
GAZİ ÜNİVERSİTESİ
Gazi
1926

TÜRK SAVUNMA SANAYİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMALARI İLE CMMC GEREKSİNİMLERİNİN DEĞERLENDİRİLMESİ

İsmail Yiğit COŞAR

YÜKSEK LİSANS TEZİ
YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2022

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İsmail Yiğit COŞAR

05/06/2022

TÜRK SAVUNMA SANAYİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMALARI İLE CMMC GEREKSİNİMLERİNİN DEĞERLENDİRİLMESİ

(Yüksek Lisans Tezi)

İsmail Yiğit COŞAR

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2022

ÖZET

Son yıllarda bilgi ve bilişim teknolojileri hayatımızda her alanda yoğun olarak kullanılmaktadır. Bu sayede yaşamımıza ait fiziksel dinamiklerin çoğu artık önemli ölçüde siber dünyaya aktarılmaktadır. Her ne kadar bu durum hayatımızı önemli ölçüde kolaylaştırıyor olsa da önemli riskleri ve farklı türde tehditleri de beraberinde getirmektedir. Bunun sonucu olarak da her geçen gün hem kişisel hem de kurumsal ölçekte bilgi güvenliği yönetiminin önemi ciddi şekilde artmaktadır. Buna karşı 90'lı yıllardan itibaren kurumsal ölçekte kuruluşların genel olarak karşı karşıya kaldığı risk ve tehditlere karşı sektörden ve bilgi türlerinden bağımsız birtakım bilgi güvenliği yönetimi uygulamaları geliştirilmekte olsa da günümüzde artan gelişmiş tehditlere ve saldırı yöntemlerine karşısında bilgi türlerine ve sektöre özel oluşturulan bilgi güvenliği yönetimi uygulamalarının sayılarının da arttığı gözlemlenmektedir. Bu uygulamaların amacı kritik sektörlerde bilgi türlerine ve sektöre özel gereksinimler oluşturarak alınacak tedbirlerin daha etkin olmasını sağlamaktır. Bu doğrultuda ABD Savunma Bakanlığı (DoD) hizmet aldığı savunma sanayi sektörü kuruluşları için CMMC adını verdiği bir bilgi güvenliği yönetimi uygulaması oluşturmuştur. Bu çalışmada ülkemiz savunma sanayi kuruluşlarına, mevcut ve gelecekteki projelerinde bu alanda ihtiyaç duyması halinde faydalı olması amacıyla; ülkemizin önemli savunma sanayi kuruluşlarının hali hazırda gerçekleştirmekte oldukları bilgi güvenliği yönetimi uygulamaları anket yöntemi ile araştırılmış, bu uygulamaların en çok kullanılanı ile CMMC hakkında bilgi verilerek her iki uygulamanın gereksinimleri ayrı ayrı uzman görüşleri doğrultusunda karşılaştırılmış, en çok kullanılan uygulamanın CMMC 'ye göre eksiklerinin olup olmadığı değerlendirilerek elde edilen sonuçlar ve yapılması gerekenler ile ilgili öneriler sunulmuştur.

Bilim Kodu	:	114601
Anahtar Kelimeler	:	Siber güvenlik, bilgi güvenliği, olgunluk modeli, savunma sanayi
Sayfa Adedi	:	145
Danışman	:	Prof. Dr. Aslıhan TÜFEKCİ

INFORMATION SECURITY MANAGEMENT SYSTEM APPLICATIONS IN TURKISH DEFENSE INDUSTRY AND EVALUATION OF CMMC REQUIREMENTS

(M. Sc. Thesis)

İsmail Yiğit COŞAR

GAZI UNIVERSITY

INFORMATICS INSTITUTE

June 2022

ABSTRACT

In recent years, information and information technologies have been used extensively in all areas of our lives. In this way, most of the physical dynamics of our lives are now significantly transferred to the cyber world. Although this situation makes our lives much easier, it also brings with it important risks and different types of threats. As a result of this, the importance of information security management on both personal and corporate scales is increasing day by day. On the other hand, although some information security management applications, independent of the sector and information types, have been developed against the risks and threats generally faced by corporate-scale organizations since the 90s, today the number of information security management applications created specifically for "information types and sector" against "advanced threats and attack methods" is increasing. The purpose of these applications is to ensure that the measures to be taken are more effective by creating information types and sector-specific requirements in critical sectors. In this direction, the US Department of Defense (DoD) has created an information security management application called CMMC for the defense industry sector which it receives service from. In this study, in order to be beneficial to our country's defense industry organizations in their current and future projects, if they need it in this field; the information security management practices that the important defense industry organizations of our country are currently carrying out were researched by survey method, by giving information about the most used of these applications and CMMC, the requirements of both applications were discussed one by one and compared in line with expert opinions, by evaluating whether the most used application has deficiencies according to CMMC, the results obtained and suggestions about what to do are presented.

Science Code	:	114601
Key Words	:	Cyber security, information security, maturity model, defense industry
Page Number	:	145
Supervisor	:	Prof. Dr. Aslıhan TÜFEKCİ

TEŞEKKÜR

Yüksek lisans çalışmalarım süresince kıymetli yardımlarını ve desteğini her daim yanımda hissettiğim değerli tez danışmanım Prof. Dr. Aslıhan TÜFEKCİ'ye; bugünlere gelmemde sonsuz emek sahibi engin fikirli, zeki ve başarılarıyla her zaman bana örnek olan annem Nermin COŞAR ve babam Yusuf Ziya COŞAR'a teşekkür eder,

Başarıya giden yolda desteğini hiçbir zaman esirgemeyen, çalışmalarım sırasında büyük fedakarlıklarda bulunan değerli eşim Dilek COŞAR'a şükranlarımı sunarım.

Çalışmamı kıymetli evlatlarım Ziya Berk COŞAR ve Remzi Batu COŞAR'a ithaf ediyorum.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ x

ŞEKİLLERİN LİSTESİ xii

KISALTMALAR xiii

1. GİRİŞ 1

2. ISO/IEC 27001, CMMC DÜNYADAKİ DİĞER UYGULAMALAR 9

2.1. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi 9

2.1.1. Gelişim süreci ve genel özellikler 9

2.1.2. Kapsam 11

2.1.3. Gereksinimler 11

2.1.4. Belgelendirme 19

2.2. Siber Güvenlik Olgunluk Modeli Sertifikasyonu (CMMC) 19

2.2.1. Gelişim süreci ve genel özellikler 19

2.2.2. Kapsam 24

2.2.3. Gereksinimler 25

2.2.4. Belgelendirme 28

2.3. Dünyadaki Diğer Uygulamalar 30

2.3.1. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Platformu 30

2.3.2. Avrupa Telekomünikasyon Standartları Enstitüsü-ETSI standartları 31

Sayfa

2.3.3. Avrupa Birliği Siber Güvenlik Ajansı-ENISA rehber dokümanları 32

2.3.4. ISO/IEC bilgi güvenliği standartları ailesi..... 33

2.3.5. NATO Ortak Siber Savunma Mükemmeliyet Merkezi-CCDCOE rehber dokümanları..... 36

2.3.6. Elektrik ve Elektronik Mühendisleri Enstitüsü-IEEE standartları 37

3. YÖNTEM..... 39

4. ARAŞTIRMA BULGULARI 41

4.1. Kuruluşlarda Mevcut Bilgi Güvenliği Uygulamaları..... 41

4.2. Kuruluşlara Son Bir Yılda Yapılan Siber Saldırılar..... 45

4.3. Kuruluşların CMMC Farkındalığı..... 47

4.4. ISO/IEC 27001 Gereksinimleri ile CMMC Uygulamalarına Ait Eşleştirme Tabloları 49

4.4.1. “AC-Erişim Kontrolü” alanı karşılıkları 49

4.4.2. “AT-Farkındalık ve Eğitim” alanı karşılıkları 57

4.4.3. “AU-Denetim ve Hesap Verebilirlik” alanı karşılıkları 59

4.4.4. “CM-Konfigürasyon Yönetimi” alanı karşılıkları 63

4.4.5. “IA-Tanımlama ve Doğrulama” alanı karşılıkları 67

4.4.6. “IR-Olay Müdahalesi” alanı karşılıkları..... 71

4.4.7. “MA-Bakım” alanı karşılıkları 72

4.4.8. “MP-Medya Koruması” alanı karşılıkları 75

4.4.9. “PS-Personel Güvenliği” alanı karşılıkları 78

4.4.10. “PE-Fiziksel Koruma” alanı karşılıkları..... 80

4.4.11. “RA-Risk Değerlendirme” alanı karşılıkları 82

4.4.12. “CA-Güvenlik Değerlendirmesi” alanı karşılıkları..... 84

4.4.13. “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları..... 87

Sayfa

4.4.14. “SI-Sistem ve Bilgi Bütünlüğü” alanı karşılıkları 93

5. SONUÇ VE ÖNERİLER 99

KAYNAKLAR 105

EKLER 111

EK-1. Uzman görüşü formu 112

EK-2. Soru listesi formu 115

EK-3. Eşleştirme değerlendirme formu 118

ÖZGEÇMİŞ 144

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. İçerik ana başlıkları 12

Çizelge 2.2. Kontrol amaçları ve kontroller..... 14

Çizelge 2.3. CMMC modelinde yararlanılan başlıca kaynaklar..... 22

Çizelge 2.4. CMMC modelinde yer alan alanlar ve uygulama sayıları 27

Çizelge 2.5. ISO/IEC 27000 ailesi standartları 15

Çizelge 4.1. Soru 1'e ait cevaplar..... 41

Çizelge 4.2. Soru 2'ye ait cevaplar 41

Çizelge 4.3. Soru 3'e ait cevaplar 42

Çizelge 4.4. Soru 4'e ait cevaplar..... 43

Çizelge 4.5. Soru 5'e ait cevaplar 44

Çizelge 4.6. Soru 6'ya ait cevaplar 44

Çizelge 4.7. CB DDO BİGR ve ISO/IEC 27001 dışındaki uygulamalar 45

Çizelge 4.8. Soru 7'ye ait cevaplar 46

Çizelge 4.9. Soru 8'e ait cevaplar 46

Çizelge 4.10. Soru 9'a ait cevaplar..... 47

Çizelge 4.11. Soru 10'a ait cevaplar 47

Çizelge 4.12. Soru 11'e ait cevaplar 49

Çizelge 4.13. "AC-Erişim Kontrolü" alanı karşılıkları..... 50

Çizelge 4.14. "AT-Farkındalık ve Eğitim" alanı karşılıkları..... 57

Çizelge 4.15. "AU-Denetim ve Hesap Verebilirlik" alanı karşılıkları 59

Çizelge 4.16. "CM-Konfigürasyon Yönetimi" alanı karşılıkları..... 63

Çizelge 4.17. "IA-"Tanımlama ve Doğrulama" alanı karşılıkları 67

Çizelge 4.18. "IR-Olay Müdahalesi" alanı karşılıkları..... 71

Çizelge **Sayfa**

Çizelge 4.19. “MA-Bakım” alanı karşılıkları 72

Çizelge 4.20. “MP-Medya Koruması” alanı karşılıkları..... 75

Çizelge 4.21. “PS-Personel Güvenliği” alanı karşılıkları 79

Çizelge 4.22. “PE-Fiziksel Koruma” alanı karşılıkları 80

Çizelge 4.23. “RA-Risk Değerlendirme” alanı karşılıkları 82

Çizelge 4.24. “CA-Güvenlik Değerlendirmesi” alanı karşılıkları 84

Çizelge 4.25. “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları 87

Çizelge 4.26. “SI-Sistem ve Bilgi Bütünlüğü” alanı karşılıkları 93

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. EN ISO/IEC 27001 gelişim aşamaları 10

Şekil 2.2. Sözleşme uyarınca toplanan, oluşturulan ve alınan bilgiler 21

Şekil 2.3. CMMC çerçeve modeli..... 26

Şekil 2.4. CMMC Seviye tanımları, uygulama sayıları ve denetim metodu 27

Şekil 4.1. ISO/IEC 27001'de karşılığı bulunmayan CMMC v2.0 uygulamalarının dağılımı 95

Şekil 4.2. CMMC v2.0 uygulamalarının alanlarına göre karşılık sayıları ve oranları.... 96

Şekil 4.3. CMMC v2.0 uygulamalarının seviyelere göre karşılık sayıları ve oranları ... 97

KISALTMALAR

Bu çalışmada kullanılmış bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri
AC	Erişim Kontrolü (Access Control)
AIA	Uzay Endüstrisi Birliği (Aerospace Industry Association)
ANSI	Amerikan Ulusal Standartlar Enstitüsü (American National Standards Institute)
AT	Farkındalık ve Eğitim (Awareness and Training)
AU	Denetim ve Hesap Verebilirlik (Audit and Accountability)
BGY	Bilgi Güvenliği Yönetimi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIGR	Bilgi ve İletişim Güvenliği Rehberi
BS	İngiliz Standardı (British Standart)
BSI	İngiliz Standarları Enstitüsü (British Standards Instition)
C3PAO	CMMC Üçüncü Taraf Değerlendirici Kuruluşu (CMMC Third-Party Assessor Organization)
CA	Güvenlik Değerlendirmesi (Security Assessment)
CAICO	CMMC Değerlendiricileri ve Eğitmenleri Sertifikasyon Organizasyonu (CMMC Assessors and Instructors Certification Organization)
CB	Cumhurbaşkanlığı
CCDCOE	Ortak Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence)
CEN	Avrupa Standartlar Komitesi (European Committee for Standardization)
CERT	Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Team)

Kısaltmalar	Açıklamalar
CIS	İnternet Güvenliği Merkezi (Center for Internet Security)
CM	Konfigürasyon Yönetimi (Configuration Management)
CMMC	Siber Güvenlik Olgunluk Modeli Sertifikasyonu (Cybersecurity Maturity Model Certification)
CMMC-AB	CMMC Akreditasyon Kuruluşu (CMMC Accreditation Body)
CUI	Kontrollü Gizli Olmayan Bilgi (Controlled Unclassified Information)
DCMA	Savunma Sözleşme Yönetim Ajansı (Defense Contract Management Agency)
DDO	Dijital Dönüşüm Ofisi
DDoS	Dağıtılmış Hizmet Reddi (Distributed Denial-of-Service)
DFARS	Savunma Federal Satın Alma Yönetmeliği Eki (Defense Federal Acquisition Regulation Supplement)
DIB	Savunma Sanayi (Defense Industry Base)
DIBCAC	Savunma Sanayi Siber Güvenlik Değerlendirme Merkezi (Defense Industrial Base Cybersecurity Assessment Center)
DISA	Savunma Bilgi Sistemleri Ajansı (Defense Information Systems Agency)
DoD	Savunma Bakanlığı (Department of Defense)
EN	Avrupa Standardı (European Norm)
ENISA	Avrupa Birliği Siber Güvenlik Ajansı (The European Union Agency for Cybersecurity)
ETSI	Avrupa Telekomünikasyon Standartlar Komitesi (European Telecommunications Standards Institute)
FAR	Federal Satın Alma Yönetmeliği (Federal Acquisition Regulation)

Kısaltmalar	Açıklamalar
FCI	Federal Sözleşme Bilgileri (Federal Contract Information)
FFRDC	Federal Olarak Finanse Edilen Araştırma ve Geliştirme Merkezleri (Federally Funded Research and Development Centers)
FIPS	Federal Bilgi İşlem Standartı (Federal Information Processing Standards)
HLS	Yüksek Seviyeli Yapı (High Level Structure)
IA	Tanımlama ve Doğrulama (Identification and Authentication)
IAF	Uluslararası Akreditasyon Forumu (The International Accreditation Forum)
IEC	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers)
IETF	İnternet Mühendisliği Görev Gücü (Internet Engineering Task Force)
IR	Olay Müdahalesi (Incident Response)
ISACA	Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association)
ISF	International Security Forum (Uluslararası Güvenlik Forumu)
ISO	Uluslararası Standartlar Teşkilatı (International Organization for Standardization)
ITAR	Uluslararası Silah Ticareti Düzenlemeleri (International Traffic in Arms Regulations)
ITIL	Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technology Infrastructure Library)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)

Kısaltmalar	Açıklamalar
JTC1	Ortak Teknik Komite 1 (Joint Technical Comitee 1)
MA	Bakım (Maintenance)
MP	Medya Koruması (Media Protection)
NAS	Ağa Bağlı Depolama (Network Attached Storage)
NATO	Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
OUSD A&S	Edinme ve Sürdürme için Savunma Müsteşarlığı Ofisi (Office of the Under Secretary of Defense for Acquisition & Sustainment)
PE	Fiziksel Koruma (Physical Protection)
PS	Personel Güvenliği (Personnel Security)
RA	Risk Değerlendirmesi (Risk Assessment)
RFC	Yorum İsteği (Request For Comments)
RMM	Esneklik Yönetim Modeli (Resilience Management Model)
SASAD	Savunma ve Havacılık Sanayii İmalatçılar Derneği
SC	Sistem ve Haberleşme Koruması (System and Communications Protection)
SI	Sistem ve Bilgi Bütünlüğü (System and Information Integrity)
TSE	Türk Standardları Enstitüsü
UARC	Üniversiteye Bağlı Araştırma Merkezi (University Affiliated Research Center)

1. GİRİŞ

Gelişen teknoloji ile hayatımızın her alanında öne çıkan "dijitalleşme" kavramı, bilgi varlıklarının türlerini ve büyüklüklerini arttırırken aynı zamanda kişi ve kurumların da bilgi güvenliğini sağlamak konusunda tedbir almalarını zorunlu hale getirmiştir [1].

Bununla birlikte geçtiğimiz son birkaç yılda dünyamızı etkisi altına alan Covid-19 salgını, içinde yaşadığımız düzeni ve alışkanlıklarımızı büyük ölçüde değiştirmiş, bilişim teknolojilerindeki ilerleme de bu değişikliklere paralel olarak oldukça artmıştır [2].

Böylece günümüzde baş döndürücü seviyelere çıkan sayısız teknolojik gelişme sayesinde yaşamakta olduğumuz fiziksel dünyaya ait dinamiklerin önemli ölçüde siber alana doğru evirilmeye başladığı söylenebilir [3].

Bu durumun öne çıkardığı önemli bir sonuç, özellikle ülkeler arası bir rekabet söz konusu olduğunda, "güç" kavramının "bilgi" kavramı ile neredeyse eş anlamlı olarak kullanılmaya başlanmasıdır [4]. Böylece ülkelerin güçlerini arttırması veya en azından mevcut olan güçlerini muhafaza edebilmeleri en başta kendi veri alt yapılarına bağlı bilgi kaynaklarının güvenliğinin sağlanması ile mümkün olabilmektedir.

Buradan da görüleceği üzere "bilgi" artık güvenliğin sağlanması için gerekli gücün temelinde yer almaktadır. Böylece ülkelerin bilgi varlıklarının güvenliğinde yaşanacak muhtemel bir zafiyet onlar için önemli bir tehdit oluşturacaktır. Bu bakımdan bilgi güvenliğine gereken önemi göstermemenin hem bireyler olarak bizlere hem de ülkemize maliyeti tahmin edilenden çok daha fazla olacaktır [5].

Buna bağlı olarak Bilgi Güvenliği Yönetimi (BGY), modern organizasyonlar için kritik bir bileşen haline gelmiş olup çoğu durumda, düzgün ve sorunsuz çalışan bilgi sistemleri olmaksızın bir işi yürütmek neredeyse imkânsız hale gelmiştir [6].

Örnek olarak, 2018 yılında Amerika Birleşik Devletleri'nde (ABD) 2016 yılı verilerine dayanarak yapılan bir çalışmada, siber saldırıların sadece ABD ekonomisine vermiş olduğu zararın 57 ila 109 milyar dolar olduğu belirtilmektedir [7]. Aynı yıl için dünya ülkelerinin

tamamında siber saldırıların neden olduğu zararın ise dünya toplam gayrisafi yurtiçi hasılasının %1'ine karşılık gelen 600 milyar dolar seviyesinde olduğu ifade edilmektedir [8].

Oldukça yüksek seviyelerde zarar verme kapasitesine sahip olabilen siber saldırılar, türleri ve etki ölçekleri bakımından da çok çeşitli olabilmektedir. Özellikle büyük ölçekte gerçekleşen siber saldırılara bakıldığında arkalarında gelişmiş ülkelerin yer aldığı durumlarla dahi karşılaşılabilmektedir. Buradan hareketle tarihte bir dönem yaşanan ülkeler arasındaki soğuk savaşların günümüzde artık siber dünyaya kaydığı söylenebilir [9].

Bu bakımdan uluslararası politik gelişmelere bağlı olarak ülkeler; kendilerine yönelik tehditleri bertaraf edebilmek, gerektiğinde diğer ülkeler nazarında bir baskı unsuru yaratabilmek veya en temelde mevcudiyetlerini sürdürülebilir kılmak için bilgi güvenliğini sağlamak adına birtakım tedbirler almak durumundadır [10]. Bu amaçla gelişmiş ülkeler 90'lı yıllardan itibaren siber dünyada risklerin ortadan kaldırılması ve güvenliğin arttırılmasına yönelik çalışmalarını özellikle bilgi güvenliği yönetimi alanında standart oluşturma faaliyetleri ile devam ettirmektedir.

Bu alanda ilk olarak 1995 yılında İngiltere'de BSI (British Standards Institution), BS 7799-1:1995 numaralı bilgi güvenliği yönetimi standardını yayınlamıştır. Bu sayede bilgi güvenliğine sistemsel bir yönetim anlayışını ortaya çıkaran ve günümüzde yaygın olarak kullanılan bilgi güvenliği yönetim sistemi standardı olan ISO/IEC 27001'in temellerinin de oluşturulduğu söylenebilir [11].

Bununla birlikte hükümetlerin ve büyük kuruluşların baskılarıyla siber güvenlik standartlarının sayıları da giderek artmakta olup daha fazla kuruluş standart geliştirme süreçlerine dahil olmaktadır.

Bu doğrultuda o günlerden günümüze dek, bilgi güvenliği yönetimi ile ilgili ulusal ve uluslararası birçok kuruluş (NIST, CIS, ISACA, ISF, ITU, ETSI, DISA, ITIL, IEEE vd.) çok sayıda standart, uygulama modeli ve rehber doküman benzeri birçok çalışma yayınlayarak kişi ve kuruluşların hizmetine sunmuştur [12].

Bu kapsamda standart yapılarına bakıldığında, ANSI ve FIPS Yayınları kapsamındaki bazı standartlar, başlıklarında standart terimini içerdikleri için kolayca ayırt edilebilirken

uluslararası bir standart geliştiricisi olan Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayınlanan standartlar, Tavsiyeler olarak adlandırıldığından standart olarak ayırt edilmesi daha zordur.

