürleri açıklar.	A.3.2	2.1	T1
BG.12	Çalışma süreçlerinde ortaya çıkan elektronik atıkların tasnif ve bertarafına yönelik prosedürleri açıklar.	A.3.2	2.1	T1
BG.13	Çalışma süreçlerinde meydana gelmesi olası çevresel risk ve tehlikeleri açıklar.	A.3.1	2.1	T1
BG.14	Çevresel risk ve tehlikelere karşı uygulaması gereken önlemleri sıralar.	A.3.1	2.1	T1
BG.15	Çalışma süreçlerinde kalitenin sağlanmasına yönelik izlemesi gereken prosedürleri açıklar.	A.4.1	2.2	T1
BG.16	Çalışma süreçlerinde tutması gereken kayıtları ve raporlaması gereken işlemleri sıralar.	A.4.1	2.2	T1
BG.17	Çalışma süreçlerinde karşılaşılması olası hataları sıralar.	A.4.2	2.2	T1
BG.18	Hataların giderilmesine yönelik yöntemleri açıklar.	A.4.2	2.2	T1
BG.19	Kişisel verilerin korunması mevzuatını açıklar.	A.5.1-3	2.3	T1
BG.20	Kişisel verilerin muhafazasına ilişkin süreci açıklar.	A.5.2	2.3	T1

b) BECERİ VE YETKİNLİKLER

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
*BY.1	-	-	-	-

(*) Performans sınavında başarılması zorunlu kritik adımlar.

22UY0515-5/A2 SİBER GÜVENLİK ARAŞTIRMALARINI YAPARAK SIZMA TESTLERİ YÜRÜTME YETERLİLİK BİRİMİ

1	**YETERLİLİK BİRİMİ ADI**	Siber Güvenlik Araştırmalarını Yaparak Sızma Testleri Yürütme
2	**REFERANS KODU**	22UY0515-5/A2
3	**SEVİYE**	5
4	**KREDİ DEĞERİ**	
5	**A) YAYIN TARİHİ**	22/06/2022
	B) REVİZYON NO	00
	C) REVİZYON TARİHİ	
6	**YETERLİLİK BİRİMİNE KAYNAK TEŞKİL EDEN MESLEK STANDARDI**	
Etik Hacker (Seviye 5) Ulusal Meslek Standardı-22UMS0788-5		
7	**ÖĞRENME KAZANIMLARI**	

Öğrenme Kazanımı 1: İSG, çevre koruma ve kalite gereklilikleri ile ilgili önlemleri uygular.

Alt Öğrenme Kazanımları:
1.1: Çalışmalarında İSG ile ilgili gereklilikleri uygular.
1.2: Çalışmalarında çevre ile ilgili gereklilikleri uygular.
1.3: Çalışmalarında kalite ile ilgili gereklilikleri uygular.
1.4: Çalışmalarında kişisel verilerin korunması gerekliliklerini uygular.

Öğrenme Kazanımı 2: İş organizasyonu yapar.
Alt Öğrenme Kazanımları:
2.1: İş planlaması yapar.
2.2: Faaliyetler için yazılım, donanım ve ekipman temin eder.
2.3: Çalışma alanının düzenini takip eder.

Öğrenme Kazanımı 3: Siber güvenlik bileşenlerini ve içeriklerini araştırır.
Alt Öğrenme Kazanımları:
3.1**:** Son kullanıcı sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.2: Ağ sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.3: Sunucu sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.4: İşletim sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.5: Yazılım uygulamalarının siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.6: Veritabanı sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.7: Anti virüs sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.8: Çevresel birimlerin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.9: Bulut sistemlerinin siber güvenlik bileşenlerini ve içeriklerini araştırır.
3.10: Son kullanıcı sebepli gerçekleşebilecek güvenlik zafiyetini araştırır.

Öğrenme Kazanımı 4: Sızma testi gerçekleştirir.
Alt Öğrenme Kazanımları:
4.1: Test için hazırlık yapar.
4.2: Testi uygular.