Benzer şekilde İnternet Mühendisliği Görev Gücü (IETF) tarafından yayınlanan bir standart, Yorum Talebi (RFC) olarak yayınlanmaya başlamakta ve standart olarak kabul edildikten sonra bile bu tanımını muhafaza etmektedir.

Standartlara ilave olarak bazı kuruluşlarda rehber niteliğinde dokümanlar yayınlamaktadır. Buna örnek olarak, ABD veya uluslararası menşeili birçok kuruluşun Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) özel yayınlarını standart olarak benimsemiş olmalarına rağmen bu belgeler ABD Federal kurumları tarafından kullanım için kılavuz olarak yayınlanmıştır [13].

Burada bahsi geçen ve uluslararası ölçekte yapılan bu çalışmaların bir kısmı sektörden bağımsız şekilde her çeşit organizasyona uygulanabilir iken bir diğer kısmı ise havacılık, telekomünikasyon, finans, sağlık, savunma vd. sektörlerde kullanılmak üzere özel olarak oluşturulmuştur.

Sektör özelinde oluşturulmuş bu tip uygulamalarla birlikte bilgi güvenliği yönetimine yönelik sektöre uygun tanımlar ve gereksinimlerin daha ayrıntılı olarak ifade edilmesine olanak sağlanmıştır.

Bu çerçeveden bakıldığında diğer sektörlerden farklı olarak savunma sanayi sektörü, kolaylıkla da anlaşılabileceği üzere, her ülke için bünyesinde bulundurduğu en kritik sektörlerin başında gelmektedir [14].

Özellikle son dönemde artan küreselleşme ile gelir dağılımının bozulması, ülkelerin sınırları içerisinde önlemler alarak korumacı siyasi alt yapının oluşmasına zemin hazırlamıştır. Uluslararası ilişkilerde de ülkeler arasındaki gelir dağılımı dengesizleşmesi, gelişmiş ülkeler ile Rusya, Hindistan ve Çin gibi gelişmekte olan ülkeler arasında iktidar mücadelelerine neden olmakta ve bu durumun yarattığı gerilim savunma sanayinin önemini daha da arttırmaktadır [15].

Artan tehdit ve riskler karşısında ülkeler, ulusal güvenliğini sağlayabilmek için yıllarca süren ve oldukça maliyetli araştırma geliştirme faaliyetleri yürütmekte böylece elde ettikleri bilgi birikimlerini kendi savunma sanayi kuruluşları aracılığıyla fiziksel güvenlik araçlarına dönüştürmektedir [16].

Bahsi geçen bu süreçlerde savunma sanayi kuruluşlarına iletilen ve/veya bu kuruluşlarla birlikte edinilen bu değerli bilgi birikimleri, projeler kapsamında ürüne dönüştürülmesi amacıyla, ihtiyaçların gerektirdiği ölçüde diğer tedarikçi niteliğindeki firmalar ile de paylaşılmaktadır. Tedarikçi niteliğinde olan bu firmalar bazı durumlarda ulusal olabilirken bazı durumlarda ise tamamen yabancı menşeili de olabilmektedir [17].

Küreselleşen dünya ekonomisinin getirmiş olduğu yeni üretim prensipleri çerçevesinde kaçınılmaz olan bu durum [18], ülkeler nezdinde savunma sanayinde bilgi güvenliği yönetiminin diğer sektörlere göre zaten daha yüksek olan önemini daha da kritik seviyeye çıkarmaktadır.

Yukarıda ifade edilen bu durum çerçevesinde, savunma sanayi sektöründe bilgi güvenliğinin sağlanabilmesi için Amerika Birleşik Devletleri-ABD Savunma Bakanlığı (DoD) savunma sanayi faaliyetlerinde asgari bilgi güvenliği şartlarını ortaya koymak amacıyla savunma sanayi tedarikçileri için “Cybersecurity Maturity Model Certification” (CMMC) adını verdiği bir uygulama oluşturmuştur [19].

“Cybersecurity Maturity Model Certification” (CMMC) Amerika Birleşik Devletleri Savunma Bakanlığının (DoD) yürütmekte olduğu savunma sanayi projelerinde bilgi güvenliği alt yapısını güçlendirmek için tedarikçilerinden gerçekleştirmesini beklediği ve modele ait gereksinimlerin uygulamanın kapsamına bağlı olarak ayrı ayrı olgunluk seviyeleri ile ifade edildiği bir bilgi güvenliği yönetimi uygulamasıdır [20].

İlk kez 2019 yılında duyurulan CMMC programı birçok bilgi güvenliği standardından faydalanılarak savunma sanayi sektörüne özel olarak hazırlanmıştır. Bu bakımdan hem yeni ve güncel olması hem de önemli bilgi güvenliği rehber ve standardına ait gereksinimleri sektöre özel derleyerek içeriğinde barındırması bakımından savunma sanayinde uygulanacak bilgi güvenliği yönetimi uygulamaları için önemli bir referans niteliği taşımaktadır [21].

Ülkemizde de özellikle son yıllarda siber saldırıların sayısı önemli ölçüde artmıştır. 2021 yılı verilerine bakıldığında yalnızca bu yıl içinde ülkemizin çeşitli kurum ve kuruluşlarının hedef olduğu 620 binin üzerinde kötü amaçlı yazılım saldırısı düzenlendiği görülmektedir [22].

Bu doğrultuda son yıllarda sürekli artan siber güvenlik tehditleri ve ülkemizin savunma sanayinin yüksek ihracat potansiyeli göz önünde bulundurulduğunda [23], çok yakın gelecekte hem ülkemizdeki yetkili otoritelerin buna benzer bir yapıyı kendi tedarikçileri için kurmasının gerekeceği hem de dünya savunma sanayi arenasında önemli oyuncular olan ülkemiz savunma sanayi kuruluşlarının ABD menşeili projelerde CMMC gereksinimleri ile karşı karşıya kalacağı ön görülmektedir.

Bu bakımdan ülkemizin savunma sanayi kuruluşlarının önceden tedbir alarak hazırlıklı olmaları ve mevcut bilgi güvenliği uygulamalarını yeni, kapsamlı ve savunma sanayine özel olan CMMC uygulamaları ile karşılaştırarak gerekli gördükleri güncellemeleri yapmalarının önem arz ettiği değerlendirilmektedir.

Yapılan bu çalışmanın amacı; milli savunma sanayi kuruluşlarında uluslararası standartlar çerçevesinde kullanılmakta olan mevcut siber güvenlik önlemlerini araştırmak, uygulamada yaygın olarak kullanılmakta olan bilgi güvenliği yönetimi uygulamasını belirleyerek ve gereksinimlerini CMMC gereksinimleri ile karşılaştırarak, CMMC süreçlerinin uygulamaya geçirilmesi ya da ülkemiz için benzer bir yapının geliştirilmesi durumunda eksikliklerin giderilmesinde kolaylık sağlayacak bir rehber ortaya koymaktır.

Dünya savunma sanayi istatistiklerine bakıldığında 2021 yılında toplam savunma harcamalarının 2 trilyon doları geçtiği ve bu harcamalarda en büyük paya ABD'nin sahip olduğu görülmektedir [24]. Bu verilere göre ABD açık ara dünyanın en büyük savunma sanayi kuruluşlarına ev sahipliği yapan ve dünyanın en büyük savunma sanayi bütçesine sahip olan ülkesidir.

Bu çalışma ile dünya savunma sanayinin lider ülkesi pozisyonunda olan ABD'nin savunma sanayi tedarikçileri için gerekli kıldığı ve görece çok yeni yürürlüğe girmiş olan siber güvenlik modelinin ülkemizde ilgili taraflarca daha iyi anlaşılması, konuyla ilgili genel

anlamda farkındalığın arttırılması ve muhtemel projelerde milli savuna sanayi kuruluşlarına gerekli olacak dönüşüm faaliyetlerinin hızlandırılması süreçlerine katkı sağlanabilecektir.

Yapılan çalışmada; ülkemizin en büyük milli savunma sanayi kuruluşlarından da bir kısmını içerisinde bulunduran farklı büyüklükte 6 kuruluş nezdinde yalnızca ulusal ve uluslararası nitelik taşıyan standartlar ve normlara bağlı bilgi güvenliği yönetimi uygulamaları araştırma kapsamına dahil edilmiştir.

Gereksinimlerin karşılaştırılması ve değerlendirilmesi için ise CMMC 'nin 2021 yılının sonunda duyurulan 2.0 versiyonu ile çalışma kapsamında yer alan savunma sanayi kuruluşlarında en yaygın şekilde kullanıldığı görülen ISO/IEC 27001 standardının milli standart kuruluşu Türk Standardları Enstitüsü tarafından en son tercüme edilerek Türk Standardı olarak kabul edilen Mayıs 2017 versiyonu esas alınmıştır.

Yine bu aşamada ISO/IEC 27001 Ek A'da belirtilen gereksinimlerin ayrıntılı olarak açıklanması ve uygulama örneklerinin belirtildiği ISO/IEC 27002 "Bilgi teknolojisi- Güvenlik teknikleri- Bilgi güvenliği kontrolleri" standardının Mayıs 2017 versiyonundan da faydalanılmıştır.

Çalışmanın yapıldığı tarihte CMMC v2.0 kapsamında Seviye 3 gereksinimleri henüz oluşturulmamış olduğundan [25], yalnızca Seviye 1 ve Seviye 2'ye ait gereksinimleri ifade eden uygulamalar çalışma kapsamında değerlendirilmiştir.

Bu doğrultuda, çalışma içeriğinde yer alan ikinci bölümde; "ISO/IEC 27001, CMMC ve DÜNYADAKİ DİĞER UYGULAMALAR" başlığı altında; ilgili uygulamalara ait gelişim süreci ve genel özellikler, kapsam, gereksinimler ve belgelendirme konuları ayrı ayrı ele alınarak dünyadaki diğer uygulamalar hakkında bilgi verilmiş, üçüncü bölümde "YÖNTEM" başlığı altında; çalışmada kullanılan araştırma evreni, veri toplama araçları ve değerlendirme modeli hakkında bilgi verilmiş, dördüncü bölümde "ARAŞTIRMA BULGULARI" başlığı altında; kapsamda yer alan savunma sanayi kuruluşlarına ait mevcut bilgi güvenliği uygulamaları, son bir yıl içinde yaygın olan siber saldırı türlerine maruz kalıp kalmadıkları ve CMMC modeline dair farkındalıkları ile uzman görüşleri doğrultusunda oluşturulan eşleştirme tablolarından elde verilere yer verilmiş, beşinci ve son bölümde ise, "SONUÇ VE ÖNERİLER" başlığı altında; araştırma bulgularına ait veriler doğrultusunda

kuruluşların uyguladıkları ISO/IEC 27001 standardı tedbirleri ile hali hazırda CMMC gereksinimlerinin ne kadarını karşıladıkları değerlendirilerek yapılması gerekenler hususunda öneriler belirtilmiştir.

2. ISO/IEC 27001, CMMC ve DÜNYADAKİ DİĞER UYGULAMALAR

Bu başlık altında ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, Siber Güvenlik Olgunluk Modeli (CMMC) ve dünyadaki diğer uygulamalar hakkında bilgi verilmiştir.

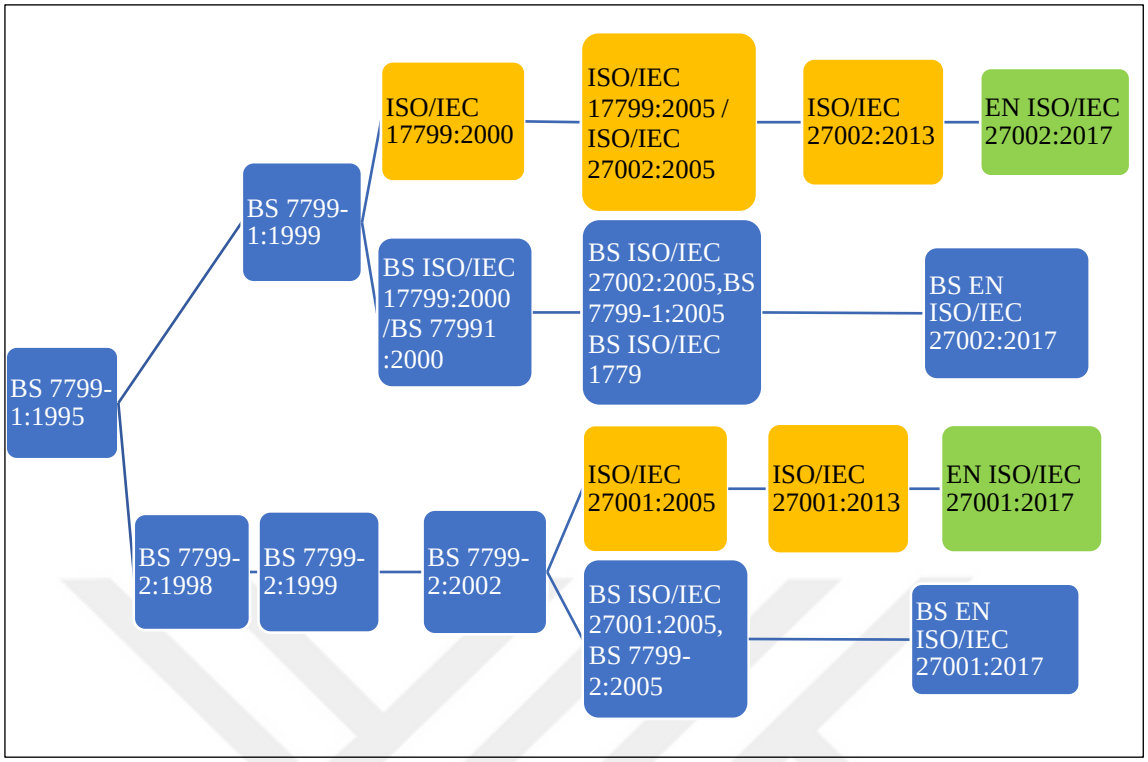
2.1. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

Bu başlık altında ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile ilgili olarak gelişim süreci ve genel özellikler, kapsam, gereksinimler ve belgelendirme konularında bilgi verilmiştir.

2.1.1. Gelişim süreci ve genel özellikler

1990'lı yıllara kadar bilgi sistemlerine yönelik tehditlere karşı tedbir alınması sorumluluğu yalnızca organizasyonların bilgi teknolojileri birimlerinde iken, BSI tarafından 1995 yılında yayınlanan BS 7799-1 standardında ön görülen "Bilgi Güvenliği Yönetim Sistemi" kavramı ile birlikte bilgi güvenliği ile ilgili görevler bilgi teknolojileri birimlerine ek olarak organizasyonun bütününe yayılmıştır [26].

Bununla birlikte burada bahsedilen BS 7799-1 standardı, Şekil 2.1.'de gösterilen gelişim basamaklarından da görüleceği üzere, ISO (International Organization for Standardization) tarafından yayınlanan ve faaliyet konularından bağımsız şekilde kuruluşlarda oluşturulabilecek bir bilgi güvenliği yönetim sisteminin sağlaması beklenen asgari şartları tanımlayan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı'nın da alt yapısını oluşturmuştur [27].



Şekil 2.1. EN ISO/IEC 27001 gelişim aşamaları

ISO'nun bünyesinde yer alan Bilgi Teknolojileri Ortak Teknik Komitesi JTC1'e ait (Joint Technical Committee 1) Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruma Alt Komitesi SC27 (Sub Committee 27), 2005 yılında ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardının ilk versiyonunu hazırlamıştır. [28].

CEN (European Committee for Standardization) tarafından 2017 yılında yayınlanan EN ISO/IEC 27001:2017 standardı ise ISO/IEC 27001:2013 standardının yayınlanan en son revizyonudur [29].

Bununla birlikte gereksinimler yönünden bakıldığında, ISO tarafından yayınlanan bir önceki versiyon ile CEN tarafından yayınlanan bu son versiyon arasında herhangi bir fark bulunmamaktadır.

Ayrıca standardın CEN tarafından yayınlanan son versiyonu 2017 yılında milli standart kuruluşu TSE tarafından "Türk Standardı" olarak kabul edilmiş olup, 2018 yılında dilimize çevrilerek TS EN ISO/IEC 27001 "Bilgi teknolojisi- Güvenlik teknikleri- Bilgi güvenliği yönetim sistemleri- Gereksinimler" adıyla ülkemizde de yayınlanmıştır [30].

EN ISO/IEC 27001:2017 standardındaki terimlerin Türkçe karşılıkları için TS EN ISO/IEC 27001:2017 standardı kullanılmıştır.

2.1.2. Kapsam

İşletmenin bağlamına uygun bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, bakımı ve sürekli geliştirilmesi için gereksinimler EN ISO/IEC 27001:2017 standardı kapsamında tanımlanmıştır. Yukarıda sözü edilen gereksinimler, standardın yapısı gereği geniş bir kapsama ve genel özelliklere sahip olacak ve tüm sektörleri uygulanabilecek şekilde oluşturulmuştur.

Standart içeriğinde gereksinimler ile ilgili hususlar 4 ila 10. Maddeler altında belirtilmektedir. Bununla beraber 6. Madde ile tanımlanan "Planlama" başlığı altındaki gereksinimlerin eksiksiz olarak uygulanmasının sağlanabilmesi için standart ekinde 18 ana başlık altında ifade edilen toplam 112 adet kontrol şartı bulunmaktadır.

Bunun yanında normal şartlar altında standardın kuruluşlar tarafından uygulanması için herhangi bir zorunluluk bulunmamaktadır. Ancak sözleşme, mevzuat gibi bir kısım özel şartlar nedeniyle kuruluşlarda standardın uygulanmasının zorunlu tutulduğu durumlar ortaya çıkabilmektedir.

EN ISO/IEC 27001:2017 standardı ile ilgili bir diğer önemli husus ise, standardın Avrupa'da 34 ülkenin üyesi olduğu CEN [31] ile dünya çapında 167 ülkenin üyesi olduğu bağımsız bir organizasyon olan ISO [32] tarafından kabul edilmiş olmasıdır.

Bu sayede standart, uluslararası ölçekte en fazla kabul gören bilgi güvenliği yönetim sistemi standardı olma özelliğine de sahip olmaktadır [33].

2.1.3. Gereksinimler

Yukarıda ifade edildiği üzere standardın tanımlamış olduğu bilgi güvenliği yönetim sisteminin sahip olması beklenen asgari gereksinimler standart ana dokümanında ve ekinde maddeler halinde ifade edilmektedir.

Söz konusu gereksinimlere yer verilen standart dokümanına ulaşabilmek için kuruluşların ücreti mukabilinde dokümanı fiziksel veya dijital ortamlardan satın almaları gerekmektedir. Bu kapsamda kuruluşlar standarda ait Türkçe ve İngilizce dillerindeki fiziksel veya dijital dokümanları TSE'den satın alabilirken [34], Fransızca gibi diğer yabancı dillerdeki dokümanlara ise ISO [35] ve CEN 'in [36] internet siteleri üzerinden ücreti karşılığında dijital olarak ulaşılabilmektedir.

Standart içeriğine bakıldığında bilgi güvenliği yönetim sistemi ile ilgili olarak;

- Sistemin kurulması,
- Uygulamaya geçirilmesi,
- Sürdürülebilirliğinin sağlanması,
- Sürekli iyileştirilmesi,

konularına dair gereksinimlerin ve diğer hususların Çizelge 2.1. ile gösterilen toplam 11 ana başlık altında ifade edildiği görülmektedir.

Çizelge 2.1. İçerik ana başlıkları

No.	**EN ISO/IEC 27001:2017**	**TS EN ISO/IEC 27001**
0	Introduction	Giriş
1	Scope	Kapsam
2	Normative references	Atıf yapılan standart ve/veya dokümanlar
3	Terms and definitions	Terimler ve tarifler
4	Context of the organization	Kuruluş Bağlamı
5	Leadership	Liderlik
6	Planning	Planlama
7	Support	Destek

Çizelge 2.2.(devam) İçerik ana başlıkları

8	Operation	İşletim
9	Performance evaluation	Performans Değerlendirme
10	Improvement	İyileştirme

Buradaki başlıklar, ISO tarafından "yüksek seviyeli yapı" HLS (High Level Structure) gereğince yönetim sistemi standartları için oluşturulan ve ISO/IEC 27001 standardı dışında diğer yönetim sistemi standartlarında da aynı şekilde kullanılan genel ifadelerden meydana gelmektedir [37].

Buradaki "yüksek seviyeli yapı" uyarınca standart kapsamında sağlanması gereken gereksinimler 4 ila 10. Maddede belirtilen başlıklar altında tanımlanmaktadır.

Bu maddeler altında ifade edilmiş olan gereksinimler, herhangi bir bilgi türüne, seviyeye veya sektöre bağlı kriter olmaksızın her sektördeki ve her tipteki kuruluşa bünyesinde bulundurduğu bilgi varlığının türünden bağımsız olarak uygulanabilecek şekilde hazırlanmıştır.

Bu doğrultuda kuruluşlar ISO/IEC 27001 standardına göre gereksinimleri sağlayarak oluşturduğu bilgi güvenliği yönetim sistemini belgelendirilebilmek için;

- "4. Kuruluş Bağlamı" başlığı uyarınca amaçları doğrultusunda bilgi güvenliği yönetim sisteminin hedeflerini etkileyebilecek iç ve dış hususları belirleme ve kapsamını oluşturma,
- "5. Liderlik" başlığı uyarınca üst yönetim bilgi güvenliği yönetim sistemi ile ilgili desteğini göstermeli, bilgi güvenliği politikasını oluşturma ve kurumsal rolleri tanımlama,
- "6. Planlama" başlığı uyarınca risk ve fırsatları belirlemeli, riskleri değerlendirmeli, risk işleme sürecini tanımlama ve bilgi güvenliği yönetim sisteminin amaçlarını belirleyerek nasıl başarılacağını planlama,

- “7. Destek” başlığı uyarınca bilgi güvenliği yönetim sistemi için kaynakları, yeterlilikleri tanımlama, farkındalık, iletişim ve yazılı bilgiye ilişkin kontrolleri sağlama,
- “8. İşletim” başlığı uyarınca bilgi güvenliği yönetim sisteminin planlanan şekilde işletimini sağlama,
- “9. Performans Değerlendirme” başlığı uyarınca izleme, ölçme, analiz-değerlendirme, iç tetkik, yönetim gözden geçirme faaliyetlerini gerçekleştirme,
- “10. İyileştirme” başlığı uyarınca da uygunsuzluk olması durumunda düzeltici faaliyet gerçekleştirme ve bilgi güvenliği yönetim sistemini sürekli iyileştirme,

faaliyetlerini etkin, sürdürülebilir ve sürekli iyileştirmeye açık olacak şekilde gerçekleştirebilmelidir [38].

Bu hususlarla ilgili olarak standart ekinde yer alan tabloda ise, “6. Planlama” maddesinde bulunan ve bilgi güvenliğine yönelik belirlenen risk işleme faaliyetlerinin gerçekleştirilmesi için referans olarak kullanılması gereken kontrol amaçları ile kontroller, doğrudan ISO/IEC 27002:2013 standardı içeriğindeki madde 5 ila 18. Maddelerinde belirtilen ifadeler referans alınarak Çizelge 2.2.’de gösterildiği üzere listelenmiştir [39].

Çizelge 2.3. Kontrol amaçları ve kontroller

No.	**ISO/IEC 27002:2013**	**TS EN ISO/IEC 27001 Ek A**	**Kontrol Şartı Sayısı**
5	Information security policies	Bilgi güvenliği politikaları	-
5.1	Management direction for information security	Bilgi güvenliği için yönetimin yönlendirmesi	2
6	Organization of information security	Bilgi güvenliğinin organizasyonu	-
6.1	Internal organization	İç organizasyon	5
6.2	Mobile devices and teleworking	Mobil cihazlar ve uzaktan çalışma	2

Çizelge 2.2.(devam) Kontrol amaçları ve kontroller

7	Human resource security	İnsan kaynakları güvenliği	-
7.1	Prior to employment	İstihdam öncesi	2
7.2	During employment	Çalışma esnasında	3
7.3	Termination and change of employment	İstihdamın sonlandırılması veya değiştirilmesi	1
8	Asset management	Varlık yönetimi	-
8.1	Responsibility for assets	Varlıkların sorumluluğu	4
8.2	Information classification	Bilgi sınıflandırma	3
8.3	Media handling	Ortam işleme	3
9	Access control	Erişim kontrolü	-
9.1	Business requirements of access control	Erişim kontrolünün iş gereklilikleri	2
9.2	User access management	Kullanıcı erişim yönetimi	6
9.3	User responsibilities	Kullanıcı sorumlulukları	1
9.4	System and application access control	Sistem ve uygulama erişim kontrolü	5
10	Cryptography	Kriptografi	-
10.1	Cryptographic controls	Kriptografik kontroller	2
11	Physical and environmental security	Fiziksel ve çevresel güvenlik	-
11.1	Secure areas	Güvenli alanlar	6

Çizelge 2.2.(devam) Kontrol amaçları ve kontroller

11.2	Equipment	Teçhizat	9
12	Operations security	İşletim güvenliği	-
12.1	Operational procedures and responsibilities	İşletim prosedürleri ve sorumlulukları	4
12.2	Protection from malware	Kötücül yazılımlardan koruma	1
12.3	Backup	Yedekleme	1
12.4	Logging and monitoring	Kaydetme ve izleme	4
12.5	Control of operational software	İşletimsel yazılımın kontrolü	1
12.6	Technical vulnerability management	Tekniklik açıklıkların yönetilmesi	2
12.7	Information systems audit considerations	Bilgi sistemleri tetkik hususları	1
13	Communications security	Haberleşme güvenliği	-
13.1	Network security management	Ağ güvenliği yönetimi	3
13.2	Information transfer	Bilgi transferi	4
14	System acquisition, development, and maintenance	Sistem edinimi, geliştirme ve bakımı	-
14.1	Security requirements of information systems	Bilgi sistemlerinin güvenlik gereksinimleri	3

Çizelge 2.2.(devam) Kontrol amaçları ve kontroller

14.2	Security in development and support processes	Geliştirme ve destek proseslerinde güvenlik	9
14.3	Test data	Test verisi	1
15	Supplier relationships	Tedarikçi ilişkileri	-
15.1	Information security in supplier relationships	Tedarikçi ilişkilerinde bilgi güvenliği	3
15.2	Supplier service delivery management	Tedarikçi hizmetleri sağlama yönetimi	2
16	Information security incident management	Bilgi güvenliği ihlal olayı yönetimi	-
16.1	Management of information security incidents and improvements	Bilgi güvenliği ihlal olaylarının ve iyileştirmelerin yönetimi	7
17	Information security aspects of business continuity management	İş sürekliliği yönetiminin bilgi güvenliği hususları	-
17.1	Information security continuity	Bilgi güvenliği sürekliliği	3
17.2	Redundancies	Yedek fazlalıklar	1
18	Compliance	Uyum	-
18.1	Compliance with legal and contractual requirements	Yasal ve sözleşmeye tabi gereksinimlere uyum	5
18.2	Information security reviews	Bilgi güvenliği gözden geçirmeleri	3

Çizelgede belirtilen hususlar çerçevesinde kuruluşlar EN ISO/IEC 27001:2017 Ek A'da verilen listede bulunan;

- "A.5 Politika" maddesinde bulunan kontrol şartlarına göre kuruluş bilgi güvenliği politikalarını belirleme ve gözden geçirme,
- "A.6 Bilgi güvenliği organizasyonu" maddesinde bulunan kontrol şartlarına göre bilgi güvenliği operasyonunu başlatma ve kontrolünü sağlama,
- "A.7 İnsan kaynakları güvenliği" maddesinde bulunan kontrol şartlarına göre çalışanlara yönelik bilgi güvenliği tedbirlerini planlama,
- "A.8 Varlık yönetimi" maddesinde bulunan kontrol şartlarına göre kuruluşun varlıklarını tespit ederek sorumlulukları tanımlama,
- "A.9 Erişim kontrolü" maddesinde bulunan kontrol şartlarına göre bilgi ve bilgi işleme erişimini kısıtlama,
- "A.10 Kriptografi" maddesinde bulunan kontrol şartlarına göre bilginin gizliliği, orijinalliği ve bütünlüğünün korunması amacıyla uygun kriptolojik yöntemin kullanılmasını sağlama,
- "A.11 Fiziksel ve çevresel güvenlik" maddesinde bulunan kontrol şartlarına göre bilgi ve bilgi işleme olanaklarına yetkisiz fiziksel erişimi engelleme,
- "A.12 İşletim güvenliği" maddesinde bulunan kontrol şartlarına göre bilgi işleme olanaklarının güvenli işletilmesini sağlama,
- "A.13 Haberleşme güvenliği" maddesinde bulunan kontrol şartlarına göre ağda yer alan bilgi işleme ve iletişim olanaklarının güvenliğini sağlama,
- "A.14 Sistem temini, geliştirme ve bakımı" maddesinde bulunan kontrol şartlarına göre bilgi sistemlerinin yaşam döngüleri boyunca bilgi güvenliği entegre etme,
- "A.15 Tedarikçi ilişkileri" maddesinde bulunan kontrol şartlarına göre tedarikçileri ile iletişiminde bilgi varlıklarının güvenliğini sağlama,
- "A.16 Bilgi güvenliği ihlal yönetimi" maddesinde bulunan kontrol şartlarına göre bilgi güvenliği ihlali olaylarında planlı, tutarlı ve etkili yaklaşımı sağlama,
- "A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları" maddesinde bulunan kontrol şartlarına göre iş sürekliliği yönetim sisteminde bilgi güvenliği sürekliliğini sağlamak için gerekli tedbirleri alma,
- "A.18 Uyum" maddesinde bulunan kontrol şartlarına göre bilgi güvenliği yönetim sistemini yasal ve sözleşme şartlarına uygun olacak şekilde düzenleme ve belirli aralıklarla gözden geçirme,

faaliyetlerinin standartta yer alan “6. Planlama” maddesinde yer alan esaslara uygun olacak şekilde gerçekleştirilmesini sağlamalıdır.

2.1.4. Belgelendirme

ISO/IEC 27001 standardı kapsamında belgelendirmeyle ilgili hususlara bakıldığında, uluslararası bağımsız standardizasyon kuruluşu olan ISO’nun yapısı ve kuruluş amaçları dolayısıyla belgelendirme faaliyeti yapmadığı görülmektedir [40].

Buna göre ISO standartları kapsamında belgelendirme hizmeti bu amaçla kurulmuş bağımsız belgelendirme kuruluşları tarafından gerçekleştirilmekte olup, EN ISO/IEC 27001 standardı gereksinimlerine göre bilgi güvenliği yönetim sistemini oluşturmuş olan kuruluşların üçüncü taraf denetimlerinin gerçekleştirilmesi ve oluşturmuş oldukları sistemlerinin belgelendirilmesi için bu kuruluşlara başvurmaları gerekmektedir.

Bu süreçte başvurulacak belgelendirme kuruluşlarının, uygunluk değerlendirme faaliyetleri kapsamında yönetim sistemlerinin tetkikini ve belgelendirmesini sağlayan kuruluşlar için şartların tanımlandığı (TS) (EN) ISO/IEC 17021-1:2015 standardına göre IAF (International Accreditation Forum) üyesi bir akreditasyon kuruluşundan akredite olması belgenin ulusal ve uluslararası geçerliliğinin güvence altına alınması bakımından önem arz etmektedir [41].

2.2. Siber Güvenlik Olgunluk Modeli Sertifikasyonu (CMMC)

Bu başlık altında Siber Güvenlik Olgunluk Modeli Sertifikasyonu (CMMC) ile ilgili olarak gelişim süreci ve genel özellikler, kapsam, gereksinimler ve belgelendirme konularında bilgi verilmiştir.

2.2.1. Gelişim süreci ve genel özellikler

Siber Güvenlik Olgunluk Modeli Sertifikasyonu (Cybersecurity Maturity Model Certification-CMMC) Amerika Birleşik Devletleri Savunma Bakanlığı’na (Department of Defense-DoD) ait savunma projelerinde tedarikçi olarak görev alan kuruluşların bilgi güvenliği yönetimi alt yapısını kontrol altında tutmak için bu kuruluşlar tarafından gerçekleştirmesini beklediği ve modele kapsamında gereksinimleri uygulamaya bağlı olarak farklı seviyeler ile tanımlanmış bir bilgi güvenliği yönetimi modelidir [42].

CMMC, ABD Savunma Bakanlığı'na, bir savunma sanayi yüklenicisinin, çok katmanlı bir tedarik zincirinde alt yüklenicilerine bilgi akışını hesaba katarak, riskle orantılı bir düzeyde tanımlı bilgi alt yapısını yeterince koruyabileceğine dair güvence sağlamak üzere tasarlanmıştır.

Günümüzde en büyük savunma sanayi olan ve ABD'deki adıyla "Defense Industrial Base-DIB Sector" olarak bilinen ABD savunma sanayi sektörü, ABD'nin askeri ihtiyaçlarını karşılamak için silah sistemleri ile bunlara ait alt sistemlerin ve bileşenlerin Ar-Ge faaliyetleri ile birlikte tasarım, üretim, teslimat ve bakımını da gerçekleştiren dünya çapında faaliyet gösteren karmaşık bir endüstriyel yapıdan meydana gelmektedir [43].

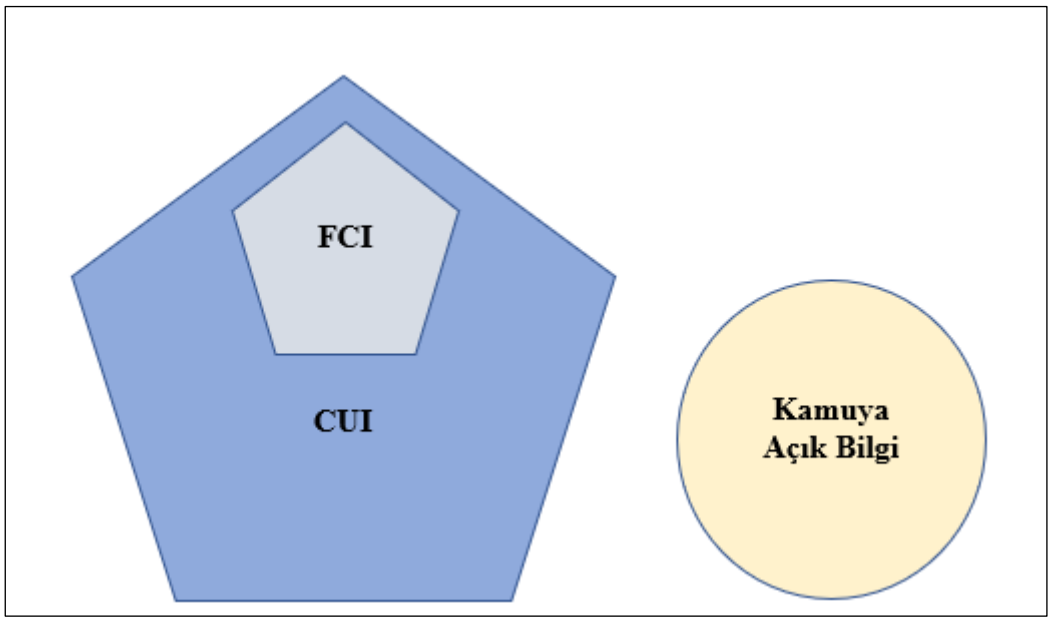
ABD Savunma sanayi sektörü, ABD Savunma Bakanlığı ile sözleşmeli olarak faaliyet gösteren ve birçok ülkede bulunan üretim varlıkları ile yerli ve yabancı kuruluşları da içeren 100.000'den fazla savunma sanayi şirketi ve bunların taşeronlarından oluşmakta ve askeri operasyonları harekete geçirmek, konuşlandırmak ve sürdürmek için gerekli olan ürün ve hizmetleri sağlamaktadır. Bununla birlikte sektör ABD Savunma Bakanlığı'nın askeri operasyonel gereksinimleri karşılamak için kullandığı güç, iletişim, ulaşım veya kamu hizmetleri gibi hizmet sağlayıcılarının ticari altyapısını içermemektedir [44].

ABD savunma sanayi sektörünün bu denli büyük ve geniş kapsamlı olması nedeniyle ABD Savunma Bakanlığı tarafından, savunma sanayi sektörü kuruluşları bünyesinde yer alan ve "Kontrollü Gizli Olmayan Bilgi" (CUI- Controlled Unclassified Information) ve "Federal Sözleşme Bilgisi" (FCI- Federal Contract Information) olarak tanımlanmış bilgilerin güvenliğinin gereken ölçüde sağlanamaması halinde ulusal güvenlik bağlamında büyük risklerin ortaya çıkacağı değerlendirilmektedir [45].

Burada ifade edilen "Kontrollü Gizli Olmayan Bilgi-CUI"; Yürütme Emri 13526-Gizli Ulusal Güvenlik Bilgileri (Executive Order 13526-Classified National Security Information) veya Atom Enerjisi Yasası (Atomic Energy Act) kapsamında gizli olarak tanımlanmış olanlar hariç tutulmak üzere ABD hükümetinin oluşturduğu veya bünyesinde bulunan veya bir kuruluşun ABD hükümeti adına veya ABD hükümeti için oluşturduğu veya bünyesinde bulundurduğu gizli olmayan fakat yürürlükteki kanunlar, regülasyonlar ve ABD hükümeti genelindeki politikalar uyarınca ve bunlarla tutarlı olmak kaydıyla güvenlik veya yayımlama kontrolü gerektiren türdeki bilgiler olarak tanımlanmaktadır [46].

Yine yukarıda sözü edilmiş olan “Federal Sözleşme Bilgisi-FCI” ise; bir ürün veya hizmetin ABD hükümetine teslimi veya geliştirilmesi için yapılan bir sözleşme dahilinde ABD hükümeti tarafından sağlanan veya ABD hükümeti için oluşturulan, kamuya açıklanmayacak türdeki bilgileri ifade etmektedir [47].

İki ayrı şekilde tanımlanan bilgi türünün birbirleriyle ve halka açık bilgi ile olan ilişkileri Şekil 2.2.’de gösterilmiştir [48].



Şekil 2.2. Sözleşme uyarınca toplanan, oluşturulan ve alınan bilgiler.

Buradan da anlaşılacağı üzere FCI, ABD Savunma Bakanlığı ile savunma sanayi sektörü kuruluşları arasında sözleşmenin yapılması ile birlikte halka açıklanması ön görülmeyen tüm bilgileri kapsamakta iken CUI, bunlar içerisinde ayrıca koruma tedbirleriyle korunması gerekli olan bilgileri ifade etmektedir.

Söz konusu tanımlar kapsamındaki bilgilere örnek vermek gerekirse;

- Bir sözleşme kapsamında bulunan ve kamuya açıklanmayacak proses dokümanları, performans raporları, program ve organizasyon tabloları FCI [49],
- Yasalarla korunan materyaller, sağlıkla ilişkili dokümanlar, teknik çizimler ve planlar, fikri mülkiyet kapsamındaki bilgiler ile askeri düzeyde teknoloji ile uğraşan veya özellikle askeri kullanım için ürünler geliştiren her şirket için önem

arz eden Uluslararası Silah Ticareti Düzenlemeleri (International Traffic in Arms Regulations – ITAR) [50] kapsamındaki ürünler ve belgeler CUI [51],

olarak tanımlanmaktadır.

Bu doğrultuda yukarıda tanımlanmış türlere ait bilgi varlıklarının güvenliğinin sağlanamaması riskini düşürmek ve tedbirleri kontrol altında tutmak amacıyla ABD Savunma Bakanlığı'nın bir alt organizasyonu olan Tedarik ve İdame Ofisi (The Office of the Under Secretary of Defense for Acquisition and Sustainment- OUSD(A&S)), gizli olarak sınıflandırılmayan iletişim alt yapılarında bilgi güvenliğini sağlamak için üniversitelere bağlı araştırma merkezleri (UARC), federal olarak finanse edilen ar-ge merkezleri (FFRDC) ve savunma sanayi sektörü kuruluşları gibi ABD Savunma Bakanlığı paydaşları ile birtakım çalışmalar yürütmüş ve bu çalışmaların neticesinde, Çizelge 2.3. ile en çok kullanılanları belirtilen bilgi güvenliği rehber ve standartlarından da faydalanarak, ortak bilgi güvenliği gereksinimlerini bir çerçevede ifade etmek amacıyla CMMC adı verilen bilgi güvenliği yönetim modelini geliştirmiştir [52].

Çizelge 2.4. CMMC modelinde yararlanılan başlıca kaynaklar

Standart/Referans No.	**Başlık**	**Kuruluş**
NIST SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	NIST (National Institute of Standards and Technology)
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations	NIST
NAS9933	Critical Security Controls for Effective Capability in Cyber Defense	AIA (Aerospace Industry Association)

Çizelge 2.3.(devam) CMMC modelinde yararlanılan başlıca kaynaklar

CERT RMM v1.2	Resilience Management Model	CERT (Computer Emergency Response Team), Carnegie Mellon University
FAR 52.204-21	Basic Safeguarding of Covered Contractor Information Systems.	(DoD) The Department of Defense
DFARS 252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting.	DoD
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	NIST

Yukarıda sözü edilen CMMC'nin ilk versiyonu 31 Ocak 2020 tarihinde ABD Savunma Bakanlığı tarafından yayınlanmıştır. Sonrasında ise fonksiyonel olmayan değişiklikler yapılarak [53] mevcut versiyon CMMC v1.02 olarak güncellenmiştir.

Bir sonraki versiyon olan CMMC v2.0 ise 4 Kasım 2021 tarihinde duyurulmuş olup bir önceki versiyona göre oldukça önemli değişiklikler içermektedir.

Bu versiyonda temel de bir öncekinden farklı olarak;

- Daha önce 5 olan seviye sayısı 3'e indirilmiş,
- Daha önce var olan süreçler ve CMMC modeline özel uygulamalar kaldırılmış,
- CMMC Seviye 1 ve bir kısım Seviye 2 uygulamaları için yıllık periyotta kuruluşların kendilerini değerlendirmelerine izin verilmiştir [54].

2.2.2. Kapsam

CMMC ‘nin amacı, savunma sanayi sektörü kuruluşlarında, çok katmanlı bir tedarik zincirinde alt yüklenicilere bilgi akışını da hesaba katarak, yukarıda tanımlanan kontrollü gizli olmayan bilgilerin (CUI) ve federal sözleşme bilgilerinin (FCI) korunması için uygulanacak bilgi güvenliği tedbirlerine ait bir çerçeve ortaya koymaktır.

Böylece ilgili savunma sanayi kuruluşunun hassas bilgileri yeteri kadar koruyabileceği konusunda ABD Savunma Bakanlığı’na daha fazla güvence sağlanması hedeflenmektedir [55].

Yukarıda belirtilen amaç ve hedef doğrultusunda CMMC v2.0 kapsamında, 3 ayrı olgunluk seviyesi (maturity level), 14 ayrı alan (domain) ve bunlara bağlı olarak şu an için yalnızca Seviye 1 ve Seviye 2 için ayrı ayrı tanımlanan toplam 110 uygulama (practice) yer almaktadır.

CMMC uygulamalarının sektör tarafından kullanımına ilişkin olarak ise “Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements” (DFARS Case 2019-D041) 30/11/2020 tarihinden itibaren yürürlüğe girmek üzere 19/09/2020 tarihinde ABD resmî gazetesi olan “Federal Register” ‘da yayınlanmıştır.

CMMC v2.0 öncesinde yayınlanmış olan bu mevzuat uyarınca, ABD Savunma Bakanlığı’na hizmet veren yüklenici/tedarikçi ve bunların alt organizasyonlarının 1/10/2025 tarihi itibariyle bilgi güvenliği yönetimi alt yapılarını CMMC gereksinimlerine uygun hale getirmeleri gerekmektedir.

Buna göre bu tarihten sonra projede teklif sahibi veya yüklenici/tedarikçi, ABD Savunma Bakanlığı’nca gerekli görülen CMMC uygulama seviyesi kapsamında yürürlükte bir CMMC uygunluk sertifikasına sahip değilse ABD Savunma Bakanlığı ihalelerine katılamayacaktır.

Buna karşın 4 Kasım 2021 tarihinde CMMC v2.0’ın duyurulması ile birlikte bu zorunlu uygulama tarihi CMMC v2.0’ın 9 ila 24 ay süreceği öngörülen mevzuat süreçlerinin tamamlanmasına dek ertelenmiştir [56].

Uygulamayla ilgili olan bu hususlara ek olarak, bahsedilen zorunlu uygulama tarihi itibariyle gerekli görülen seviye için CMMC sertifikasyon gereksinimlerinin, aktarılan bilgi varlıklarının önemine ve hassasiyetine bağlı olarak, yüklenici/tedarikçi alt organizasyonlarında yer alan her kuruluş tarafından da gerçekleştirilmesi beklenmektedir [57].

Buradan da anlaşılacağı üzere CMMC uygulamaları her ne kadar mevzuatı itibariyle ABD'ye ait ulusal nitelik taşıyor olsa da uygulama tarihinden itibaren dünya genelinde ABD Savunma Bakanlığı'na yüklenici/tedarikçi olarak hizmete veren tüm savunma sanayi kuruluşları ve onların alt organizasyonları için CMMC gerekliliklerinin sağlanmasının zorunlu olacağı değerlendirilmektedir.