8	ÖLÇME VE DEĞERLENDİRME

8 a) Teorik Sınav

Çoktan Seçmeli Sorularla Sınav (T1): A2 yeterlilik birimine yönelik olarak teorik sınav, Ek A2-2'de yer alan Bilgiler Kontrol Listesine göre gerçekleştirilir. Teorik değerlendirme için adaylara en az on (10) soruluk, dört (4) seçenekli, çoktan seçmeli ve her biri eşit puan değerinde olan sorularla düzenlenmiş yazılı sınav uygulanmalıdır. Bu sınavda boş bırakılan veya yanlış cevaplandırılmış sorulardan herhangi bir puan indirimi yapılmaz.
Sınavda adaylara her soru için ortalama bir buçuk (1,5) dakika zaman verilir. T1 sınavında soruların en az %70'ine doğru yanıt veren aday başarılı sayılır. Sınav soruları, bu birimde T1 sınavı ile ölçülmesi öngörülen tüm bilgi ifadelerini (Ek A2-2) ölçmelidir.

8 b) Performansa Dayalı Sınav

(P1): A2 birimine yönelik performansa dayalı sınav Ek A2-2'de yer alan "Beceriler ve Yetkinlikler" kontrol listesine göre gerçek veya gerçeğine uygun olarak düzenlenmiş çalışma ortamında gerçekleştirilir. Adaydan Ek A2-2'de yer alan beceri ve yetkinlik uygulamalarını gerçeğe uygun düzenlenmiş ortamda yapması beklenir.

Beceri ve yetkinlikler kontrol listesinde aday tarafından başarılması zorunlu kritik adımlar belirlenir.
Adayın, (P1) performans sınavından başarı sağlaması için kritik adımların tamamından başarılı performans göstermek koşuluyla sınavın genelinden asgari % 80 başarı göstermesi gerekir. (P1) Performansa dayalı sınavın süresi, belirlenen kapsamda, gerçek uygulama şartlarındaki süreye karşılık gelmelidir. (P1) olarak belirlenen Beceri ve Yetkinlik İfadelerinin (Ek A2-2) tamamı (P1) performansa dayalı sınav ile ölçülmelidir.

8 c) Ölçme ve Değerlendirmeye İlişkin Diğer Koşullar

Birim için öngörülen sınavların geçerlilik süresi sınavın başarıldığı tarihten itibaren 1 yıldır. Birimin elde edilebilmesi için başarılan sınav tarihleri arasındaki süre farkı 1 yılı geçemez. Birimin elde edilebilmesi için adayların birimde tanımlanan tüm sınavlardan başarılı olması gerekir.
Yeterlilik biriminin geçerlilik süresi birimin başarıldığı tarihten itibaren 2 yıldır.
Adayın kendi ve diğer kişilerin can güvenliğini tehlikeye sokacak bir davranış göstermesi halinde adayın sınavına son verilir.

9	**YETERLİLİK BİRİMİNİ GELİŞTİREN KURUM/KURULUŞ(LAR)**	Türkiye Bilişim Vakfı
10	**YETERLİLİK BİRİMİNİ DOĞRULAYAN SEKTÖR KOMİTESİ**	MYK Bilişim Teknolojileri Sektör Komitesi

YETERLİLİK BİRİMİ EKLERİ

EK [A2] -1: Yeterlilik Biriminin Kazandırılması için Tavsiye Edilen Eğitime İlişkin Bilgiler

1. **İSG, çevre ve kalite**
   1.1. İş sağlığı ve güvenliği önlemleri
   1.2. Çevre koruma
   1.3. Kalite gereklilikleri
   1.4. Kişisel verilerin korunması gereklilikleri
2. **İş organizasyonu**
   2.1. İş planlaması
   2.2. Yapılan işlerin kayıtları
   2.3. Çalışma alanının düzeni