2.2.3. Gereksinimler

CMMC, yukarıda bahsedilen bilgi güvenliği yönetim sistemi standartlarından farklı olarak resmi bir devlet kuruluşu tarafından oluşturulmuştur. Bu sebepten dolayı CMMC modeline ait kılavuz, rehber ve çerçeve dokümanı olan Cybersecurity Maturity Model Certification CMMC Model Overview Version 2.0 December 2021 (ModelOverview_V2.0_FINAL2_20211202_508) güncel hali ABD Savunma Bakanlığı alt kuruluşu olan Tedarik ve İdame Ofisi'ne (The Office of the Under Secretary of Defense for Acquisition and Sustainment- OUSD(A&S)) ait internet sitesinde ücretsiz olarak kullanıma açık şekilde yayınlanmaktadır [58].

Her ne kadar CMMC v2.0'de siber güvenlik olgunluk modeli 3 ayrı seviyede ele alınmış olsa da hali hazırda CMMC v2.0 hazırlık süreci tamamlanmadığından söz konusu ana dokümanda yalnızca seviye 1 ve seviye 2'ye ait uygulamalar yer almaktadır.

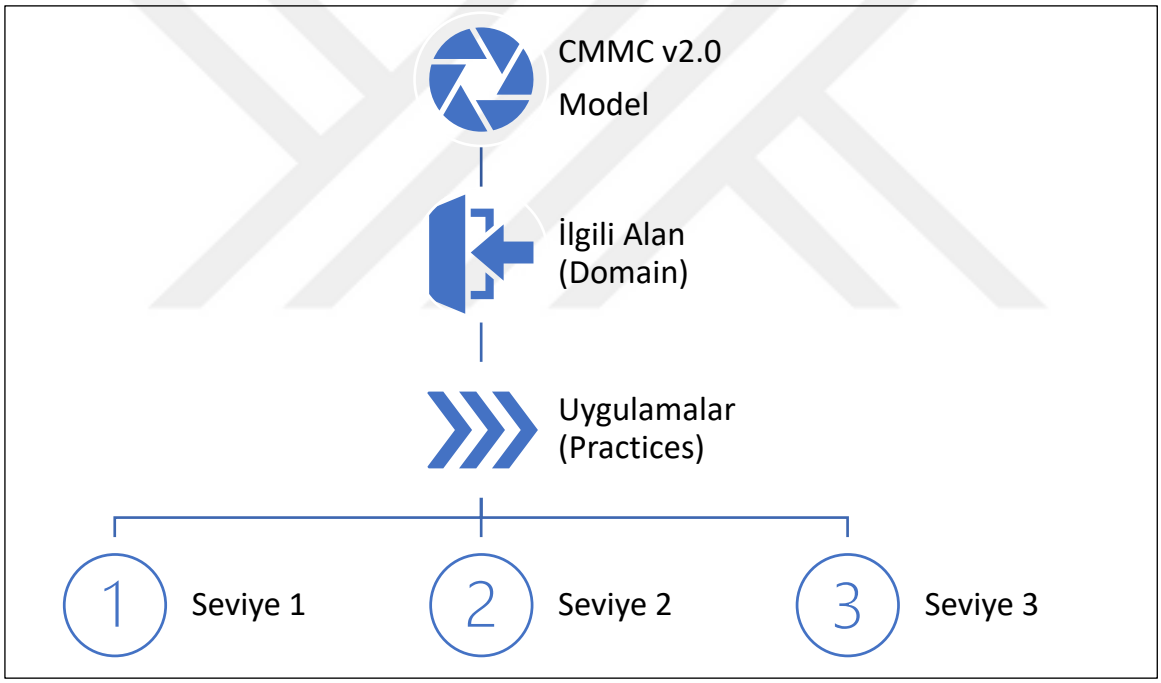
Daha önce CMMC v1.02'de kullanılan ve burada bahsedilen seviyeler bağlamında olgunluk yaklaşımı; kuruluşların iş süreçlerini yönetmedeki performanslarını değerlendirmek için birtakım kriterlere haiz ardışık seviyelerinden oluşan bir yaklaşımdır [59].

Buna göre bu seviyelerin her biri için CMMC kılavuz dokümanında, koruma gerektiren ve risk altında olan bilgi varlıklarının türüne ve önemine göre ayrı uygulamalara yer verilmektedir [60]. Örneğin, kılavuz dokümanda FCI türü bilgi varlıkları için temel seviye,

CUI türü bilgi varlıkları için ise daha ileri seviye güvenlik gereksinimlerinin yer aldığı görülmektedir.

Buna bağlı olarak savunma sanayi kuruluşları, kendi organizasyon yapıları içerisinde farklı bilgi türlerini işleyen farklı birimlere sahipse, CMMC gereksinimlerine bağlı uygulamaları birimleri bazında farklı seviyelerde gerçekleştirebilir veya bir kısım birimleri CMMC uygulamaları kapsamı dışında da bırakabilir.

CMMC v2.0 modeli çerçevesinde gereksinimleri ifade eden "uygulamalar" Şekil 2.3.'te gösterildiği üzere belirli sayıda "alan" içerisinde tanımlanarak 3 ayrı olgunluk seviyesine dağıtılmıştır.



Şekil 2.3. CMMC çerçeve modeli

Bu 3 ayrı uygulama seviyesinin tanımları, her seviye içerisinde yer alan uygulama sayıları ve denetim metodu Şekil 2.4. ile gösterilmiştir.



Şekil 2.4. CMMC Seviye tanımları, uygulama sayıları ve denetim metodu

CMMC modeli ana dokümanı içerisinde NIST SP 800-171'den faydalanılarak oluşturulan toplam 14 "alan" ve bunlara bağlı olarak 2 ayrı seviyede ifade edilen toplam 110 adet "uygulama" bulunmaktadır. Söz konusu alanlar ve bunlara bağlı tanımlanan uygulamalar Çizelge 2.4.'te gösterilmiştir.

Çizelge 2.5. CMMC modelinde yer alan alanlar ve uygulama sayıları

Alan Adı	**Uygulama Sayıları**	
	Seviye 1	**Seviye 2**
Erişim Kontrolü (AC)	4	18
Farkındalık ve eğitim (AT)	0	3
Denetim ve Hesap Verebilirlik (AU)	0	9
Konfigürasyon Yönetimi (CM)	0	9
Tanımlama ve Doğrulama (IA)	2	9

Çizelge 2.4.(devam) CMMC modelinde yer alan alanlar ve uygulama sayıları

Olay Müdahalesi (IR)	0	3
Bakım (MA)	0	6
Medya Koruması (MP)	1	8
Personel Güvenliği (PS)	0	2
Fiziksel Koruma (PE)	4	2
Risk Değerlendirmesi (RA)	0	3
Güvenlik Değerlendirmesi (CA)	0	4
Sistem ve Haberleşme Koruması (SC)	2	14
Sistem ve Bilgi Bütünlüğü (SI)	4	3

2.2.4. Belgelendirme

Yukarıda bahsedilen bilgi güvenliği yönetimi standartları belgelendirme süreçlerinde olduğu gibi düzenleyici kurum olan ABD Savunma Bakanlığı veya onun bünyesinde yer alan Tedarik ve İdame Ofisi, oluşturmuş oldukları CMMC uygulamaları kapsamında belgelendirme faaliyeti gerçekleştirmemektedir.

Bununla birlikte, CMMC belgelendirme faaliyetleriyle ilgili olarak ABD Savunma Bakanlığı birtakım iş ve işlemleri tanımlamış ve bunların yürütülmesinde düzenleyici otorite olarak görev yapmak üzere CMMC Akreditasyon Kuruluşu'nu (CMMC-AB) yetkilendirmiştir [61].

CMMC Akreditasyon Kuruluşu, uygunluk değerlendirmesi yapan kuruluşları akredite eden kuruluşlar için şartları tanımlayan ISO/IEC 17011 standardına göre akredite ve bağımsız bir organizasyon olacak şekilde, CMMC kapsamında uygunluk değerlendirmesi yapacak kuruluşların faaliyetlerini denetlemek üzere kurulmuştur.

Buna göre düzenleyici otorite olan bu kuruluş, üçüncü taraf denetimleri ve/veya belgelendirme görevlerini gerçekleştirmek üzere “CMMC Üçüncü Taraf Denetim Organizasyonlarını” (C3PAO) ve CMMC denetçilerinin/eğitimcilerinin personel belgelendirme faaliyetleri için “CMMC Denetçi ve Eğitimci Belgelendirme Organizasyonlarını” (CAICO) değerlendirmekte ve yetkilendirmektedir.

Bir kuruluşun C3PAO olarak yetkilendirilebilmesi için çeşitli tiplerdeki muayene kuruluşlarının işletimi için şartları tanımlayan ISO/IEC 17020 standardına göre akredite olması, CAICO olarak yetkilendirilebilmesi için ise personel belgelendirmesi yapan kuruluşlar için genel şartları tanımlayan ISO/IEC 17024 standardına göre akredite olması gerekmektedir. Bununla birlikte CMMC-AB kuruluşun ilgili şartları sağladığını doğrulaması halinde akreditasyon olmaksızın yetkilendirme yapabilmektedir. Böyle bir durumda kuruluşun yetkilendirme tarihi itibariyle 27 ay içinde faaliyet alanıyla ilgili olan standart kapsamında akredite olması gerekmektedir [62].

Yukarıda ifade edilenler hususlar çerçevesinde, CMMC kapsamında gereksinimleri sağlayan savunma sanayi kuruluşları gerektiğinde üçüncü taraf denetimlerinin sağlanması ve CMMC belgelendirmesi için CMMC-AB tarafından yetkilendirilmiş ve onun internet sitesi üzerinde listelenecek C3PAO’lardan birine başvurmalıdır [63].

Bununla birlikte yeni yayınlanan CMMC v2.0 ile kuruluşlar, “Kapsanan Yüklenici Bilgi Sistemlerinin Temel Korunması” olan FAR 52.204-21 kapsamında izin verilenlere benzer şekilde Seviye 1 ve kısmen Seviye 2 uygulamaları kapsamında 3.taraf denetimlerine ihtiyaç duyulmaksızın yıllık periyotlarda kendi içlerinde denetim faaliyetlerini yürütebileceklerdir. Buradaki temel fark, yöneticilerin artık işlerindeki uyum düzeyini belgelemek zorunda kalacak olmalarıdır.

Yine bu doğrultuda Seviye 2 tedarikçileri, değerlendirmeler için iki dahili katmana sahiptir ve yukarıda belirtildiği üzere Seviye 1 için kuruluşlar yıllık öz değerlendirmelerini kendilerinin yapmalarına olanak sağlanmaktadır. Ancak, yaklaşık 40.000'den fazla olduğu tahmin edilen "kritik ulusal güvenlik bilgilerini" işleyen Seviye 2 kuruluşlarının C3PAO'lar tarafından yapılan değerlendirmelerden geçmesi gerekmektedir.

Burada Seviye 2 kuruluşlarının kullandığı CUI türü, bir C3PAO denetiminin mi yoksa Seviye 2 uyumluluğu için bir öz değerlendirmenin mi gerektiğini belirlemektedir.

Örneğin, bir tedarikçi kritik silahlara veya savunma sistemlerine malzeme sağlıyorsa, bir C3PAO denetimine tabi olması gerekmektedir.

Seviye 3 kuruluşlarının ise her üç yılda bir hükümet tarafından yürütülen bir denetimden geçmeleri gerekmektedir. Bu denetimleri hangi kurumun yürüteceğine dair birtakım ayrıntılar olsa da bunun Savunma Sözleşme Yönetim Ajansı'nın (DCMA) Savunma Sanayi Üssü Siber Güvenlik Değerlendirme Merkezi (DIBCAC) olacağı tahmin edilmektedir [64].

2.3. Dünyadaki Diğer Uygulamalar

Yukarıda ifade edilen, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ve Siber Güvenlik Olgunluk Modeli Sertifikasyonu-CMMC uygulamalarına benzer şekilde dünyada bir ülkeye mensup ulusal kuruluşlarla birlikte uluslararası birçok organizasyonun da hazırlamış olduğu önemli siber güvenlik standartları ve rehber güvenlik uygulamaları bulunmaktadır.

Bu kapsamda, ulusal bir kuruluş olan ABD Ulusal Standartlar ve Teknoloji Enstitüsü-NIST, Avrupa Telekomünikasyon Standartları Enstitüsü-ETSI ve Avrupa Birliği Siber Güvenlik Ajansı-ENISA ile uluslararası kuruluşlar olan Uluslararası Standartlar Organizasyonu-ISO, Uluslararası Elektroteknik Komisyonu-IEC, NATO Ortak Siber Savunma Mükemmeliyet Merkezi-CCDCOE, Elektrik ve Elektronik Mühendisleri Enstitüsü-IEEE'nin hazırlamış oldukları siber güvenlik standartları ve rehber güvenlik uygulamaları bu aladaki çalışmalara önemli birer örnek olarak gösterilebilir [65].

2.3.1. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Platformu

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) 1901'de ABD'nin endüstriyel rekabet edebilirliğine yönelik büyük bir zorluğu ortadan kaldırmak için kurulmuş ülkenin en eski fizik bilimi laboratuvarlarından biri olup hali hazırda ABD Ticaret Bakanlığı'na bağlı olarak faaliyetlerini sürdürmektedir [66].

Kuruluşların siber güvenlik riskini daha iyi yönetmesi ve azaltması için mevcut standartlara, yönergelere ve uygulamalara dayanan gönüllü bir rehber güvenlik uygulaması olan ve kuruluşların riskleri yönetmesine ve azaltmasına yardımcı olmanın yanı sıra, hem iç hem de dış kurumsal paydaşlar arasında risk ve siber güvenlik yönetimi iletişimini desteklemek için tasarlanan NIST Siber Güvenlik Platformu'nun ilki (V1.0), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından özel sektörden alınan kapsamlı görüşler doğrultusunda hazırlanarak Şubat 2014'te yayınlanmış olup en güncel hali olan 1.1 versiyonu ise, ana dokümanın ikinci taslağı hakkında 45 gün süren bir kamuoyu yoklaması sonrasında 16 Nisan 2018'de yayınlanmıştır [67].

Platform, siber güvenlik riskini yönetmeye yönelik risk tabanlı bir yaklaşıma sahiptir ve "Platform Çekirdeği", "Platform Uygulama Katmanları", "Platform Profilleri" olmak üzere üç bölümden oluşmaktadır.

Burada "Platform Çekirdeği" bölümü; bir dizi siber güvenlik faaliyeti, istenen sonuçlar ve kritik altyapı sektörlerinde ortak olan geçerli referansları sunmak, "Platform Uygulama Katmanları" bölümü; kuruluşun siber güvenlik riskini nasıl gördüğüne ve bu riski yönetmek için mevcut süreçlere ilişkin bağlam sağlamak, "Platform Profilleri" bölümü ise; kuruluşun platform kategorileri ve alt kategorilerinden seçtiği iş ihtiyaçlarına dayalı sonuçları temsil etmek üzere hazırlanmıştır [68].

2.3.2. Avrupa Telekomünikasyon Standartları Enstitüsü-ETSI standartları

Avrupa Telekomünikasyon Standartları Enstitüsü-ETSI, kuruluş üyelerine açık, kapsayıcı ve işbirliğine dayalı bir ortam sağlamak ve bu şekilde bilgi ve iletişim teknolojilerinin etkin olduğu sistemler, uygulamalar ve hizmetler için küresel ölçekte geçerli standartların zamanında geliştirilmesini, onaylanmasını, test edilmesini desteklemek üzere Avrupa Komisyonu'nun teklifleri doğrultusunda bir Avrupa Standartları Kuruluşu (ESO) olarak Avrupa Posta ve Telekomünikasyon İdareleri Konferansı (CEPT) tarafından 1988 yılında kurulmuş olup 65 ülkeden 900'ün üzerinde üyesiyle faaliyetlerini sürdürmektedir [69].

ETSI internet sitesinde yer alan standart kütüphanesinde birçok konuyla birlikte siber güvenlik konusuyla da ilgili hali hazırda yayınlanmış olan 64 adet standart bulunmaktadır.

2.3.3. Avrupa Birliği Siber Güvenlik Ajansı-ENISA rehber dokümanları

Avrupa Birliği Siber Güvenlik Ajansı (ENISA), Birliğin Avrupa çapında yüksek düzeyde ve ortak şekilde siber güvenliğini sağlamak üzere 10 Mart 2004 tarihli Avrupa Parlamentosu ve Konseyi'nin (EC) 460/2004 sayılı Tüzüğü vasıtasıyla kurulmuş olup bilgi paylaşımı, kapasite geliştirme ve bilinçlendirme yoluyla bağlantılı ekonomiye olan güveni güçlendirmek, Birliğin altyapısının dayanıklılığını artırmak ve nihayetinde Avrupa toplumunu ve vatandaşlarını dijital olarak güvende tutmak için kilit paydaşlarıyla birlikte çalışmalarını sürdürmektedir [70].

ENISA, siber güvenlik faaliyetleri ile ilgili olarak;

- Yüksek düzeyde uzmanlık geliştirmek ve sürdürmek.
- Birlik kurumlarına, organlarına, ofislerine ve ajanslarına ağ ve bilgi güvenliğine ilişkin politikalar geliştirmede yardımcı olmak,
- Birlik kurumlarına, organlarına, ofislerine ve ajanslarına ve Üye Devletlere, Birliğin mevcut ve gelecekteki yasal düzenlemeleri kapsamında ağ ve bilgi güvenliğinin yasal ve düzenleyici gerekliliklerini karşılamak için gerekli politikaların uygulanmasında yardımcı olmak ve böylece iç pazarın düzgün işleyişini sağlamak,
- Birliğe ve Üye Devletlere, ağ ve bilgi güvenliği sorunları ve olaylarını önleme, tespit etme ve bunlara müdahale etme kapasitelerini ve hazırlıklarını artırma ve güçlendirme konusunda yardımcı olmak,
- Edindiği uzmanlık ile kamu ve özel sektörden aktörler arasında geniş iş birliğini teşvik etmek,

amaçları doğrultusunda kurulmuştur [71].

ENISA internet sitesinde bu amaçlara uygun olarak siber güvenlikle ilgili hali hazırda yayınlanmış olan 411 adet rapor, 25 adet siber güvenlik bilgi notu ve 22 adet görüş bildirisi bulunmaktadır.

2.3.4. ISO/IEC bilgi güvenliği standartları ailesi

Uluslararası Standartlar Örgütü-ISO ve Uluslararası Elektroteknik Komisyonu-IEC sırasıyla 1947 ve 1906 yıllarında Londra'da kurulan bağımsız uluslararası elektrik-elektronik alanında birçok standardın hazırlanması süreçlerinde organizasyonlardır ve birlikte görev almışlardır [72], [73].

Bu organizasyonların bilgi güvenliği alanında yukarıda ayrıntılı şekilde ifade edilen ISO/IEC 27001 Bilgi güvenliği Yönetim Sistemi Standardının da içinde yer aldığı ISO/IEC 27000 ailesi olarak ifade edilen ve Çizelge 2.5.'de belirtilen standartlar dünyada en çok kullanılan siber güvenlik standartları arasında yer almaktadır [74].

Çizelge 2.6. ISO/IEC 27000 ailesi standartları

Tanım Standardı	**Gereksinim Standartları**	**Kılavuz Standartlar**	**Sektör Özelinde Kılavuz Standartlar**	**Kontrol Özelinde Kılavuz Standartlar**
ISO/IEC 27000: Bilgi güvenliği yönetim sistemleri-Genel bakış ve kelime bilgisi	ISO/IEC 27001: Bilgi güvenliği yönetim sistemleri-Gereksinimler	ISO/IEC 27002: Bilgi güvenliği kontrolleri için uygulama prensipleri	ISO/IEC 27010: sektörler arası ve organizasyonlar arası iletişim için bilgi güvenliği yönetimi	ISO/IEC 2703x

Çizelge 2.5.(devam) ISO/IEC 27000 ailesi standartları

	ISO/IEC 27006: Bilgi güvenliği yönetim sistemi tetkik ve belgelendirmesini yapan kuruluşlar için gereklilikler	ISO/IEC 27003: Bilgi güvenliği yönetim sistemi uygulama kılavuzu	ISO/IEC 27011: Telekomünikasyon kuruluşları için ISO / IEC 27002'ye dayalı bilgi güvenliği denetimleri için uygulama prensipleri	ISO/IEC 2704x
	ISO/IEC 27009: ISO/IEC 27001 'in sektöre özel uygulaması-Gereklilikler	ISO/IEC 27004: Bilgi Güvenliği Yönetimi-Ölçüm	ISO/IEC 27017: Bulut hizmetlerinde ISO/IEC 27002 standardına dayalı bilgi güvenliği kontrolleri için uygulama ilkesi	ISO/IEC 2705x
		ISO/IEC 27005: Bilgi güvenliği risk yönetimi	ISO/IEC 27018: PII (Kişi tanımlama bilgisi) işleyen açık bulut ağlarda kişi tanımlama bilgisinin korunması için uygulama prensipleri	

Çizelge 2.5.(devam) ISO/IEC 27000 ailesi standartları

		ISO/IEC 27007: Bilgi Güvenliği Yönetim Sistemleri Denetimi için kılavuz	ISO/IEC 27019: Enerji hizmet endüstrisi bilgi güvenliği önlemleri.	
		ISO/IEC 27008: Denetçiler için bilgi güvenliği kontrolleri kılavuzu	ISO/IEC 27799: ISO/IEC 27002 standardını kullanarak sağlıkta bilgi güvenliği yönetimi	
		ISO/IEC 27013: ISO/IEC 27001 ve ISO/IEC 20000-1 standartlarının tümleşik uygulaması hakkında kılavuz		
		ISO/IEC 27014: Bilgi güvenliği yönetimi		

Çizelge 2.5.(devam) ISO/IEC 27000 ailesi standartları

		ISO/IEC 27016: Bilgi güvenliği yönetimi-Örgütsel ekonomi		
		ISO/IEC 27021: Bilgi güvenliği yönetim sistemleri uzmanları için yeterlilik gereksinimleri		

2.3.5. NATO Ortak Siber Savunma Mükemmeliyet Merkezi-CCDCOE rehber dokümanları

Kuzey Atlantik Antlaşması Örgütü-NATO, Sovyetler Birliği'nin oluşturduğu tehdide yanıt olmanın yanında Sovyet yayılmacılığını caydırmak, Avrupa kıtasında güçlü bir Kuzey Amerika varlığı aracılığıyla Avrupa'da milliyetçi militarizmin canlanmasını önlemek ve Avrupa'nın siyasi bütünleşmesini teşvik etmek üzere 12 ülke tarafından Kuzey Atlantik Antlaşması'nı imzalanması ile 4 Nisan 1949'da kurulmuş olup ilerleyen dönemde 18 ülke daha örgüte katılım sağlamıştır [75].

NATO Ortak Siber Savunma Mükemmeliyet Merkezi-CCDCOE ise Estonya'nın girişimiyle Almanya, İtalya, Letonya, Litvanya, Slovak Cumhuriyeti ve İspanya olmak üzere altı ülke ile birlikte 18 Mayıs 2008 tarihinde kurulmuş olup misyonu teknoloji, strateji, operasyonlar ve hukukun odak alanlarını kapsayan siber savunma araştırmaları, eğitimleri ve tatbikatları alanında benzersiz disiplinler arası deneyimlerle üye ülkeleri ve NATO'yu desteklemektir [76].

CCDCOE internet sitesinde kuruluş tarihinden itibaren yayınlanmakta olan çok sayıda makale, teknik rapor ve kitaba ücretsiz olarak ulaşılabilmekle beraber siber güvenlikle ilgili stratejik, operasyonel, hukuki ve teknik birçok eğitime katılım imkânı da sunulmaktadır [77].

2.3.6. Elektrik ve Elektronik Mühendisleri Enstitüsü-IEEE standartları

Elektrik ve Elektronik Mühendisleri Enstitüsü-IEEE bir grup mühendis tarafından insanlık yararına yenilik ve teknolojik mükemmelliği geliştirmek amacıyla 1884 yılında ABD'de kurulmuş dünyanın en büyük teknik profesyonel topluluğudur ve modern uygarlığın temelini oluşturan elektrik, elektronik ve bilgisayar alanlarının ve ilgili bilim ve teknolojinin tüm yönleriyle ilgili profesyonellere hizmet etmek için tasarlanmıştır [78].

IEEE günümüzde neredeyse her alanda gerçekleştirdiği çalışmalar sayesinde birçok konuda önemli tecrübeleri bünyesinde barındırmakta ve bu tecrübeleri hazırlamış olduğu standartlarla kuruluşların hizmetine sunmaktadır.

IEEE bu amaçla küresel teknolojileri besleyen, geliştiren ve ilerleten lider bir fikir birliği oluşturma organizasyonu olan IEEE Standartları Birliği-IEEE SA'yı kurmuş olup bu sayede 160'tan fazla ülkede iş birliği kurduğu düşünce liderleriyle yeniliği teşvik etmekte, uluslararası pazarların oluşturulmasına ve genişletilmesine katkı sağlamakta, sağlık ve kamu güvenliğinin korunmasına yardımcı olmaktadır [79].

IEEE SA internet sitesinde hali hazırda 130'adet siber güvenlik konulu standart bulunmakta olup ücret karşılığında kullanıcıların erişimine sunulmaktadır.

3. YÖNTEM

Bu çalışmada kullanılan yöntem; ülkemizin önemli savunma sanayi kuruluşlarının bilgi güvenliği yönetimi uygulamalarının mevcut durumu hakkında verilerin toplanması, toplanan bu veriler yardımıyla uluslararası standartlar bağlamında kuruluşlarda yaygın olarak kullanılan bilgi güvenliği yönetimi uygulamasının belirlenmesi, belirlenen bu uygulamaya ait gereksinimler ile CMMC v2.0 uygulamalarının karşılaştırılması ve bu sayede hali hazırda uygulandığı görülen mevcut bilgi güvenliği yönetimi uygulaması ile CMMC v2.0 şartlarının ne ölçüde karşılandığına dair verilerin ortaya konması amaçlarına uygun olacak şekilde belirlenmiştir.

Bu bölümde, yukarıdaki amaçlara uygun olarak yöntemde yer alan; araştırma evreni, veri toplama araçları, değerlendirme modeli, hakkındaki bilgilere yer verilmiştir.

Çalışmada dikkate alınan araştırma evreni ülkemizde faaliyet gösteren ve "Savunma ve Havacılık Sanayi İmalatçılar Birliği" (SASAD) üyesi olan 122 savunma sanayi kuruluşu [80] içerisinden seçilen ve ülkemizin önde gelen 6 savunma sanayi kuruluşundan oluşmaktadır.

Buradaki kuruluşların 3'ü İstanbul Sanayi Odası'nın verilerine göre Türkiye'nin en büyük 500 sanayi şirketinin yer aldığı İSO 500 listesinde ilk 100'de yer alanlar içerisinden seçilmiş olup, diğer 3'ü ise bu listede ilk 100'de yer almayan kuruluşlar içerisinden seçilmiştir.

Sonraki aşamada çalışmada kullanılacak verilerin anket yöntemiyle [81] elde edilmesi amacıyla öncelikle bu savunma sanayi kuruluşlarına ait;

- Bilgi güvenliği uygulamaları,
- Son bir yıl içinde yaygın siber saldırı türlerine maruz kalıp kalınmadığı,
- CMMC farkındalığı,

hakkında sorular içeren bir soru listesi oluşturulması planlanmıştır.

Buna uygun olarak Ek-1'de sunulan uzman görüşü formu yardımıyla, savunma sanayinde görev yapan 2 siber güvenlik uzmanı ve siber güvenlik alanında uzman 1 akademisyenden

alınan görüş ve değerlendirmeler doğrultusunda Ek-2'de belirtilen soru listesinin son hali oluşturulmuştur [82].

Sonrasında Ek-2'de yer alan soru listesinin, araştırma evrenini oluşturan ülkemizin öncü 6 büyük savunma sanayi kuruluşunda görev yapan bilgi güvenliği yönetimi sorumlularına karşılıklı görüşme veya e-posta yoluyla iletilerek cevaplandırılması sağlanmıştır.

Çalışmanın devamında, Ek-2'de yer alan soru listesine verilen cevaplar doğrultusunda elde edilen veriler yardımıyla söz konusu savunma sanayi kuruluşlarına uluslararası standartlar bağlamında ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardının yaygın olarak kullanıldığı tespit edilmiştir.

Çalışmanın amacı doğrultusunda iki farklı uygulama için değerlendirme modeli olarak kullanılmak üzere, CMMC v2.0 gereksinimleri ile ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardının gereksinimleri eşleştirilerek 5. Bölüm 'de "ARAŞTIRMA BULGULARI" başlığı altında son halleri sunulan eşleştirme tablolarının ilk taslakları oluşturulmuştur.

Oluşturulan bu taslak eşleştirme tabloları Ek-3'te yer alan eşleştirme değerlendirme formu ile bilgi güvenliği yönetimi alanında en az 10 yıl deneyimi bulunan ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Denetçisi unvanına haiz 3 uzmana iletilmiş, onlardan gelen geri bildirimler doğrultusunda eşleştirme tablolarına son halleri verilmiştir.

Söz konusu tablolar yardımıyla, karşılanması hedeflenen ve CMMC v2.0'da "uygulama" olarak ifade edilen gereksinimlerin, yaygın olarak kullanıldığı görülen ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardına ait mevcut durumda savunma sanayi kuruluşlarınca karşılandığı kabul edilen gereksinimleri ile hangilerinin sağlandığı eşleştirme yapılarak belirlenmiştir.

Bunun sonucunda karşılığı bulunmadığı görülen CMMC v2.0 uygulamalarının alanlara göre dağılım oranları ile CMMC v2.0 seviyeleri ve alanlarına göre eşleşme oranları kolaylıkla anlaşılabilir olması için oluşturulan şekiller ile gösterilmiştir.

Burada belirtilen yöntem ile elde edilen verilerin tamamı kuruluşlardan gelen talepler ve konunun hassasiyeti nedeniyle kuruluş ismi belirtilmeksizin çalışmaya aktarılmıştır.

4. ARAŞTIRMA BULGULARI

Bu başlık altında çalışma kapsamında elde edilen bulgular konularına bağlı olarak ayrı ayrı başlıklar ile ifade edilmiştir.

4.1. Kuruluşlarda Mevcut Bilgi Güvenliği Uygulamaları

Kuruluşların mevcut bilgi güvenliği yönetimi uygulamalarının ne olduğunu görmek üzere Soru Listesindeki ilk 6 soruya ait kuruluşlardan gelen cevaplar aşağıdaki çizelgelerde belirtilmiştir.

Çizelge 4.1. Soru 1'e ait cevaplar

Soru 1: Kuruluşunuzda ait yazılı bir bilgi güvenliği politikası mevcut mudur?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☒	☒	☒	☒	☒
Hayır	☐	☐	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☐	☐	☐

Çizelge 4.1.'de görüldüğü üzere araştırma kapsamında yer alan kuruluşların tamamında yazılı bir bilgi güvenliği politikası bulunmaktadır. Bu sonuçlar kuruluşların belirli bir seviyede bilgi güvenliği farkındalığına sahip olduğunu göstermesi bakımından önemlidir.

Çizelge 4.2. Soru 2'ye ait cevaplar

Soru 2: Kuruluşunuz tarafından düzenli olarak bilgi güvenliği politikalarının uygunluğu denetlenmekte midir?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☐	☒	☒	☒	☒

Çizelge 4.2.(devam) Soru 2'ye ait cevaplar

Hayır	☐	☒	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☐	☐	☐

Çizelge 4.2.'de görüldüğü üzere kuruluşların 5'inde düzenli aralıklarla kuruluşa ait bilgi güvenliği politikalarının uygunluğunu denetlenmekte iken bunların dışında kalan diğer kuruluşta bilgi güvenliği politikalarının uygunluğu herhangi bir şekilde denetlenmemektedir.

Çizelge 4.3. Soru 3'e ait cevaplar

Soru 3: Kuruluşunuza ait iş süreçlerine özgü en uygun siber güvenlik tedbirlerinin belirlenmesi nasıl yapılmaktadır?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Kurumsal organizasyona bağlı yapılar ile iç değerlendirmeler yapılarak	☐	☐	☒	☐	☒	☐
Sektördeki diğer kuruluşlarla ortak değerlendirmeler yapılarak	☐	☐	☒	☐	☒	☐
Sektörden bağımsız diğer kuruluşlarla ortak değerlendirmeler yapılarak	☐	☐	☒	☒	☐	☐

Çizelge 4.3.(devam) Soru 3'e ait cevaplar

Sektöre özel yaygın olarak kullanılan yöntemler göz önünde bulundurularak	☐	☐	☒	☐	☒	☐
Sektörden bağımsız yaygın olarak kullanılan yöntemler göz önünde bulundurularak	☒	☒	☒	☐	☒	☐
Cevap verilmedi	☐	☐	☐	☒	☐	☒

Çizelge 4.3.'e bakıldığında kuruluşların yalnızca 4'ünün ilgili soruyu cevaplandırmış olduğu görülmektedir. Buna göre söz konusu kuruluşların tamamı kendilerine ait iş süreçlerine özgü en uygun siber güvenlik tedbirlerini belirlerken sektörden bağımsız yaygın olarak kullanılan yöntemleri göz önünde bulundurmakta iken bu kuruluşlardan 2'si buna ilave olarak diğer yöntemlerden de faydalandığını belirtmektedir.

Çizelge 4.4. Soru 4'e ait cevaplar

Soru 4: Kuruluşunuzda 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde belirtilenlerden farklı olarak uyguladığınız ilave tedbirler bulunmakta mıdır?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☐	☒	☐	☒	☐
Hayır	☐	☒	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☒	☐	☒

Çizelge 4.4.'de ilgili soruya kuruluşların yine 4'ünün cevap verdiği görülmektedir. Buna göre bu kuruluşların 3'ü 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde belirtilenlerden farklı olarak ilave tedbirler uygulamakta iken diğer kalan diğer kuruluş herhangi bir ilave tedbir uygulamadığını belirtmektedir.

Çizelge 4.5. Soru 5'e ait cevaplar

Soru 5: Kuruluşunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgesi bulunuyor mu?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☐	☒	☒	☒	☒
Hayır	☐	☒	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☐	☐	☐

Çizelge 4.5.'de kuruluşların biri haricinde tamamının ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgesinin bulunduğu böylece ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardının yaygın olarak kullanıldığı görülmektedir.

Çizelge 4.6. Soru 6'ya ait cevaplar

Soru 6: Kuruluşunuzda bilgi güvenliği alt yapısı oluşturulurken referans alınan ulusal veya uluslararası ölçekte kabul görmüş diğer bir standart ve/veya uygulama modeli / rehber doküman bulunmakta mıdır?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☐	☒	☐	☒	☐
Hayır	☐	☒	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☒	☐	☒

Çizelge 4.6.'da kuruluşların yalnızca 4'ünün ilgili soruya cevap verdiği görülmektedir. Buna göre söz konusu kuruluşların 3'ü bilgi güvenliği alt yapılarını oluştururken ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı dışında ulusal veya uluslararası ölçekte kabul görmüş diğer bir standart ve/veya uygulama modeli / rehber dokümanı referans olarak kullanmıştır.

Çizelge 4.7. CB DDO BİGR ve ISO/IEC 27001 dışındaki uygulamalar

	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
CIS V8	☒	☐	☒	☐	☒	☐
NIST SP 800-53	☐	☐	☒	☐	☐	☐
NIST Cybersecurity Framework	☐	☐	☒	☐	☒	☐
Cevap verilmedi	☐	☒	☐	☒	☐	☒

Çizelge 4.7.'ye göre bilgi güvenliği alt yapılarını oluştururken ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı dışında ulusal veya uluslararası ölçekte kabul görmüş diğer bir standart ve/veya uygulama modeli / rehber dokümanı referans olarak kullanan bu kuruluşlar CIS V8, NIST SP 800-53 standardı ile CIS V8 ve NIST Cybersecurity Framework uygulamalarından da faydalanmaktadır.

4.2. Kuruluşlara Son Bir Yılda Yapılan Siber Saldırılar

Kuruluşların son bir yıl içinde yaygın siber saldırı türlerine maruz kalıp kalmadığını görmek üzere Soru Listesinde bulunan 7,8 ve 9. soruya ait kuruluşlardan gelen cevaplar aşağıdaki çizelgelerde belirtilmiştir.

Çizelge 4.8. Soru 7'ye ait cevaplar

Soru 7: Kuruluşunuza ait web sitesi veya ağlar son bir yıl içinde DDoS veya herhangi bir siber saldırıya maruz kalmış mıdır?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☐	☐	☐	☐	☐
Hayır	☐	☒	☐	☐	☒	☐
Cevap verilmedi	☐	☐	☒	☒	☐	☒

Çizelge 4.8.'de kuruluşlardan yalnızca 3'ünün ilgili soruya cevap verdiği görülmektedir. Buna göre yalnızca 1 kuruluşa ait web sitesi veya ağlar son bir yıl içinde DDoS veya herhangi bir siber saldırıya maruz kalmıştır.

Çizelge 4.9. Soru 8'e ait cevaplar

Soru 8: Kuruluşunuza ait bilgisayarlarda ve/veya ağlarda, son bir yıl içinde tespit edilen zararlı yazılım(lar) oldu mu?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☒	☐	☐	☐	☐	☐
Hayır	☐	☒	☐	☐	☒	☐
Cevap verilmedi	☐	☐	☒	☒	☐	☒

Çizelge 4.9.'da kuruluşlardan yalnızca 3'ünün ilgili soruya cevap verdiği görülmektedir. Buna göre yalnızca 1 kuruluşa ait bilgisayarlarda ve/veya ağlarda, son bir yıl içinde tespit edilen zararlı yazılım(lar) mevcuttur.

Çizelge 4.10. Soru 9'a ait cevaplar

Soru 9: Kuruluş ağlarından, son bir yıl içerisinde yetkisiz kullanıcılar tarafından bilgi kaçırılmasına yönelik herhangi bir olay gerçekleşti mi?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☐	☐	☐	☐	☐	☐
Hayır	☒	☒	☐	☐	☒	☐
Cevap verilmedi	☐	☐	☒	☒	☐	☒

Çizelge 4.10.'da da yukarıdakilere benzer şekilde yine 3 kuruluşun ilgili soruya cevap verdiği görülmektedir. Buna göre bu kuruluşlara ait ağlardan son bir yıl içerisinde yetkisiz kullanıcılar tarafından bilgi kaçırılmasına yönelik herhangi bir olay gerçekleşmemiştir.

4.3. Kuruluşların CMMC Farkındalığı

Kuruluşların CMMC farkındalığı hakkında bilgi almak üzere Soru Listesinde bulunan 7,8 ve 9. soruya ait kuruluşlardan gelen cevaplar aşağıdaki çizelgelerde belirtilmiştir.

Çizelge 4.11. Soru 10'a ait cevaplar

Soru 10: Amerika Birleşik Devletleri Savunma Bakanlığının savunma sanayine yönelik bilgi güvenliği alt yapısını güçlendirmek için oluşturduğu CMMC adı verilen bilgi güvenliği yönetimi modeli hakkında bilginiz var mı?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Bilgim yok	☐	☐	☐	☒	☐	☐
S1) İsmini duydum	☒	☐	☐	☐	☐	☐

Çizelge 4.11.(devam) Soru 10’a ait cevaplar

S2) İsmini duydum ve tanımını biliyorum	☐	☒	☐	☐	☐	☒
S3) Tanımıyla birlikte modelin uygulanma gerekçesini ve kapsamını biliyorum	☐	☐	☒	☐	☐	☐
S4) S3’e ilave olarak modelin uygulama yöntemi ve seviyeleri hakkında bilgi sahibiyim	☐	☐	☐	☐	☒	☐
S5) S4’e ilave olarak modelin ne şekilde uygulanacağını, içerdiği tanımları ve seviyelerine bağlı gereksinimleri hakkında da bilgi sahibiyim.	☐	☐	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☐	☐	☐

Çizelge 4.11.’e göre kuruluşların büyük çoğunluğunda belirli seviyelerde CMMC modeline yönelik farkındalık bulunmaktadır. Bunlar içerisinde en yüksek farkındalık seviyesi S4 iken en düşük farkındalık seviyesinin ise S1 olduğu görülmektedir.

Çizelge 4.12. Soru 11'e ait cevaplar

Soru 11: Yakın gelecekte ABD Savunma Bakanlığı, tüm tedarikçi ve onların alt tedarikçileri için CMMC kapsamında belgeli olma şartını getirmeyi planlamaktadır. Bu bağlamda kuruluşunuzun ilerleyen herhangi bir tarihte CMMC belgesine sahip olması gerektiğini düşünüyor musunuz?						
	Kuruluş 1	Kuruluş 2	Kuruluş 3	Kuruluş 4	Kuruluş 5	Kuruluş 6
Evet	☐	☒	☒	☐	☒	☒
Hayır	☒	☐	☐	☐	☐	☐
Cevap verilmedi	☐	☐	☐	☒	☐	☐

Çizelge 4.12.'de de benzer şekilde kuruluşların önemli bir kısmını oluşturan 4 tanesinin ilerleyen herhangi bir tarihte CMMC belgesine sahip olmasının gerekeceğini düşündüğü görülmektedir.

4.4. ISO/IEC 27001 Gereksinimleri ile CMMC Uygulamalarına Ait Eşleştirme Tabloları

ISO IEC 27001 BGYS Denetçilerinden oluşan uzmanların görüşleri doğrultusunda yapılan değerlendirmeye göre CMMC v2.0'da yer alan uygulamaların ISO IEC 27001 gereksinimleri ile eşleştirildiği tablolar alan konularına göre gruplandırılarak tablolar halinde aşağıdaki başlıklar altında belirtilmiştir.

4.4.1. "AC-Erişim Kontrolü" alanı karşılıkları

CMMC v2.0'da bulunan "AC-Erişim Kontrolü" konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.13. ile belirtilmiştir.

Çizelge 4.13. “AC-Erişim Kontrolü” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
AC-Erişim Kontrolü			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
AC. L1-3.1.1 *Yetkili Erişim Kontrolü* Yetkili kullanıcılara, yetkili kullanıcılar adına hareket eden süreçlere veya cihazlara (diğer bilgi sistemleri dahil) bilgi sistemi erişimini sınırlayın.	**AC.L2-3.1.3** *CUI Akış Kontrolü* Onaylanmış yetkilendirmelere göre CUI akışını kontrol edin.	A.9.2 Kullanıcı erişim yönetimi A.9.2.2 Kullanıcı erişimine izin verme	Bulunmuyor
AC.L1-3.1.2 *İşlem ve İşlev Kontrolü* Yetkili kullanıcıların yürütmesine izin verilen işlem türleri ve işlevlere bilgi sistemi erişimini sınırlayın.	**AC.L2-3.1.4** *Görevlerinin ayrılması* Örtülü niyetler olmaksızın kötü niyetli faaliyet riskini azaltmak için bireylerin görevlerini ayırın.	A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.1 Bilgiye erişimin kısıtlanması	A.6.1 İç organizasyon A.6.1.2 Görevlerin ayrılığı

Çizelge 4.13.(devam) “AC-Erişim Kontrolü” alanı karşılıkları

AC.L1-3.1.20 *Dış Bağlantılar* Harici bilgi sistemlerine bağlantıları ve bunların kullanımını doğrulayın ve kontrol edin/sınırlayın.	**AC.L2-3.1.5** *En Az Ayrıcalık* Belirli güvenlik işlevleri ve ayrıcalıklı hesaplar dahil olmak üzere en az ayrıcalık ilkesini kullanın.	A.13.2 Bilgi transferi A.13.2.1 Bilgi transfer politikaları ve prosedürleri	A.9.2 Kullanıcı erişim yönetimi A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
AC.L1-3.1.22 *Kamu Bilgilerini Kontrol Et* Kamuya açık bilgi sistemlerinde yayınlanan veya işlenen bilgileri kontrol edin.	**AC.L2.-3.1.6** *Ayrıcalıksız Hesap Kullanımı* Güvenlikle ilgili olmayan işlevlere erişirken ayrıcalıklı olmayan hesapları veya rolleri kullanın.	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması	Bulunmuyor

Çizelge 4.13.(devam) “AC-Erişim Kontrolü” alanı karşılıkları

	AC.L2-3.1.7 *Ayrıcalıklı İşlevler* Ayrıcalıklı olmayan kullanıcıların ayrıcalıklı işlevleri yürütmesini önleyin ve bu tür işlevlerin yürütülmesini denetim günlüklerinde yakalayın.		A.9.2 Kullanıcı erişim yönetimi A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
	AC.L2-3.1.8 *Başarısız Oturum Açma Denemeleri* Başarısız oturum açma girişimlerini sınırlayın.		Bulunmuyor
	AC.L2-3.1.9 *Gizlilik ve Güvenlik Bildirimleri* Geçerli CUI kurallarıyla tutarlı gizlilik ve güvenlik bildirimleri sağlayın.		Bulunmuyor

Çizelge 4.13.(devam) “AC-Erişim Kontrolü” alanı karşılıkları

	AC.L2-3.1.10 *Oturum Kilidi* Belirli bir süre işlem yapılmadığında verilere erişimi ve verilerin görüntülenmesini önlemek için desen gizleme ekranlarıyla oturum kilidini kullanın.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.2 Güvenli oturum açma prosedürleri
	AC.L2-3.1.11 *Oturum Sonlandırma* Tanımlanmış bir koşuldan sonra bir kullanıcı oturumunu (otomatik olarak) sonlandırın.		Bulunmuyor
	AC.L2-3.1.12 *Uzaktan Erişimi Kontrol Et* Uzaktan erişim oturumlarını izleyin ve kontrol edin.		A.6.2 Mobil cihazlar ve uzaktan çalışma A.6.2.2 Uzaktan çalışma

Çizelge 4.13.(devam) “AC-Erişim Kontrolü” alanı karşılıkları

	AC.L2-3.1.13 *Uzaktan Erişim Gizliliği* Uzaktan erişim oturumlarının gizliliğini korumak için kriptografik mekanizmalar kullanın.		Bulunmuyor
	AC.L2-3.1.14 *Uzaktan Erişim Yönlendirme* Yönetilen erişim kontrol noktaları aracılığıyla uzaktan erişimi yönlendirin.		Bulunmuyor
	AC.L2-3.1.15 *Ayrıcalıklı Uzaktan Erişim* Ayrıcalıklı komutların uzaktan yürütülmesine ve güvenlikle ilgili bilgilere uzaktan erişime yetki verin.		Bulunmuyor

Çizelge 4.13.(devam) “AC-Erişim Kontrolü” alanı karşılıkları

	AC.L2-3.1.16 *Kablosuz Erişim Yetkilendirmesi* Bu tür bağlantılara izin vermeden önce kablosuz erişimi yetkilendirin.		A.9.1 Erişim kontrolünün iş gereklilikleri A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1 Ağ güvenliği yönetimi A.13.1.1 Ağ kontrolleri
	AC.L2-3.1.17 *Kablosuz Erişim Koruması* Kimlik doğrulama ve şifreleme kullanarak kablosuz erişimi koruyun.		A.13.1 Ağ güvenliği yönetimi A.13.1.2 Ağ hizmetlerinin güvenliği
	AC.L2-3.1.18 *Mobil Cihaz Bağlantısı* Mobil cihazların bağlantısını kontrol edin.		A.6.2 Mobil cihazlar ve uzaktan çalışma A.6.2.1 Mobil cihaz politikası

Çizelge 4.13.(devam) “AC-Erişim Kontrolü” alanı karşılıkları

	AC.L2-3.1.19 *Mobil Cihazda CUI'yi Şifreleyin* CUI'yi mobil cihazlarda ve mobil bilgi işlem platformlarında şifreleyin.		Bulunmuyor
	AC.L2-3.1.21 *Taşınabilir Depolama Kullanımı* Harici sistemlerde taşınabilir depolama cihazlarının kullanımını sınırlayın.		A.8.3 Ortam işleme A.8.3.1 Taşınabilir ortam yönetimi

4.4.2. “AT-Farkındalık ve Eğitim” alanı karşılıkları

CMMC v2.0’da bulunan “AT-Farkındalık ve Eğitim” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.14. ile belirtilmiştir.