3. Siber güvenlik bileşenlerini ve içeriklerini araştırma

3.1. Son kullanıcı sistemlerinin siber güvenlik bileşenleri ve içerikleri
3.2. Yerel ağ ve kablosuz ağda bulunan sistemlerin envanteri
3.3. Ağ sistemlerinin siber güvenlik bileşenleri ve içerikleri
3.4. Güvenlik duvarının güvenlik standartlarına uygunluğu
3.5. Yerel ağda bulunan sistemlerin konfigürasyonu
3.6. Sunucu sistemlerin siber güvenlik bileşenleri ve içerikleri
3.7. Sunucu sanallaştırma yazılımları
3.8. Sunucu depolama alanları ile sunucular arasında veri trafiği
3.9. İşletim sistemlerinin siber güvenlik bileşenleri ve içerikleri
3.10. İşletim sistemlerinin güvenlik yamalarını yükleme
3.11. Yazılım uygulamalarının siber güvenlik bileşenleri ve içerikleri
3.12. Uluslararası yazılım güvenliği standartları
3.13. Kapalı kaynak kodlu sistemlerin kurulumu
3.14. Açık kaynak kodlu yazılımlar
3.15. Veritabanı sistemlerinin siber güvenlik bileşenleri ve içerikleri
3.16. Veritabanı güvenliğini tehdit eden açıklar hakkında periyodik incelemeler
3.17.Anti virüs sistemlerinin siber güvenlik bileşenleri ve içerikleri
3.18. Anti virüs sunucularının güncel yama ve güncelleştirmelerini kurma
3.19. Virüs ve türevlerinin takibi
3.20. Çevresel birimlerin siber güvenlik bileşenleri ve içerikleri
3.21. Bulut sistemlerinin siber güvenlik bileşenleri ve içerikleri
3.22. Bulut güvenlik politikaları
3.23. Bulut sistemlerinde oluşan trafik anomalileri
3.24. Veri sızıntısı ve veri kaybı senaryoları
3.25. Açık kaynak istihbaratı çalışmaları
3.26. Temel seviye ağ bilgisi

4. Sızma testlerini gerçekleştirme

4.1. Sızma testlerinin yöntemleri
4.2. Sızma testlerinin uygulanma süreci
4.3. Sızma testi yapılacak alandaki verileri KVKK'ya göre sınıflandırma
4.4. Ağ yapısında kullanılan protokoller
4.5. Sızma testinde kullanılan yazılım araçları
4.6. Ağ sızma testleri
4.2. Etki alanı ve istemci sızma testleri
4.3. Web uygulamalarının sızma testleri
4.4. Veritabanı sızma testleri
4.5. Mobil uygulama sızma testleri
4.6. Sosyal mühendislik sızma testleri
4.7. DDOS testleri
4.8. Kaynak kod testleri
4.9. Yazılım gereçlerini verimli şekilde kullanılmasını sağlayan Linux yazılımı

5. Siber risklere karşı önleyici faaliyetler yapma

5.1. Sistemlerin kesintisiz çalışması için alınması gerekli önlemler
5.2. Sistemlerin saldırılara karşı korunması amaçlı önlemler
5.3. Güvenlik duvarı ayarları
5.3. Dijital arşivleme

EK [A2]-2: Yeterlilik Biriminin Ölçme ve Değerlendirmesinde Kullanılacak Kontrol Listesi

a) BİLGİLER

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BG.1	Siber güvenlik bileşenlerini ve içeriklerini açıklar.	C.1-C.10	3.1-3.9	T1
BG.2	Sızma testlerinin yöntemlerini açıklar.	D.2	4.1-2	T1
BG.3	Sızma testlerinin uygulanma sürecini tanımlar.	D.2	4.1-2	T1
BG.4	Sistemlerin kesintisiz çalışması için alınması gereken tedbirleri sıralar.	D.1	4.1	T1
BG.5	Sızma testi yapılacak alandaki verileri KVKK'ya göre sınıflandırır.	A.5	4.1	T1
BG.6	Ağ yapısında kullanılan protokolleri açıklar.	C.1	4.1	T1
BG.7	Sızma testi yapacağı ortamda kullanılan bilgisayarda var olan işletim sistemini açıklar.	D.1.1	4.1	T1
BG.8	Sızma testinde kullanılan yazılım araçlarını açıklar.	D.1.2	4.1	T1
BG.9	Sistemlerin siber saldırılara karşı korunması amaçlı alınabilecek önlemleri açıklar.	D.2	4.2	T1
BG.10	Güvenlik duvarı ayarlarını açıklar.	C.2.2	4.2	T1