Çizelge 4.14. “AT-Farkındalık ve Eğitim” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
AT-Farkındalık ve Eğitim			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	AT.L2-3.2.1 *Rol Bazlı Risk Farkındalığı* Yöneticilerin, sistem yöneticilerinin ve kurumsal sistemlerin kullanıcılarının, faaliyetleriyle ilişkili güvenlik risklerinden ve bu sistemlerin güvenliğiyle ilgili geçerli politikalar, standartlar ve prosedürlerden haberdar olmalarını sağlayın.		A.7.2 Çalışma esnasında A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi

Çizelge 4.14.(devam) “AT-Farkındalık ve Eğitim” alanı karşılıkları

	AT.L2-3.2.2 *Rol Bazlı Eğitim* Personelin, kendilerine atanan bilgi güvenliği ile ilgili görev ve sorumluluklarını yerine getirmek için eğitildiğinden emin olun.		A.7.2 Çalışma esnasında A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi
	AT.L2-3.2.3 *İçeriden Tehdit Farkındalığı* İçeriden gelen tehdidin potansiyel göstergelerini tanıma ve raporlama konusunda güvenlik bilinci eğitimi sağlayın.		A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.3 Bilgi güvenliği açıklıklarının raporlanması

4.4.3. “AU-Denetim ve Hesap Verebilirlik” alanı karşılıkları

CMMC v2.0’da bulunan “AU-Denetim ve Hesap Verebilirlik” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.15. ile belirtilmiştir.

Çizelge 4.15. “AU-Denetim ve Hesap Verebilirlik” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
AU-Denetim ve Hesap Verebilirlik			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	AU.L2-3.3.1 *Sistem Denetimi* Yasa dışı veya yetkisiz sistem etkinliğinin izlenmesini, analizini, araştırılmasını ve raporlanmasını sağlamak için gereken ölçüde sistem denetim günlüklerini ve kayıtlarını oluşturun ve saklayın.		A.12.4 Kaydetme ve izleme A.12.4.1 Olay kaydetme

Çizelge 4.15.(devam) “AU-Denetim ve Hesap Verebilirlik” alanı karşılıkları

	AU.L2-3.3.2 *Kullanıcı Sorumluluğu* Bireysel sistem kullanıcılarının eylemlerinin bu kullanıcılara benzersiz bir şekilde izlenebildiğinden emin olun, böylece eylemlerinden sorumlu tutulabilirler.		A.12.4 Kaydetme ve izleme A.12.4.3 Yönetici ve operatör kayıtları
	AU.L2-3.3.3 *Etkinlik İncelemesi* Günlüğe kaydedilen olayları gözden geçirin ve güncelleyin.		A.12.4 Kaydetme ve izleme A.12.4.1 Olay kaydetme
	AU.L2-3.3.4 *Denetim Hatası Uyarısı* Denetim günlüğü işlemi hatası durumunda uyar.		Bulunmuyor

Çizelge 4.15.(devam) “AU-Denetim ve Hesap Verebilirlik” alanı karşılıkları

	AU.L2-3.3.5 *Denetim Korelasyonu* Soruşturma ve yasa dışı, yetkisiz, şüpheli veya olağandışı faaliyet belirtilerine yanıt için denetim kaydı incelemesi, analizi ve raporlama süreçleri arasında ilişki kurun.		Bulunmuyor
	AU.L2-3.3.6 *Azaltma ve Raporlama* İsteğe bağlı analiz ve raporlamayı desteklemek için denetim kayıtlarını azaltma ve rapor oluşturmayı sağlayın.		Bulunmuyor

Çizelge 4.15.(devam) “AU-Denetim ve Hesap Verebilirlik” alanı karşılıkları

	AU.L2-3.3.7 *Yetkili Zaman Kaynağı* Denetim kayıtları için zaman damgaları oluşturmak üzere dahili sistem saatlerini yetkili bir kaynakla karşılaştıran ve senkronize eden bir sistem yeteneği sağlayın.		A.12.4 Kaydetme ve izleme A.12.4.4 Saat senkronizasyonu
	AU.L2-3.3.8 *Denetim Koruması* Denetim bilgilerini ve denetim günlüğü araçlarını yetkisiz erişime, değiştirmeye ve silmeye karşı koruyun.		A.12.4 Kaydetme ve izleme A.12.4.2 Kayıt bilgisinin korunması
	AU.L2-3.3.9 *Denetim Yönetimi* Denetim günlüğü işlevselliğinin yönetimini ayrıcalıklı kullanıcıların bir alt kümesiyle sınırlayın.		Bulunmuyor

4.4.4. “CM-Konfigürasyon Yönetimi” alanı karşılıkları

CMMC v2.0’da bulunan “CM-Konfigürasyon Yönetimi” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.16. ile belirtilmiştir.

Çizelge 4.16. “CM-Konfigürasyon Yönetimi” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
CM-Konfigürasyon Yönetimi			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	CM.L2-3.4.1 *Sistem Temeli Belirleme* İlgili sistem geliştirme yaşam döngüleri boyunca kurumsal sistemlerin (donanım, yazılım, bellenim ve belgeler dahil) temel yapılandırmalarını ve envanterlerini oluşturun ve sürdürün.		A.8.1 Varlıkların sorumluluğu A.8.1.1 Varlıkların envanteri

Çizelge 4.16.(devam) “CM-Konfigürasyon Yönetimi” alanı karşılıkları

	CM.L2-3.4.2 *Güvenlik Yapılandırma Uygulaması* Kurumsal sistemlerde kullanılan bilgi teknolojisi ürünleri için güvenlik yapılandırma ayarlarını oluşturun ve uygulayın.		A.12.1 İşletim prosedürleri ve sorumlulukları A.12.1.1 Yazılı işletim prosedürleri
	CM.L2-3.4.3 *Sistem Değişiklik Yönetimi* Organizasyonel sistemlerde yapılan değişiklikleri takip edin, gözden geçirin, onaylayın veya onaylamayın ve günlüğe kaydedin.		A.12.1 İşletim prosedürleri ve sorumlulukları A.12.1.2 Değişiklik yönetimi
	CM.L2-3.4.4 *Güvenlik Etki Analizi* Uygulamadan önce değişikliklerin güvenlik etkisini analiz edin.		A.12.1 İşletim prosedürleri ve sorumlulukları A.12.1.2 Değişiklik yönetimi

Çizelge 4.16.(devam) “CM-Konfigürasyon Yönetimi” alanı karşılıkları

	CM.L2-3.4.5 *Değişiklik için Erişim Kısıtlamaları* Kurumsal sistemlerdeki değişikliklerle ilişkili fiziksel ve mantıksal erişim kısıtlamalarını tanımlayın, belgeleyin, onaylayın ve uygulayın.		A.14.2 Geliştirme ve destek süreçlerinde güvenlik A.14.2.2 Sistem değişiklik kontrolü prosedürleri
	CM.L2-3.4.6 *En Az İşlevsellik* Yalnızca temel yetenekleri sağlamak için organizasyonel sistemleri yapılandırarak en az işlevsellik ilkesini kullanın.		Bulunmuyor

Çizelge 4.16.(devam) “CM-Konfigürasyon Yönetimi” alanı karşılıkları

	CM.L2-3.4.7 *Gereksiz İşlevsellik* Gerekli olmayan programların, işlevlerin, bağlantı noktalarının, protokollerin ve hizmetlerin kullanımını kısıtlayın, devre dışı bırakın veya önleyin.		Bulunmuyor
	CM.L2-3.4.8 *Uygulama Yürütme Politikası* Yetkisiz yazılımların kullanımını önlemek için özel durumla reddet (kara listeye alma) ilkesini veya yetkili yazılımın yürütülmesine izin vermek için tümünü reddet, özel durumla izin ver (beyaz listeye alma) ilkesini uygulayın.		A.12.2 Kötücül yazılımlardan koruma A.12.2.1 Kötücül yazılımlara karşı kontroller

Çizelge 4.16.(devam) “CM-Konfigürasyon Yönetimi” alanı karşılıkları

	CM.L2-3.4.9 *Kullanıcı Tarafından Yüklenen Yazılım* Kullanıcı tarafından yüklenen yazılımı kontrol edin ve izleyin.		A.12.6 Teknik açıklık yönetimi A.12.6.2 Yazılım kurulumu kısıtlamaları

4.4.5. “IA-Tanımlama ve Doğrulama” alanı karşılıkları

CMMC v2.0’da bulunan “IA-Tanımlama ve Doğrulama” konu alanında yer alan uygulamaların ISO/IEC 27001 standardındaki karşılıkları Çizelge 4.17. ile belirtilmiştir.

Çizelge 4.17. “IA-Tanımlama ve Doğrulama” alanı karşılıkları.

CMMC v2.0		**ISO IEC 27001**	
IA-Tanımlama ve Doğrulama			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
IA.L1-3.5.1 *Tanılama* Bilgi sistemi kullanıcılarını, kullanıcılar adına hareket eden süreçleri veya cihazları tanımlayın.	IA.L2-3.5.3 *Çok Faktörlü Kimlik Doğrulama* Ayrıcalıklı hesaplara yerel ve ağ erişimi için ve ayrıcalığı olmayan hesaplara ağ erişimi için çok faktörlü kimlik doğrulamayı kullanın.	A.9.2 Kullanıcı erişim yönetimi A.9.2.1 Kullanıcı kaydetme ve kayıt silme	Bulunmuyor

Çizelge 4.17.(devam) “IA-Tanımlama ve Doğrulama” alanı karşılıkları

IA.L1-3.5.2 *Kimlik doğrulama* Kurumsal bilgi sistemlerine erişime izin vermek için bir ön koşul olarak bu kullanıcıların, süreçlerin veya cihazların kimliklerini doğrulayın.	IA.L2-3.5.4 *Tekrara Dayanıklı Kimlik Doğrulama* Ayrıcalıklı ve ayrıcalıklı olmayan hesaplara ağ erişimi için tekrara dayanıklı kimlik doğrulama mekanizmalarını kullanın.	Bulunmuyor	A.9.3 Kullanıcı sorumlulukları A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı
	IA.L2-3.5.5 *Tanımlayıcı Yeniden Kullanımı* Tanımlayıcıların belirli bir süre boyunca yeniden kullanılmasını önleyin.		Bulunmuyor
	IA.L2-3.5.6 *Tanımlayıcı İşleme* Belirli bir hareketsizlik süresinden sonra tanımlayıcıları devre dışı bırakın.		Bulunmuyor

Çizelge 4.17.(devam) “IA-Tanımlama ve Doğrulama” alanı karşılıkları

	IA.L2-3.5.7 *Şifre Karmaşıklığı* Yeni parolalar oluşturulduğunda minimum parola karmaşıklığı ve karakter değişikliği uygulayın.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.3 Parola yönetim sistemi
	IA.L2-3.5.8 *Şifre Yeniden Kullanımı* Belirli sayıda dönem için parolanın yeniden kullanılmasını yasaklayın.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.3 Parola yönetim sistemi
	IA.L2-3.5.9 *Geçici Şifreler* Kalıcı bir parolayla anında değişiklik yaparak sistem oturumları için geçici parola kullanımına izin verin.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.3 Parola yönetim sistemi

Çizelge 4.17.(devam) “IA-Tanımlama ve Doğrulama” alanı karşılıkları

	IA.L2-3.5.10 *Kriptografik Olarak Korunan Şifreler* Yalnızca kriptografik olarak korunan parolaları saklayın ve iletin.		Bulunmuyor
	IA.L2-3.5.11 *Belirsiz Geri Bildirim* Kimlik doğrulama bilgileri ile ilgili belirsiz geri bildirim yap.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.2 Güvenli oturum açma prosedürleri

4.4.6. "IR-Olay Müdahalesi" alanı karşılıkları

CMMC v2.0'da bulunan "IR-Olay Müdahalesi" konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.18. ile belirtilmiştir.

Çizelge 4.18. "IR-Olay Müdahalesi" alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
IR-Olay Müdahalesi			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	IR.L2-3.6.1 *Olay Yönetimi* Hazırlık, tespit, analiz, muhafaza, kurtarma ve kullanıcı müdahale faaliyetlerini içeren kurumsal sistemler için operasyonel bir olay işleme yeteneği oluşturun.		A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.1 Sorumluluklar ve prosedürler
	IR.L2-3.6.2 *Olay Raporlama* Olayları takip edin, belgeleyin ve kuruluş içindeki ve dışındaki belirlenmiş görevlilere ve/veya yetkililere bildirin.		A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.2 Bilgi güvenliği olaylarının raporlanması

Çizelge 4.18.(devam) “IR-Olay Müdahalesi” alanı karşılıkları

	IR.L2-3.6.3 *Olay Müdahale Testi* Kurumsal olay yanıt yeteneğini test edin.		Bulunmuyor

4.4.7. “MA-Bakım” alanı karşılıkları

CMMC v2.0’da bulunan “MA-Bakım” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.19. ile belirtilmiştir.

Çizelge 4.19. “MA-Bakım” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
MA-Bakım			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	MA.L2-3.7.1 *Bakım Yap* Organizasyonel sistemlerde bakım gerçekleştirin.		A.11.2 Teçhizat A.11.2.4 Teçhizat bakımı

Çizelge 4.19.(devam) “MA-Bakım” alanı karşılıkları

	MA.L2-3.7.2 *Sistem Bakım Kontrolü* Sistem bakımını yürütmek için kullanılan araçlar, teknikler, mekanizmalar ve personel üzerinde kontroller sağlayın.		A.11.2 Teçhizat A.11.2.4 Teçhizat bakımı
	MA.L2-3.7.3 *Ekipman Sanitasyonu* Tesis dışı bakım için kaldırılan ekipmanın herhangi bir CUI'den arındırıldığından emin olun.		A.11.2 Teçhizat A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği
	MA.L2-3.7.4 *Medya Denetimi* Medya kurumsal sistemlerde kullanılmadan önce, tanılama ve test programlarını içeren medyayı kötü amaçlı kod açısından kontrol edin.		Bulunmuyor

Çizelge 4.19.(devam) “MA-Bakım” alanı karşılıkları

	MA.L2-3.7.5 Yerel Olmayan Bakım Harici ağ bağlantıları aracılığıyla yerel olmayan bakım oturumları oluşturmak ve yerel olmayan bakım tamamlandığında bu tür bağlantıları sonlandırmak için çok faktörlü kimlik doğrulaması gerektir.		Bulunmuyor
	MA.L2-3.7.6 *Bakım Personeli* Gerekli erişim yetkisi olmayan bakım personelinin bakım faaliyetlerini denetleyin.		A.11.2 Teçhizat A.11.2.4 Teçhizat bakımı

4.4.8. “MP-Medya Koruması” alanı karşılıkları

CMMC v2.0’da bulunan “MP-Medya Koruması” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.20. ile belirtilmiştir.

Çizelge 4.20. “MP-Medya Koruması” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
MP-Medya Koruması			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
MP.L1-3.8.3 *Medya İmhası* Federal Sözleşme Bilgilerini (FCI) içeren bilgi sistemi ortamını atmadan veya yeniden kullanım için serbest bırakmadan önce sanitize veya imha edin.	MP.L2-3.8.1 *Medya Koruması* Hem kâğıt hem de dijital olarak CUI içeren sistem ortamını koruyun (örn. fiziksel olarak kontrol edin ve güvenli bir şekilde saklayın).	A.11.2 Teçhizat A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı	A.8.3 Ortam işleme 8.3.1 Taşınabilir ortam yönetimi
	MP.L2-3.8.2 *Medya Erişimi* Sistem ortamındaki CUI'ye erişimi yetkili kullanıcılarla sınırlayın.		Bulunmuyor

Çizelge 4.20.(devam) “MP-Medya Koruması” alanı karşılıkları

	MP.L2-3.8.4 *Medya İşaretleri* Medyayı gerekli CUI işaretleri ve dağıtım sınırlamaları ile işaretleyin.		A.8.2 Bilgi sınıflandırma A.8.2.2 Bilgi etiketlemesi
	MP.L2-3.8.5 *Medya Sorumluluğu* CUI içeren medyaya erişimi kontrol edin ve kontrollü alanların dışına taşıma sırasında medya için hesap verebilirliği sağlayın.		Bulunmuyor

Çizelge 4.20.(devam) “MP-Medya Koruması” alanı karşılıkları

	MP.L2-3.8.6 *Taşınabilir Depolama Şifrelemesi* Alternatif fiziksel güvenlik önlemleriyle korunmadığı sürece, taşıma sırasında dijital ortamda depolanan CUI'nin gizliliğini korumak için kriptografik mekanizmalar uygulayın.		A.8.3 Ortam işleme A.8.3.3 Fiziksel ortam aktarımı
	MP.L2-3.8.7 *Çıkarılabilir Medya* Sistem bileşenlerinde çıkarılabilir medya kullanımını kontrol edin.		A.8.3 Ortam işleme A.8.3.1 Taşınabilir ortam yönetimi

Çizelge 4.20.(devam) “MP-Medya Koruması” alanı karşılıkları

	MP.L2-3.8.8 *Paylaşılan Medya* Bu tür cihazların tanımlanabilir bir sahibi olmadığında taşınabilir depolama cihazlarının kullanımını yasaklayın.		Bulunmuyor
	MP.L2-3.8.9 *Yedeklemeleri Koruyun* Depolama konumlarında yedek CUI'nin gizliliğini koruyun.		A.12.3 Yedekleme A.12.3.1 Bilgi yedekleme

4.4.9. “PS-Personel Güvenliği” alanı karşılıkları

CMMC v2.0’da bulunan “PS-Personel Güvenliği” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.21. ile belirtilmiştir.

Çizelge 4.21. “PS-Personel Güvenliği” alanı karşılıkları.

CMMC v2.0		**ISO IEC 27001**	
PS-Personel Güvenliği			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	PS.L2-3.9.1 *Bireyleri Tarayın* CUI içeren kurumsal sistemlere erişim yetkisi vermeden önce bireyleri tarayın.		A.7.1 İstihdam öncesi A.7.1.1 Tarama
	PS.L2-3.9.2 *Personel İşlemleri* Sonlandırma ve transferler gibi personel eylemleri sırasında ve sonrasında CUI içeren kurumsal sistemlerin korunmasını sağlayın.		A.7.3 İstihdamın sonlandırılması ve değiştirilmesi A.7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi

4.4.10. “PE-Fiziksel Koruma” alanı karşılıkları

CMMC v2.0’da bulunan “PE-Fiziksel Koruma” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.22. ile belirtilmiştir.

Çizelge 4.22. “PE-Fiziksel Koruma” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
PE-Fiziksel Koruma			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
PE.L1-3.10.1 *Fiziksel Erişimi Sınırla* Kurumsal bilgi sistemlerine, ekipmana ve ilgili işletim ortamlarına fiziksel erişimi yetkili kişilerle sınırlandırın.	PE.L2-3.10.2 *Tesisi İzle* Fiziksel tesisi koruyun ve izleyin ve 80rganizasyonel sistemler için altyapıyı destekleyin.	A.11.1 Güvenli alanlar A.11.1.1 Fiziksel güvenlik sınırı	A.11.1 Güvenli alanlar A.11.1.1 Fiziksel güvenlik sınırı
PE.L1-3.10.3 *Ziyaretçilere Eşlik Et* Ziyaretçilere eşlik edin ve ziyaretçi etkinliğini izleyin.	PE.L2-3.10.6 *Alternatif Çalışma Sahaları* Alternatif çalışma sahalarında CUI için koruma önlemleri uygulayın.	A.11.1 Güvenli alanlar A.11.1.2 Fiziksel giriş kontrolleri	Bulunmuyor

Çizelge 4.22.(devam) “PE-Fiziksel Koruma” alanı karşılıkları

PE.L1-3.10.4 *Fiziksel Erişim Günlükleri* Fiziksel erişimin denetim günlüklerini koruyun.		A.11.1 Güvenli alanlar A.11.1.2 Fiziksel giriş kontrolleri	
PE.L1-3.10.5 *Fiziksel Erişimi Yönet* Fiziksel erişim cihazlarını kontrol edin ve yönetin.		A.11.2 Teçhizat A.11.2.1 Teçhizat yerleştirme ve koruma	

4.4.11. “RA-Risk Değerlendirme” alanı karşılıkları

CMMC v2.0’da bulunan “PE-Fiziksel Koruma” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.23. ile belirtilmiştir.

Çizelge 4.23. “RA-Risk Değerlendirme” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
RA-Risk Değerlendirme			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	RA.L2-3.11.1 *Risk Değerlendirmesi* Kurumsal sistemlerin işleyişinden ve ilgili işleme, depolama veya CUI iletiminden kaynaklanan kurumsal operasyonlara (misyon, işlevler, imaj veya itibar dahil), kurumsal varlıklara ve bireylere yönelik riski periyodik olarak değerlendirin.		6 Planlama 6.1 Risk ve fırsatları ele alan faaliyetler 8 İşletim 8.1 İşletimsel planlama ve kontrol

Çizelge 4.23.(devam) “RA-Risk Değerlendirme” alanı karşılıkları

	RA.L2-3.11.2 *Güvenlik Açığı Taraması* Düzenli aralıklarla ve bu sistemleri ve uygulamaları etkileyen yeni güvenlik açıkları belirlendiğinde, kurumsal sistemlerdeki ve uygulamalardaki güvenlik açıklarını tarayın.		A.12.6 Teknik açıklık yönetimi A.12.6.1 Teknik açıklıkların yönetimi
	RA.L2-3.11.3 *Güvenlik Açığı Giderme* Güvenlik açıklarını risk değerlendirmelerine göre giderin.		A.12.6 Teknik açıklık yönetimi A.12.6.1 Teknik açıklıkların yönetimi

4.4.12. “CA-Güvenlik Değerlendirmesi” alanı karşılıkları

CMMC v2.0’da bulunan “CA-Güvenlik Değerlendirmesi” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.24. ile belirtilmiştir.

Çizelge 4.24. “CA-Güvenlik Değerlendirmesi” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
CA-Güvenlik Değerlendirmesi			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
	CA.L2-3.12.1 *Güvenlik Kontrol Değerlendirmesi* Kontrollerin uygulamalarında etkili olup olmadığını belirlemek için kurumsal sistemlerdeki güvenlik kontrollerini periyodik olarak değerlendirin.		9 Performans değerlendirme 9.1 İzleme, ölçme, analiz ve değerlendirme A.18.2 Bilgi güvenliği gözden geçirmeleri A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirmesi

Çizelge 4.24.(devam) “CA-Güvenlik Değerlendirmesi” alanı karşılıkları

	CA.L2-3.12.2 *Eylem Planı* Kurumsal sistemlerdeki eksiklikleri gidermek ve güvenlik açıklarını azaltmak veya ortadan kaldırmak için tasarlanmış eylem planları geliştirin ve uygulayın.		6 Planlama 6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama
	CA.L2-3.12.3 *Güvenlik Kontrol İzleme* Kontrollerin etkinliğinin devam etmesini sağlamak için güvenlik kontrollerini sürekli olarak izleyin.		8 İşletim 8.1 İşletimsel planlama ve kontrol

Çizelge 4.24.(devam) “CA-Güvenlik Değerlendirmesi” alanı karşılıkları

	CA.L2-3.12.4 *Sistem Güvenlik Planı* Sistem sınırlarını, sistem çalışma ortamlarını, güvenlik gereksinimlerinin nasıl uygulandığını ve diğer sistemlerle ilişkileri veya diğer sistemlerle olan bağlantıları açıklayan sistem güvenlik planlarını geliştirin, belgeleyin ve periyodik olarak güncelleyin.		8 İşletim 8.1 İşletimsel planlama ve kontrol

4.4.13. “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

CMMC v2.0’da bulunan “SC-Sistem ve Haberleşme Koruması” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.25. ile belirtilmiştir.

Çizelge 4.25. “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

CMMC v2.0		**ISO IEC 27001**	
SC-Sistem ve Haberleşme Koruması			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
SC.L1-3.13.1 Sınır Koruması Bilgi sistemlerinin dış sınırlarında ve temel iç sınırlarında kurumsal iletişimleri (örn. kurumsal bilgi sistemleri tarafından iletilen veya alınan bilgiler) izleyin, kontrol edin ve koruyun.	SC.L2-3.13.2 *Güvenlik Mühendisliği* Kurumsal sistemlerde etkin bilgi güvenliğini destekleyen mimari tasarımları, yazılım geliştirme tekniklerini ve sistem mühendisliği ilkelerini kullanın.	A.13.1 Ağ güvenliği yönetimi A.13.1.1 Ağ kontrolleri	A.14.2 Geliştirme ve destek süreçlerinde güvenlik A.14.2.5 Güvenli sistem mühendisliği prensipleri

Çizelge 4.25.(devam) “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

SC.L1-3.13.5 *Genel Erişim Sistemi Ayrımı* Dahili ağlardan fiziksel veya mantıksal olarak ayrılmış, genel olarak erişilebilir sistem bileşenleri için alt ağlar uygulayın.	SC.L2-3.13.3 *Rol Ayrımı* Kullanıcı işlevselliğini sistem yönetimi işlevselliğinden ayırın.	A.13.1 Ağ güvenliği yönetimi A.13.1.3 Ağlarda ayrım	A.6.1 İç organizasyon A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları
	SC.L2-3.13.4 *Paylaşılan Kaynak Kontrolü* Paylaşılan sistem kaynakları aracılığıyla yetkisiz ve istenmeyen bilgi aktarımını önleyin.		Bulunmuyor
	SC.L2-3.13.6 *İstisnaya Göre Ağ İletişimi* Varsayılan olarak ağ iletişim trafiğini reddet ve ağ iletişim trafiğine istisnaya göre izin ver (örn. hepsini reddet, istisnaya göre izin ver).		A.13.1 Ağ güvenliği yönetimi A.13.1.2 Ağ hizmetlerinin güvenliği

Çizelge 4.25.(devam) “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

	SC.L2-3.13.7 *Bölünmüş Tünelleme* Uzak cihazların aynı anda kurumsal sistemlerle uzaktan olmayan bağlantılar kurmasını ve harici ağlardaki kaynaklara başka bir bağlantı aracılığıyla iletişim kurmasını (örn. bölünmüş tünelleme) önleyin.		Bulunmuyor
	SC.L2-3.13.8 *Aktarılan Veriler* Alternatif fiziksel güvenlik önlemleriyle korunmadığı sürece, iletim sırasında CUI'nin yetkisiz ifşasını önlemek için kriptografik mekanizmalar uygulayın.		A.13.2 Bilgi transferi A.13.2.1 Bilgi transfer politikaları ve prosedürleri

Çizelge 4.25.(devam) “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

	SC.L2-3.13.9 *Bağlantı Sonlandırma* Oturumların sonunda veya belirli bir etkinlik dışı kalma süresinden sonra iletişim oturumlarıyla ilişkili ağ bağlantılarını sonlandırın.		A.11.2 Teçhizat A.11.2.8 Gözetimsiz kullanıcı teçhizatı
	SC.L2-3.13.10 *Anahtar Yönetimi* Kurumsal sistemlerde kullanılan kriptografi için kriptografik anahtarlar oluşturun ve yönetin.		A.10.1 Kriptografik kontroller A.10.1.2 Anahtar yönetimi
	SC.L2-3.13.11 *CUI Şifrelemesi* CUI'nin gizliliğini korumak için kullanıldığında FIPS onaylı şifreleme kullanın.		Bulunmuyor

Çizelge 4.25.(devam) “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

	SC.L2-3.13.12 *Ortak Cihaz Kontrolü* Ortak bilgi işlem cihazlarının uzaktan etkinleştirilmesini yasaklayın ve cihazda bulunan kullanıcılara kullanımda olan cihazların göstergesini sağlayın.		Bulunmuyor
	SC.L2-3.13.13 *Mobil Kod* Mobil kodun kullanımını kontrol edin ve izleyin.		Bulunmuyor
	SC.L2-3.13.14 *İnternet Protokolü Üzerinden Ses* İnternet Üzerinden Ses Protokolü (VoIP) teknolojilerinin kullanımını kontrol edin ve izleyin.		A.13.2 Bilgi transferi A.13.2.1 Bilgi transfer politikaları ve prosedürleri

Çizelge 4.25.(devam) “SC-Sistem ve Haberleşme Koruması” alanı karşılıkları

	SC.L2-3.13.15 *İletişim Güvenilirliği* İletişim oturumlarının güvenilirliğini koruyun.		A.13.1 Ağ güvenliği yönetimi A.13.1.1 Ağ kontrolleri
	SC.L2-3.13.16 *Duran Veriler* Bekleyen CUI'nin gizliliğini koruyun.		A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum A.18.1.3 Kayıtların korunması

4.4.14. “SI-Sistem ve Bilgi Bütünlüğü” alanı karşılıkları

CMMC v2.0’da bulunan “SI-Sistem ve Bilgi Bütünlüğü” konu alanında yer alan uygulamaların ISO/IEC 27001 standardında yer alan karşılıkları Çizelge 4.26. ile belirtilmiştir.

Çizelge 4.26. “SI-Sistem ve Bilgi Bütünlüğü” alanı karşılıkları.

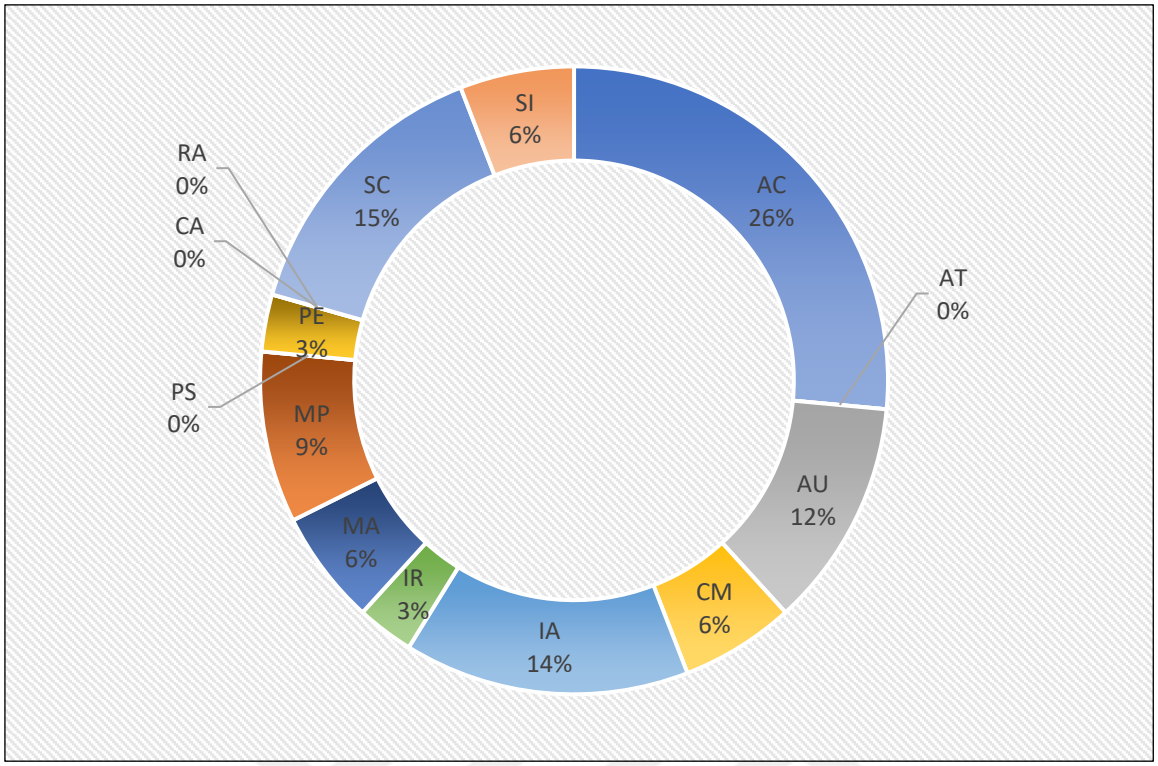
CMMC v2.0		**ISO IEC 27001**	
SI-Sistem ve Bilgi Bütünlüğü			
Seviye 1	**Seviye 2**	**Seviye 1 Karşılığı**	**Seviye 2 Karşılığı**
SI.L1-3.14.1 *Kusur Giderme* Bilgi ve bilgi sistemi kusurlarını zamanında tespit edin, raporlayın ve düzeltin.	SI.L2-3.14.3 *Güvenlik Uyarıları ve Önerileri* Sistem güvenlik uyarılarını ve önerilerini izleyin ve karşılık vermek üzere harekete geçin.	A.12.6 Teknik açıklık yönetimi A.12.6.1 Teknik açıklıkların yönetimi	A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.1 Sorumluluklar ve prosedürler
SI.L1-3.14.2 *Kötü Amaçlı Kod Koruması* Kurumsal bilgi sistemleri içinde uygun yerlerde kötü amaçlı kodlara karşı koruma sağlayın.	SI.L2-3.14.6 *Saldırılar için İletişimi İzleyin* Saldırıları ve olası saldırıların göstergelerini tespit etmek için gelen ve giden iletişim trafiği dahil olmak üzere kurumsal sistemleri izleyin.	Bulunmuyor	A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.1 Sorumluluklar ve prosedürler

Çizelge 4.26.(devam) “SI-Sistem ve Bilgi Bütünlüğü” alanı karşılıkları

SI.L1-3.14.4 *Kötü Amaçlı Kod Korumasını Güncelle* Yeni sürümler çıktığında kötü amaçlı kod koruma mekanizmalarını güncelleyin.	SI.L2-3.14.7 *Yetkisiz Kullanımı Tanımlayın* Organizasyonel sistemlerin yetkisiz kullanımını tanımlayın.	Bulunmuyor	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.1.1 Erişim kontrol politikası
SI.L1-3.14.5 *Sistem ve Dosya Tarama* Dosyalar indirilirken, açılırken veya yürütülürken, bilgi sisteminin periyodik taramalarını ve harici kaynaklardan gelen dosyaların gerçek zamanlı taramalarını gerçekleştirin.		A.12.2 Kötücül yazılımlardan koruma A.12.2.1 Kötücül yazılımlara karşı kontroller	

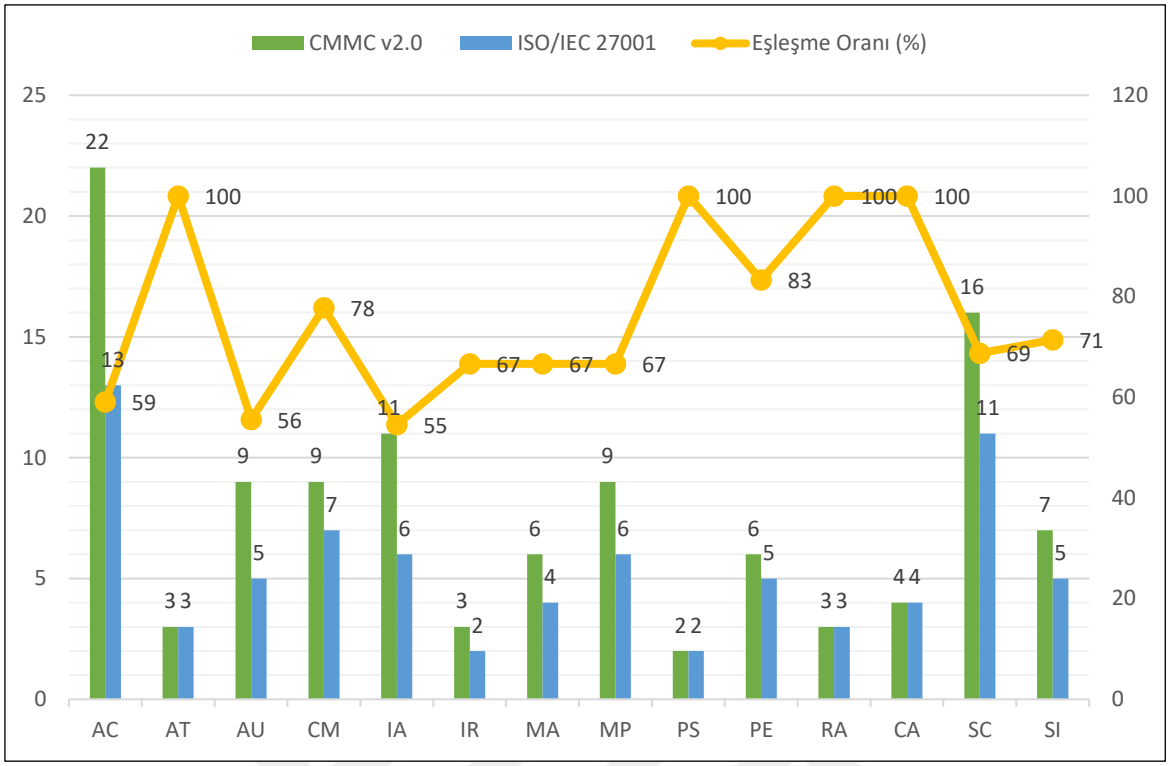
Yukarıdaki tablolardan görüldüğü üzere toplam 14 farklı alanda ve 2 farklı seviyede toplam 110 adet CMMC uygulaması bulunmaktadır. Yapılan çalışma sonucunda bunların 34 tanesinin ISO/IEC 27001 standardı kapsamında karşılıkları bulunmadığı görülmüştür.

Karşılığı bulunmayan CMMC v2.0 uygulamalarının alanlarına göre dağılımı ile uygulamaların alanlarına ve seviyelerine göre ISO/IEC 27001 karşılık sayıları ve oranları aşağıdaki şekiller ile gösterilmiştir.



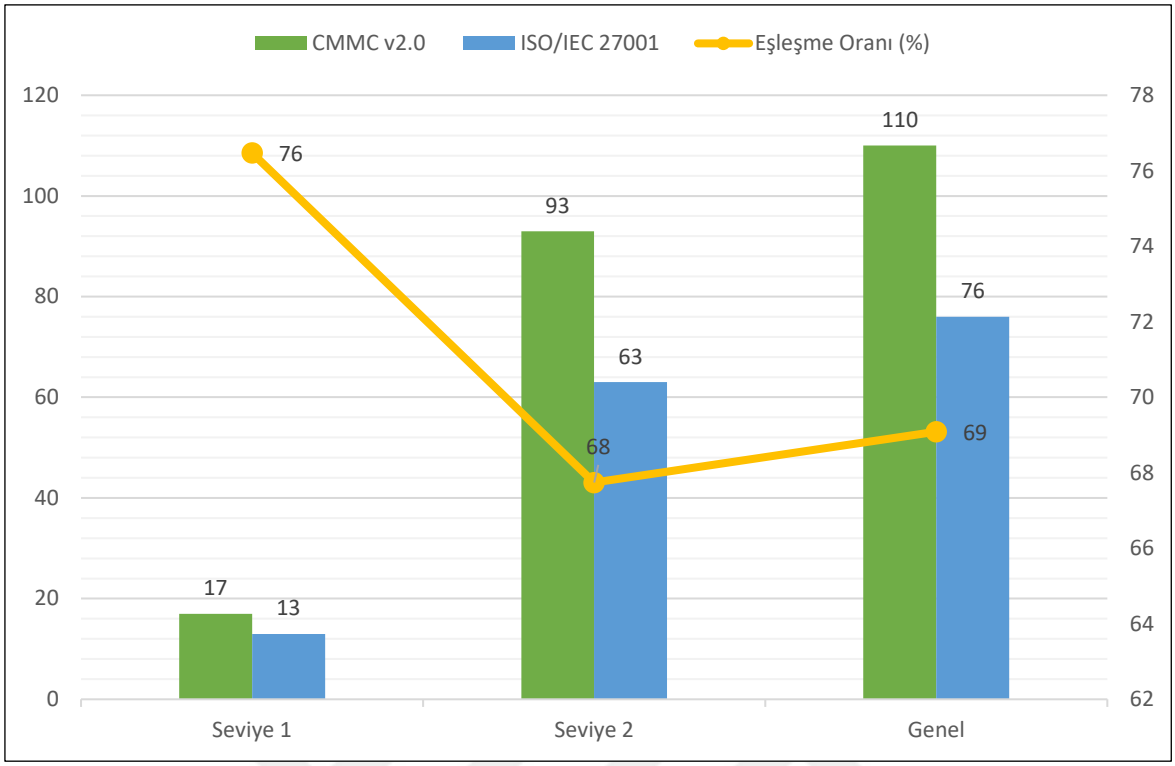
Şekil 4.1. ISO/IEC 27001'de karşılığı bulunmayan CMMC v2.0 uygulamalarının dağılımı

Şekil 4.1. ile görüldüğü üzere ISO/IEC 27001 Standardında karşılığı bulunmayan CMMC v2.0 uygulamalarının en çok olduğu alanlar sırasıyla; "AC-Erişim Kontrolü", "SC-Sistem ve Haberleşme Koruması", "IA-Tanımlama ve Doğrulama", "AU-Denetim ve Hesap Verebilirlik", "MP-Medya Koruması", "MA-Bakım", "CM-Konfigürasyon Yönetimi", "IR-Olay Müdahalesi", "PE-Fiziksel Koruma", "RA-Risk Değerlendirme", "CA-Güvenlik Değerlendirmesi", "PS-Personel Güvenliği", "AT-Farkındalık ve Eğitim" alanları olmaktadır.



Şekil 4.2. CMMC v2.0 uygulamalarının alanlarına göre karşılık sayıları ve oranları

Bununla birlikte Şekil 4.2. ile gösterilen CMMC v2.0'nin uygulama alanları bazında ISO/IEC 27001 Standardı ile eşleşme oranlarına bakıldığında en düşük eşleşme oranına sahip alanların sırasıyla; "IA-Tanımlama ve Doğrulama", "AU-Denetim ve Hesap Verebilirlik", "AC-Erişim Kontrolü", "IR-Olay Müdahalesi", "MA-Bakım", "MP-Medya Koruması", "SC-Sistem ve Haberleşme Koruması", "SI-Sistem ve Bilgi Bütünlüğü", "CM-Konfigürasyon Yönetimi", "PE-Fiziksel Koruma", "RA-Risk Değerlendirme", "CA-Güvenlik Değerlendirmesi", "PS-Personel Güvenliği", "AT-Farkındalık ve Eğitim" olduğu görülmektedir.



Şekil 4.3. CMMC v2.0 uygulamalarının seviyelere göre karşılık sayıları ve oranları

Şekil 4.3.'de gösterilen CMMC v2.0'nin uygulamaların seviyeleri bazında ISO/IEC 27001 Standardı ile eşleşme oranlarına bakıldığında ise Seviye 1 için %76 olan eşleşme oranının Seviye 2'ye gelindiğinde %68'e gerilediği ve genelde uygulamalar arası eşleşme oranının %69 seviyesinde olduğu görülmektedir.