b) BECERİ VE YETKİNLİKLER

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BY.1	Çalışmalarında İSG ile ilgili gereklilikleri uygular.	A.1.1	1.1	P1
BY.2	Çalışmalarında çevre ile ilgili gereklilikleri uygular.	A.3.1	1.2	P1
BY.3	Çalışmalarında kalite ile ilgili gereklilikleri uygular.	A.4.1	1.3	P1
*BY.4	Çalışmalarında kişisel verilerin korunması gerekliliklerini uygular.	A.5.1	1.4	P1
BY.5	İşletme yöntem, kural ve formatlarına uygun olarak iş emirlerini sistemden/ilgili birimden/amirden alarak gelen iş emrine yönelik ilgili kaynaklardan bilgi toplar.	B.1.1	2.1	P1
BY.6	Aldığı iş emirlerine ve topladığı bilgilere göre yapılacak faaliyetlerin sınıflamasını ve sıralamasını yaparak tahmini işlem sürelerini saptar.	B.1.2	2.1	P1
BY.7	İş emrine konu olan bilgisayar donanımlarının özelliklerine ve ortam koşullarına göre, uygun çalışma alanının (donanımların bulunduğu alan veya özel atölye) neresi olduğuna karar verir.	B.1.3	2.1	P1

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BY.8	Yaptığı sıralama ve belirlediği tahmini işlem sürelerini esas alarak eldeki iş gücü ve zaman kapasitesine göre işletme formatına uygun şekilde iş planını yaparak amirine onaylatır.	B.1.4	2.1	P1
BY.9	İş programına ve iş emirlerine göre yöneticinin bilgisi dâhilinde ilgili personele bilgi vererek işlemlerin gerçekleştirilmesini sağlar.	B.1.6	2.1	P1
BY.10	İş süreçlerinde kullanacağı ekipman ve yazılımların ön kontrollerini yapar.	B.2.1	2.2	P1
*BY.11	Çalışma için gerekli yazılım, donanım ve ekipmanları çalışmaya hazır hale getirir.	B.2.2	2.2	P1
BY.12	Çalışmaların kesintisiz ve uygun şekilde sürdürülmesi için, çalışma alanını inceleyerek özelliklerini ve çalışma noktalarının kapsamını belirler.	B.5.1	2.3	P1
BY.13	Çalışma alanının, kapsamına ve belirlenen özelliklerine göre, emniyet ve teknik olarak yapılacak işe uygun ortam koşullarına getirilmesini sağlar.	B.5.2	2.3	P1
BY.14	Çalışma sonunda, çalışma sahasını işin özelliklerine, etkisine ve bunlarla ilgili yöntemlere göre temizleyerek düzenler.	B.5.4	2.3	P1
BY.15	Son kullanıcı sistemlerinde kullanılan donanım ve yazılımların siber güvenlik standartlarını işletme talimatlarına göre araştırır.	C.1.1	3.1	P1
*BY.16	Yerel ağ ve kablosuz ağda bulunan sistemlerin envanterini çıkarır.	C.1.2	3.1	P1
*BY.17	Sistemlerde ortaya çıkabilecek muhtemel güvenlik zafiyetlerini tespit eder.	C.1.3	3.1	P1
BY.18	Ağ trafiğinde standart dışı veri tespiti yapabilecek bir yapının varlığını işletme talimatlarına göre araştırır.	C.2.1	3.2	P1
BY.19	Güvenlik duvarının güvenlik standartlarına uygunluğunu araştırır.	C.2.2	3.2	P1
BY.20	Yerel ağda bulunan sistemlerin konfigürasyonunu kontrol ederek sonucunu raporlar.	C.2.3	3.2	P1
BY.21	Sunucuların fiziksel güvenlik durumlarını araştırır.	C.3.1	3.3	P1
BY.22	Sunucu sanallaştırma yazılımlarının güncelleme durumlarını araştırır.	C.3.2	3.3	P1
BY.23	Sunucu depolama alanları ile sunucular arasında veri trafiğinin güvenlik durumunu araştırır.	C.3.3	3.3	P1
BY.24	İşletim sistemlerinin sistem günlük kayıtlarında anormal durumları tespit eder.	C.4.1	3.4	P1

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BY.25	İşletim sistemlerinin güvenlik yamalarını yükler.	C.4.2	3.4	P1
BY.26	İşletim sistemi içerisinde bulunan yazılım, servis, kayıt defteri, disk aktivitelerini detaylı analiz ederek analiz sonuçlarını raporlar.	C.4.3	3.4	P1
BY.27	Geliştirilen yazılımların uluslararası yazılım güvenliği standartlarında geliştirildiğini kontrol ederek sonucunu raporlar.	C.5.1	3.5	P1
*BY.28	Geliştirilen kapalı kaynak kodlu sistemlerin kurulumunda siber güvenlik önlemlerini alır.	C.5.3	3.5	P1
BY.29	Açık kaynak kodlu yazılımlarda bütünsel siber güvenlik kontrollerini yapar.	C.5.4	3.5	P1
BY.30	İnternet ve yerel ağ üzerinde çalışan yazılımların siber güvenlik politikalarını uygular.	C.5.5	3.5	P1
*BY.31	Veritabanı servislerinin yalnızca ilişkili sistemlerle çalışması için gerekli yetkilendirme politikalarını uygular.	C.6.1	3.6	P1
BY.32	Veritabanında gerçekleşebilecek olası veri kayıplarının önüne geçecek sistem geliştirmelerini uygular.	C.6.2	3.6	P1
BY.33	Veritabanı güvenliğini tehdit eden açıklar hakkında periyodik incelemeleri yapar.	C.6.3	3.6	P1
BY.34	Antivirüs sunucularının güncel yama ve güncelleştirmelerini kurar.	C.7.1	3.7	P1
BY.35	Virüs bulaşan cihazları genel sisteme zarar vermeyeceği şekilde izole eder.	C.7.2	3.7	P1
*BY.36	Virüs ve türevlerinin takibini yapar.	C.7.3	3.7	P1
BY.37	Genel virüs taramalarının periyodik olarak yapılmasını sağlar.	C.7.4	3.7	P1
BY.38	Antivirüs sistemlerinde oluşabilecek anlık hareketlenmelere karşı bildirim sistemini kurar.	C.7.5	3.7	P1
BY.39	Yazıcı, santral, güvenlik kameraları, kartlı geçiş sistemleri gibi çevresel sistemlerin olası sızmalara karşı güvenlik önlemlerini alır.	C.8.1	3.8	P1
*BY.40	Çevresel sistemlerde oluşabilecek saldırılara karşı son sistem konfigürasyonlarını yedekler.	C.8.2	3.8	P1
BY.41	Sistemlere erişim günlük kayıtlarını periyodik olarak kontrol eder.	C.8.3	3.8	P1
BY.42	Bulut sistemlerinin erişim kayıtlarını periyodik olarak kontrol eder.	C.9.1	3.9	P1
BY.43	Bulut güvenlik politikalarını uygulayacak geliştirmeleri yapar.	C.9.2	3.9	P1
*BY.44	Yerel sistemlerin olası ataklara karşı kesintisiz çalışma senaryolarını uygular.	C.9.3	3.9	P1

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
*BY.45	Bulut sistemlerinde oluşan trafik anomalilerini tespit etmek için gerekli geliştirmeleri yapar.	C.9.4	3.9	P1
BY.46	Sisteme erişen kötü niyetli kişilerin izlerini sürecek sistemleri geliştirir.	C.9.5	3.9	P1
BY.47	Veri sızıntısı ve veri kaybı senaryolarına karşı politika önerileri sunar.	C.9.6	3.9	P1
*BY.48	Açık kaynak istihbaratı çalışmalarını gerçekleştirir.	C.10.1	3.10	P1
BY.49	Elde ettiği verileri uygun şekilde derler.	C.10.2	3.10	P1
BY.50	Test için işletmenin ihtiyaçlarına uygun geçerli metodu belirler.	D.1.1	4.1	P1
BY.51	Gerekli yazılımı çalıştırarak yazılım için çalışırlık kontrolleri yapar.	D.1.2	4.1	P1
*BY.52	Talimatlara uygun şekilde ağ taraması yapar.	D.2.1	4.2	P1
*BY.53	Sızma testi uygulayarak zafiyeti araştırır.	D.2.2	4.2	P1
BY.54	İşletme talimatları uyarınca yapılan teste ait sonuçları raporlar.	D.2.3	4.2	P1

(*) Performans sınavında başarılması zorunlu kritik adımlar.

YETERLİLİK EKLERİ

1. Ulusal Yeterlilik Hazırlama Ekibi ve Teknik Çalışma Grubu Üyeleri

No	Adı - Soyadı	Eğitim Bilgileri* (Tarih - Eğitim Kurumu/Bölüm Adı)	Deneyim Bilgileri* (Tarih – İş Yeri – Unvan)
1.	Musa DEMİR (Moderatör)	1997 – Gazi Üniversitesi Sağlık Bilimleri Enstitüsü – İşçi Sağlığı ve İş Güvenliği (Yüksek Lisans) 1989 - Yıldız Üniversitesi Elektrik Mühendisliği (Lisans)	• 2020-Aralık 2021 Serbest Danışman • Temmuz 2019-Kasım 2020 – TEKLAS – İSG Yetkilisi • 1993-Şubat 2018 – ÇSGB – İş Başmüfettişi
2.	Yakup Hakan COŞKUN (Mesleki Yeterlilik Uzmanı)	2004 - Hacettepe Üniversitesi Kamu Yönetimi Bölümü	• 2016-Devam ediyor Pamir Uygunluk Değerlendirme Ltd. Şti.- Genel Müdür • 2008-2015 - Mesleki Yeterlilik Kurumu – Mesleki Yeterlilik Uzmanı • 2005-2008 - İŞKUR – Memur
3.	Ayhan DEMİR	2012 - Worwick üniversitesi Computer Engineer/ phd	• 2016 - Devam Liberta Yazılım CEO • 2008 - 2015 Özkaplan Halı IT direktörü
4.	Bekir OTURAKÇI	2007 - Selçuk Üniversitesi Teknik Eğitim Fakültesi- Bilgisayar	• 2016 Infotech Academy Eğitim Koordinatörü • 2010 İşte Site Proje Yöneticisi • 2007 Biltekno Yazılım Geliştirme
5.	Mahir DOĞAN	2021 - Ahmet Yesevi Üniversitesi Siber Güvenlik Yüksek Lisans	• 2021 İSMEK Bilişim Teknolojileri Okulu Yönetici Yardımcısı • 2006 - 2020 İSMEK Bilişim Teknolojileri Öğretmeni

No	Adı - Soyadı	Eğitim Bilgileri* (Tarih - Eğitim Kurumu/Bölüm Adı)	Deneyim Bilgileri* (Tarih – İş Yeri – Unvan)
6.	Marwa Issam ABDULKAREEM	2017 - Bağdat Üniversitesi Elektronik ve Haberleşme Mühendisliği	• 2020 Blue-Ram Siber Güvenlik Uzmanı • 2019-2020 Teknofriend Ağ Bulut Uzmanı • 2018-2019 Uzmantek Bilişim BT Uzmanı
7.	Minhac ÇELİK	2004 - 2009 Boğaziçi Üniversitesi / Siyaset Bilimi ve Uluslararası İlişkiler (Lisans) 2021 - 2023 Tallinn University of Technology / Technology Governance (Yüksek Lisans)	• 2013 - 2014 TÜBİTAK / SGE Kıdemli Uzman • 2014 - 2020 Microsoft / Kanal Yöneticisi • 2020 - Devam Siber Tehdit İstihbarat Analisti
8.	Nilgün YAKUT	1982, Orta Doğu Teknik Üniversitesi-Ekonomi, Lisans 1987-Boğaziçi Üniversitesi-Ekonomi, Yüksek Lisans 2020-Anadolu Üniversitesi-Tarım, Ön Lisans	• 2020 – Nisan 2022 TBV Proje Yöneticisi • 2018 - 2020 Sivas İŞGEM Genel Müdür • 2012 - 2020 Kobi ve Start Up Serbest Danışmanı, Mentor, İşletme Koçu • Türk Kahvesi Kültürü ve Araştırmaları Derneği/Genel Müdür • Mikrokredi Projesi/Direktör, • Finansal Okuryazarlık Derneği/Proje Direktörü • Koç Grubu, Genel Müdür Yardımcısı (1991-2011) • 2001-2002, Marmara Üniversitesi Öğretim Görevlisi (Yarı Zamanlı) • 2012-2013,İstanbul Ticaret Üniversitesi Öğretim Görevlisi (Yarı Zamanlı)

No	Adı - Soyadı	Eğitim Bilgileri* (Tarih - Eğitim Kurumu/Bölüm Adı)	Deneyim Bilgileri* (Tarih – İş Yeri – Unvan)
9.	Ömer Faruk AYAZ	2017 - Anadolu Üniversitesi İşletme Fakültesi	• 2020 Çözüm Eğitim Kurumları Eğitim Koordinatörü • 2017 Binot Yayınları Pazarlama Müdürü • 2016 Kobilim - Kobi Danışmanlık Hizmetleri Kurucu
10.	Salih PİLAV	1993-Anadolu Üniversitesi İİBF-İşletme	• 2021 – Ocak 2022 TBV Proje Mali ve İdari İşler - Eşfinansman • 2019-2020 Tila Kompozit Genel Müdür Yardımcısı • 2014-2020 Pilatek Ortak
11.	Selçuk HALICI	1987-Selçuk Üniversitesi Fen Edebiyat Fakültesi – Matematik	• 2020 – Nisan 2022 TBV Proje Sertifikasyon Uzmanı • 2014 - 2015 Freelanse SAP Danışmanı • 1987 - 2014 Bilkom A.Ş. Proje ve İş Geliştirme Müdürü

No	Adı - Soyadı	Eğitim Bilgileri* (Tarih - Eğitim Kurumu/Bölüm Adı)	Deneyim Bilgileri* (Tarih – İş Yeri – Unvan)
12.	Şebnem ÖZDEMİR	2004 - Yıldız Teknik Üniversitesi - Matematik	• 2019 – devam İstinye Üniversitesi - Yönetim & Bilişm Sistemleri Bölüm Başkanı • 2019 - Devam MIT Computer Science and Artificial Araştırma İşbirlikçisi • 2018 - Devam Beykent Üniversitesi Yönetim Bilişim Sistemleri Doktor Öğretim Üyesi
13.	Turgay KAYA	1990-İstanbul Üniveristesi Fen Fakültesi Fizik	• 2011 - Devam Blu-ram Kurucu - CEO • 2005 - 2011 Forever Living Product BT Yöneticisi • 2005 - 2011 Bilge Adam Şube Md. Yrd.
14.	Volkan TÜRKYILMAZ	2002-Karadeniz Teknik Üniversitesi - Elektrik-Elektronik Mühendisliği	• 2020 – Haziran 2021 TBV Proje Teknik Uzmanı • 2020 -Devam İstinye Üniversitesi Misafir Öğretim Görevlisi • 2018 - 2020 Dijital Dönüşüm Pro Dijital Dönüşüm Danışmanı

**Yalnızca meslekle ilgili olan eğitim/deneyim bilgilerine yer verilecektir.*

2. Görüş İstenen Kişi, Kurum ve Kuruluşlar

Ankara Sanayi Odası (ASO)
Ankara Ticaret Odası (ATO)
Belediye Yazılım Sanayicileri ve İş İnsanları Derneği (BEYSİAD)
Belgelendirme Kuruluşları Derneği (BEKDER)
Bilgi Güvenliği Derneği (BGD)
Bilgi Teknolojileri Derneği (BİTEKDER)
Bilgisayar Mühendisleri Odası (BMO)
Bilişim Güvenliği Derneği (TBGD)

Bilişim Medyası Derneği (BMD)
Bilişim Sanayicileri Derneği (TÜBİSAD)
Bilişim Sektörü Derneği (TÜBİDER)
Bilişim Sektörü Dernekleri Federasyonu (TÜBİFED)
Bilişim ve Yazılım Eser Sahipleri Meslek Birliği (BİYESAM)
Çağrı Merkezleri Derneği (ÇMD)
Çalışma ve Sosyal Güvenlik Bakanlığı (İş Sağlığı ve Güvenliği Genel Müdürlüğü)
Ege Bölgesi Sanayi Odası (EBSO)
Elektronik Ticaret Altyapı Sağlayıcıları Derneği (EDER)
Fütüristler Derneği
Hak-İş Konfederasyonu
ISACA Bilişim Yönetişim ve Denetim Derneği
İnternet Temelli Televizyon Teknolojileri Derneği
İstanbul Ticaret Odası (İTO)
Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı (KOSGEB)
LİNUX Kullanıcılar Derneği (LKD)
Milli Eğitim Bakanlığı Hayat Boyu Öğrenme Genel Müdürlüğü
Milli Eğitim Bakanlığı Mesleki ve Teknik Eğitim Genel Müdürlüğü
Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Mobil İletişim Araçları ve BT İş Adamları Derneği (MOBİSAD)
Mobil Servis Sağlayıcı İş Adamları Derneği (MOBİLSİAD)
Oyun Tasarımcıları, Geliştiricileri, Yapım ve Yayıncıları Derneği (OYUNDER)
Sağlık Bilişim Derneği
Sektörel Araştırmalar Derneği
Serbest Telekomünikasyon İşletmecileri Derneği (TELKODER)
SİNERJİTÜRK
Teknolojide Kadın Derneği (Wtech)
Telekomünikasyon İnternet ve Bilgi Teknolojileri Derneği (TEDER)
TOBB Türkiye Yazılım Meclisi
Tüketici Hakları Derneği (THD)
Tüm İnternet Derneği (TİD)
Türk Elektronik Sanayicileri Derneği (TESİD)
Türkiye Devrimci İşçi Sendikaları Konfederasyonu (DİSK)
Türkiye Esnaf ve Sanatkârları Konfederasyonu (TESK)
Türkiye İhracatçılar Meclisi (TİM)
Türkiye İstatistik Kurumu (TÜİK)
Türkiye İş Kurumu (İş ve Meslek Danışmanlığı Dairesi Başkanlığı)
Türkiye İşçi Sendikaları Konfederasyonu (TURK-İŞ)
Türkiye İşveren Sendikaları Konfederasyonu (TİSK)
Türkiye Küçük ve Orta Ölçekli İşletmeler Serbest Meslek Mensupları ve Yöneticiler Vakfı (TOSYÖV)
Türkiye Odalar ve Borsalar Birliği (TOBB)
Türkiye Zeka Vakfı (TZV)
Uydu Elektronik İletişim İş İnsanları Derneği (TUYAD)
Yazılım Sanayicileri Derneği (YASAD)
Yetkilendirilmiş Belgelendirme Kuruluşları Derneği (YBKDER)
Yükseköğretim Kurulu Başkanlığı (YÖK)

3. MYK Sektör Komitesi Üyeleri ve Uzmanlar

Prof. Dr. Ahmet ÖZMEN	Başkan (Yükseköğretim Kurulu Başkanlığı)
Yasemin AKPINAR	Başkan Vekili (Milli Eğitim Bakanlığı)
Mesut AKANER	Üye (Çalışma ve Sosyal Güvenlik Bakanlığı)
Emrullah EMEN	Üye (Sanayi ve Teknoloji Bakanlığı)
Muzaffer ÇALIŞKAN	Üye (Ulaştırma ve Altyapı Bakanlığı)
Melek BAR ELMAS	Üye (Türkiye Odalar ve Borsalar Birliği)
Gökhan Recep BİŞKİN	Üye (Hak İşçi Sendikaları Konfederasyonu)
Tayfun ARIKAZAN	Üye (Türkiye İşveren Sendikaları Konfederasyonu)
Umut Barış ERDOĞAN	Üye (Türkiye İşçi Sendikaları Konfederasyonu)
Umut CÜYAZ	Üye (Türkiye Esnaf ve Sanatkârları Konfederasyonu)
Esma DOĞAN	Üye (Mesleki Yeterlilik Kurumu)
Yaprak AKÇAY ZİLELİ	Daire Başkanı, Mesleki Yeterlilik Kurumu

4. MYK Yönetim Kurulu

Adem CEYLAN	Başkan (Çalışma ve Sosyal Güvenlik Bakanlığı Temsilcisi)
Prof. Dr. Mehmet SARIBIYIK	Üye (Yükseköğretim Kurulu Temsilcisi)
Dr. Recep ALTIN	Üye (Milli Eğitim Bakanlığı Temsilcisi)
Bendevi PALANDÖKEN	Üye (Meslek Kuruluşları Temsilcisi)
Dr. Osman YILDIZ	Üye (İşçi Sendikaları Konfederasyonları Temsilcisi)
Celal KOLOĞLU	Üye (İşveren Sendikaları Konfederasyonu Temsilcisi)