5. SONUÇ VE ÖNERİLER

Gelişen teknoloji ile birlikte sürekli değişen ve dönüşen günümüz dünyasında bilginin önemi giderek daha da artmaktadır. Bunun sonucu olarak da "Bilgi" ve onu muhteva eden alt yapılar, artan önemlerine paralel olarak daha fazla saldırıya ve güvenlik riskine maruz kalmaktadır.

Bu duruma çerçevesinde, mevcut bilgi güvenliği yönetimi alt yapılarının da artan saldırı ve güvenlik risklerini karşılayacak şekilde güncellenerek geliştirilmesi, gerektiğinde ihtiyaca yönelik yeni modellerin oluşturularak mevcut sistemlere entegrasyonun sağlanması gerekmektedir.

Dünya çapında bilgi güvenliğine yönelik artan tehdit ve riskler, ülkemiz özelinde milli savunma sanayinin önemi ve gelişme potansiyeli ile birlikte değerlendirildiğinde, savunma sanayi sektörüne özel daha ayrıntılı tanımlanmış etkin tedbirlerin alınmasının ne kadar önemli olduğu ortaya çıkmaktadır.

Bu çalışmada yukarıdaki perspektife bağlı olarak, bilgi güvenliği yönetimi sistemlerinin gelişim ve dönüşüm süreçlerinin farklı aşamalarına ait iki ayrı bilgi güvenliği yönetimi modeli olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ile ABD Siber Güvenlik Olgunluk Modeli Sertifikasyonu-CMMC v2.0 uygulamaları ele alınmıştır.

Bu kapsamda elde edilen ve çalışmada ifade edilen bulgular çerçevesinde, günümüzde birçok sektörde olduğu gibi bu çalışma kapsamına dahil edilen 6 adet savunma sanayi kuruluşunda da ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı uygulamalarının en yaygın şekilde kullanıldığı anlaşılmıştır.

Buna ilave olarak Ek-2'de verilen soru listesinde yer alan sorulara bu kuruluşlar tarafından verilen cevaplara göre;

- Kuruluşların tamamı için bir bilgi güvenliği politikasının oluşturulmuş olması,
- Kuruluşlarda, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi (CB DDO BİGR) ve ISO/IEC 27001 Standardı dışında

faydalanılan uygulamalar içerisinde CMMC modeli için faydalanılanlara benzer NIST standartlarının da bulunuyor olması,

- Kuruluşların bir tanesi haricinde tamamının CMMC modeli hakkında farkındalığa sahip olması,
- Bunun yanında kuruluşların çoğunun gelecekte CMMC belgesine sahip olmasının gerekeceğini düşünüyor olması,

dikkat çekicidir.

Yine bu çalışma ile hali hazırda savunma sanayi kuruluşlarında bilgi güvenliği alt yapılarına entegrasyonu sağlanarak gereksinimleri karşılanmış bulunan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ile ABD Siber Güvenlik Olgunluk Modeli Sertifikasyonu-CMMC v2.0, kapsamlarında yer alan gereksinimleri bakımından karşılaştırılmış, bu karşılaştırma sonucunda CMMC v2.0'da bulunan bir takım güvenlik uygulamalarına ISO/IEC 27001 Standardı kapsamında yer verilmediği görülmüştür.

Buna göre;

- CMMC v2.0 kapsamında tanımlanan 4 adet alanın: "RA-Risk Değerlendirme", "CA-Güvenlik Değerlendirmesi", "PS-Personel Güvenliği", "AT-Farkındalık ve Eğitim", içeriğinde yer alan uygulamalar bakımından ISO/IEC 27001 standardı gereksinimleriyle tümüyle eşleştiği,
- Bunlara ilave olarak CMMC v2.0 kapsamında tanımlanan diğer 8 alanın ise, içeriğinde yer alan uygulamalar bakımından ISO/IEC 27001 standardı gereksinimleriyle kısmen eşleştiği,
- Kısmen eşleşen bu alanlar içerisinde en çok eşleşme oranına sahip olan alanın "PE-Fiziksel Koruma" olduğu,
- Bununla birlikte en az eşleşme oranına sahip olan alanın ise "AU-Denetim ve Hesap Verebilirlik" olduğu,

görülmektedir.

Buradan anlaşılacağı üzere kuruluşların güncel tehdit ve riskleri de göz önünde bulundurarak mevcut tedbirler kapsamında karşılanmadığı değerlendirilen eksik uygulamaları gözden geçirerek mevcut bilgi güvenliği yönetimi alt yapılarına entegre etmeleri gerekmektedir.

Bununla birlikte CMMC 'ye ait modeldeki farklılıklar dolayısıyla, bahse konu eksik uygulamaların kuruluşlardaki mevcut bilgi güvenliği yönetim sistemine entegrasyonu öncesinde, birtakım hususların CMMC modeli çerçevesinde ele alınarak yeniden değerlendirilmesinin uygun olacağı değerlendirilmektedir.

Buna göre kuruluşların öncelikle;

- Bilgi varlıklarını yeniden değerlendirerek sınıflandırması,
- İhtiyaç duyduğu uygulama seviyesini belirlemesi,
- Mevcut dokümantasyon gerekliliklerini yeniden değerlendirmesi,

uygun olacaktır.

Bu bağlamda kuruluşlar uygulayacakları CMMC seviyesi belirleyebilmek için ilk aşamada ilgili başlıkta ifade edilen tanımlar çerçevesinde mevcut bilgi varlıklarını "kamuya açık bilgi", "kamuya açık olmayan federal sözleşme bilgisi (FCI)" ve "kontrollü gizli olmayan bilgi (CUI) programı kapsamında korunması gerekli bilgi" olacak şekilde ayrı ayrı sınıflandırmalıdır.

Bunun için kuruluşlar;

- Yürütmekte olduğu projeleri gözden geçirerek ABD Savunma Bakanlığı'na tedarikçi veya alt tedarikçi konumunda olduğu projeleri tespit etmeli,
- Bu projelere ait sözleşmeleri ve gizlilik taahhütlerini gözden geçirmeli,
- Buna bağlı olarak belirlenen projeler kapsamında yer alan bilgi varlıklarını CMMC modelinde yer alan tanımlara uygun olacak şekilde türlerine göre gruplandırmalı ve bilgi envanterini güncellemeli,
- Etiketleme ve erişim kuralları kullanarak verileri ayrıştırmalı,
- Eksik hususların etkin olarak tespit edilmesini sağlamak için merkezi bir yapı ile kendi içerisinde uyumluluğu değerlendirmeli,

- Personel becerilerinin geliştirilmesine yardımcı olmak için eğitimlerden olanaklarını araştırmalı ve ilgili personelin bu eğitimlere katılımını sağlamalıdır.

Devam eden süreçte ise kuruluş, ISO/IEC 27001'den farklı olarak oluşturulan güncel ve CMMC modeline uygun bilgi envanterini kapsamına alacak şekilde uygulanacak seviyeyi belirlemeli, dokümantasyon alt yapısını seçilen seviye kapsamında güncellemeli ve buna göre faaliyetlerini planlanmalıdır [83].

Bu planlama çerçevesinde kuruluş, yukarıda verilen karşılaştırma tablolarında gösterilen CMMC v2.0'da belirtilen ancak ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardında yer almayan 34 adet uygulamayı öncelikli olarak göz önünde bulundurmalıdır.

Bununla birlikte mevcut CMMC v2.0 kapsamında Seviye 3 uygulamaları henüz oluşturulma aşamasındadır. Bu çalışma tamamlanarak Seviye 3 uygulamaları da CMMC v2.0 kapsamına dahil edildiğinde ISO/IEC 27001 Standardında karşılığı olmayan uygulama sayısının muhtemelen daha da artacağı ön görülmekte olup kuruluşların Seviye 3 uygulamalarının tamamlanma sürecini de yakından takip etmeleri faydalı olacaktır.

Sonuç olarak, çalışmada da belirtildiği üzere ilk bilgi güvenliği yönetimi standardı olan ve İngiliz standardizasyon kuruluşu BSI tarafından 1995 yılında yayınlanan BS 7799 standardı ile başlayan kurumsal ölçekte bilgi güvenliğine yönelik çalışmalar [84], o günden bugüne gelişen ve değişen tehditler ve bunlara bağlı oluşan güvenlik ihtiyaçları doğrultusunda günümüzde en çok kullanılan bilgi güvenliği yönetimi standardı olan ISO/IEC 27001'in güncel halini ortaya çıkarmıştır.

Ancak ISO/IEC 27001 standardı ile kuruluşların faaliyet alanlarından bağımsız ve her ölçekteki organizasyon ve her türde bilgi varlığı için yeterli seviyede koruma sağlayabilecek bir bilgi güvenliği yönetim sisteminin oluşturulmasına yönelik gerekli gereksinimlerin ortaya konması hedeflenmiştir.

Bu doğrultuda ISO/IEC 27001 standardının uygulama ve belgelendirme kapsamının çok geniş olduğu bununla beraber gereksinim bakımından da günümüzde artık temel kabul edilebilecek genel tedbirleri içerdiği görülmektedir.

Fakat günümüzde eskiye oranla çok daha hızlı gelişen ve değişen tehditler, potansiyel hedeflerin türlerini ve sayılarını da arttırarak bilgi güvenliği yönetimi noktasında öncekilerden farklı olarak hem bilgi varlıklarının türüne hem de sektöre özel oluşturulmuş daha ileri seviyede, daha ayrıntılı ve daha etkin bilgi güvenliği tedbirlerinin alınmasını zorunlu kılmıştır.

Bu kapsamda alınan tedbirlerin savunma sanayi özelinde ilk uygulaması ABD Savunma Bakanlığı tarafından CMMC ile hayata geçirilmiştir. Böylece ABD Savunma Bakanlığı başta ulusal güvenliği korumak için diğer paydaşlarıyla birlikte savunma sanayi sektörüne özel kademeli, ayrıntılı ve etkin bir model ortaya koymayı hedeflemiştir.

Bu bağlamda çalışmada elde edilen bulgular çerçevesinde;

- İlerleyen süreçte artan tehdit ve risklerle birlikte sektörden bağımsız olarak oluşturulan ve genel tedbirleri içeren bilgi güvenliği yönetimi modellerinin etkinliklerini yitireceği, erken dönemde farkındalık yaratılması bakımından önemli olan ve günümüzde yaygın olarak kullanılan bu modellerin yerlerini zamanla sektöre ve bilgi türlerine özel oluşturulan kademelendirilmiş bilgi güvenliği uygulamalarını içeren modellere bırakacağı,
- Bu dönüşüm süreci devam ederken ülkemize yönelik siber tehditlerin bertaraf edilmesi bakımından, özellikle kamu ve savunma sanayi sektöründe CMMC ’ye benzer bilgi türlerine ve sektöre özel kademelendirilmiş tedbirleri içeren bilgi güvenliği yönetimi modellerinin ivedilikle oluşturularak uygulanmaya başlamasının ülkemizin ulusal güvenliği bakımından kritik öneme sahip olduğu,
- Bununla ilgili olarak, gelecekte ülkemizde uygulanacak siber güvenlik yol haritasının belirtildiği 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde ülkemiz savunma sanayine özel herhangi bir uygulamanın oluşturulmadığı görüldüğünden, yeni hazırlanacak strateji ve eylem planında böyle bir modele yer verilebilmesi için hazırlık çalışmalarına vakit kaybetmeksizin başlanmasının gerektiği,
- Bu kapsamda yapılacak hazırlık çalışmalarına öncü olmak bakımından milli standardizasyon kuruluşu olan Türk Standardları Enstitüsü’nün de mevcut ulusal ve uluslararası bilgi güvenliği yönetimi standartlarından referans alarak milli savunma sanayine yönelik model standart oluşturmasının önem arz ettiği,

- Uluslararası alanda önemli başarılara imza atmış milli savunma sanayi kuruluşlarının gelecekte potansiyel olarak tedarikçisi olacağı kuruluşlarca veya devletlerce gerçekleştirilmesi talep edilebilecek olan CMMC gereksinimleri ile ilgili önceden hazırlıklı olmak amacıyla bilgi güvenliği yönetimi faaliyetlerinde bünyesinde görev verdiği personeline ilgili eğitimleri ivedilikle aldırmasının faydalı olacağı,
- Çalışmanın devamı olarak, henüz yayınlanmamış olan CMMC v2.0 Seviye 3 uygulamalarının da yayınlanması sonrasında Seviye 1 ve 2 uygulamalarına Seviye 3 uygulamalarının da eklenerek daha kapsamlı bir araştırmanın yapılabileceği,

değerlendirilmektedir.

KAYNAKLAR

1. Atasoy, İ. ve Ormanlı, O. (2009). Teknoloji ve Siber Güvenlik: Dijital Toplumun Geleceği. *İstanbul Aydın Üniversitesi Dergisi*, 11 (4), 399-409.

2. Soto-Acosta, P. (2020). COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear. *Information Systems Management*, 37 (4), 260-266.

3. Patil, S. and Mishra, V. (2022). Democracy, Technology, Geopolitics. *RAISINA FILES*, 28 (1), 28-34.

4. Akçoraoğlu, A., (2019). Yeni Kapitalizm Teorileri Dijital Devrim ve Türkiye Kapitalizmi. *Mülkiye Dergisi*, 43 (3), 525-575.

5. Canbek, G. ve Sağıroğlu, Ş. (2008). Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(1), 165-180.

6. Zviran, M. and Haga, W. J. (2015). Password Security: An Empirical Study. *Journal of Management Information Systems*, 15 (4), 161-185.

7. İnternet: McAfee, The Economic Impact of Cybercrime—No Slowing Down Executive Summary. URL: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf, Son Erişim Tarihi: 01.06.2022.

8. Internet: The Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy. URL: https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/, Son Erişim Tarihi: 01.06.2022.

9. Sağıroğlu, Ş., Alkan, M., Samet, R. (2018). *Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık*. Ankara: Grafiker Yayıncılık, 42-45.

10. Srinivas, J., Das, A. K., Kumar N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92 (1), 178-188.

11. Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit-DuD*, 35 (1), 7-11.

12. Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., ... & Khan, A. W. (2021). Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. *ACM Computing Surveys (CSUR)*, 54 (3), 1-36.

13. Scarfone, K., Benigni, D., & Grance, T. (2009). Cyber security standards. *National Institute of Standards and Technology (NIST), Gaithersburg, Maryland*.

14. Ziylan, A. (2004). Ulusal Teknoloji Yeteneği ve Savunma Sanayii. *Savunma Sanayicileri Derneği*, 2004 (1).

15. Şişman, D. (2017). Küreselleşme, kriz ve savunma sanayi. *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 39 (1), 223-237.

16. Cheung, T.M. (2021). A conceptual framework of defence innovation. *Journal of Strategic Studies*, 44 (6), 1-27.

17. Eceral, T. Ö. (2017). Türk Savunma ve Havacılık Sanayisinin Küresel, Ulusal ve Yerel Dinamikleri: Ankara Örneği. *Gazi Akademik Bakış*, 11 (21), 87-106.

18. Çiçek, E. ve Bay, M. (2007). Stratejik Küresel Tedarik Zinciri Yönetimi ve Lojistik. *Sosyal Ekonomik Araştırmalar Dergisi*, 7 (13), 91-117.

19. İnternet: CMMC Home Page. URL: https://www.acq.osd.mil/cmmc/index.html, Son Erişim Tarihi: 13.02.2022.

20. Selinger, J. (2022). The Dod's Cybersecurity Maturity Model Certification and Resulting Tensions with U.S. Standard-Setting Policy and Established it Security Authorities. *SSRN Electronic Journal*, 3985000.

21. Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J. and Modaresnezhad, M. (2021). Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base. *Proceedings of the Conference on Information Systems Applied Research* , 2167 (1), 1508.

22. İnternet: WatchGuard: Türkiye'de 2021'in ilk yarısında 288 bini aşkın siber saldırı gerçekleşti. URL: https://tr.investing.com/news/markets/watchguard-turkiyede-2021in-ilk-yarsnda-288-bini-askn-siber-saldr-gerceklesti-2153670, Son Erişim Tarihi: 01.06.2022.

23. Yeşilyurt, F. ve Yeşilyurt, M.E. (2019). Türkiye'de Savunma Sanayi. *Pamukkale Journal of Eurasian Socioeconomic Studies*, 6 (2), 1-42.

24. İnternet: World military expenditure passes $2 trillion for first time | SIPRI. URL: https://sipri.org/media/press-release/2022/world-military-expenditure-passes-2-trillion-first-time, Son Erişim Tarihi: 07.05.2022.

25. İnternet: OUSD A&S – CMMC MODEL. URL: https://www.acq.osd.mil/cmmc/model.html, Son Erişim Tarihi: 08.05.2022.

26. Humphreys, E., (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13 (4), 247-255.

27. Hsu, C., Wang, T., and Lu, A. (2016). The impact of ISO 27001 certification on firm performance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2016 (3).

28. İnternet: ISO Technical Committees. URL: https://www.iso.org/technical-committees.html, Son Erişim Tarihi: 05.06.2021.

29. İnternet: CEN, CEN/CLC/JTC 13 - Cybersecurity and Data Protection, URL: https://standards.cen.eu/, Son Erişim Tarihi: 05.06.2021.

30. İnternet: TSE, TSE.NET Standard Detayı TS EN ISO/IEC 27001:2017. URL: https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073083043047076078043057108043104101, Son Erişim Tarihi: 05.06.2021.

31. İnternet: CEN and CENELEC - CEN-CENELEC. URL: https://www.cencenelec.eu/european-standardization/cen-and-cenelec/, Son Erişim Tarihi: 10.05.2022.

32. İnternet: ISO - About us.URL: https://www.iso.org/about-us.html, Son Erişim Tarihi: 10.05.2022.

33. Susanto, H., Almunawar, M. N., and Tuan, T. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences IJECS-IJENS*, 11 (5), 23-29.

34. İnternet: Standart Satış ve Enformasyon - Standart Satın Al/Abone Ol. URL: https://www.tse.org.tr/IcerikDetay?ID=154&ParentID=7590, Son Erişim: 10.05.2022.

35. İnternet: ISO - Store. URL: https://www.iso.org/store.html, Son Erişim: 10.05.2022.

36. İnternet: CEN - CENELEC - Search standards. URL: https://standards.cencenelec.eu/dyn/www/f?p=CEN:105::RESET, Son Erişim Tarihi: 10.05.2022.

37. İnternet: ISO, ISO Management System Standards. URL: https://www.iso.org/management-system-standards.html, Son Erişim Tarihi: 05.06.2021.

38. Türk Standardları Enstitüsü. (2018). *TS EN ISO/IEC 27001*. Ankara: Türk Standardları Enstitüsü, 1-7.

39. Uluslararası Standartlar Teşkilatı. (2013). *ISO/IEC 27002*. Cenevre: Uluslararası Standartlar Teşkilatı, 2-79.

40. İnternet: ISO - Certification & conformity. URL: https://www.iso.org/conformity-assessment.html, Son Erişim Tarihi: 10.05.2022.

41. İnternet: ISO Certification. URL: https://www.iso.org/certification.html, Son Erişim Tarihi: 06.06.2021.

42. İnternet: IDEALS @ Illinois: Trusted CI Webinar: Cybersecurity Maturity Model Certification (CMMC). URL: https://www.ideals.illinois.edu/handle/2142/108404, Son Erişim Tarihi: 07.05.2022.

43. İnternet: InfraGard San Diego| Defense Industrial Base Sector. URL: https://www.infragardsd.org/sector-defense.shtml, Son Erişim Tarihi: 07.05.2022.

44. İnternet: CISA, Defense Industrial Base Sector. URL: https://www.cisa.gov/defense-industrial-base-sector, Son Erişim Tarihi: 06.06.2021.

45. İnternet: National Archives, About CUI. URL: https://www.archives.gov/cui/about, Son Erişim Tarihi: 06.06.2021.

46. İnternet: Controlled Unclassified Information. URL: https://www.dcsa.mil/mc/isd/cui/, Son Erişim Tarihi: 09.05.2022.

47. İnternet: Definition: Federal contract information from 48 CFR § 52.204-21 | LII / Legal Information Institute. URL: https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=c3c19c60725bd952b69ef7557334313d&term_occur=2&term_src=Title:48:Chapter:1:Subchapter:H:Part:52:Subpart:52.2:52.204-21, Son Erişim Tarihi: 09.05.2022.

48. İnternet: National Archives, FCI and CUI, what is the difference? URL: https://isoo.blogs.archives.gov/2020/06/19/fci-and-cui-what-is-the-difference/, Son Erişim Tarihi: 06.06.2021.

49. İnternet: Shawn Hays, What is FCI? and How to Meet CMMC Level 1? URL: https://info.summit7.us/blog/fci, Son Erişim Tarihi: 06.12.2021.

50. Cook, K. L. (2010, March). The ITAR and you-what you need to know about the International Traffic in Arms Regulations. In *2010 IEEE Aerospace Conference* (1-12). IEEE.

51. İnternet: North Carolina Interagency Cybersecurity Coordinating Committee (I3C), FCI/CUI. URL: https://www.cybernc.us/fci-cui/, Son Erişim Tarihi: 06.12.2021.

52. OUSD(A&S). (2020). *CMMC Appendices v1.02.* Washington: OUSD(A&S), 3-36.

53. İnternet: Wisconsin Procurement Institute Introduction to CMMC Level 1 requirements. URL: https://www.wispro.org/wp-content/uploads/2020/05/Introduction-to-CMMC-Level-1-requirements-May-15-2020-final.pdf, Son Erişim Tarihi: 01.06.2022.

54. BDO, (2021). NEW CMMC MODEL 2.0 IS RELEASED: Major Changes Ahead, Affecting DoD Contractors.

55. İnternet: Cybersecurity Requirements Likely for Defense Contracts by June 2020 > U.S. Department of Defense > Defense Department News. URL: https://www.defense.gov/News/News-Stories/Article/Article/2036713/cybersecurity-requirements-likely-for-defense-contracts-by-june-2020/, Son Erişim Tarihi: 08.05.2022.

56. İnternet: Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program > U.S. Department of Defense > Release. URL: https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/, Son Erişim Tarihi: 08.05.2022.

57. Department of Defense (2020). DFARS Case 2019-D041. *Federal Register*, 29/09/2020, 61505-61522.

58. İnternet: OUSD A&S-Cybersecurity Maturity Model Certification (CMMC). https://www.acq.osd.mil/cmmc/documentation.html, Son Erişim Tarihi: 08.05.2022.

59. Royce, W. (2002). CMM vs. CMMI: From conventional to modern software management. *The Rational Edge*, 1, 2-9.

60. OUSD(A&S). (2021). *Cybersecurity Maturity Model Certification (CMMC) Model Overview*. Washington: OUSD(A&S), 3-5.

61. İnternet: CMMC-AB |. URL: https://cmmcab.org/, Son Erişim Tarihi: 08.05.2022.

62. İnternet: FAQ. URL: https://cmmcab.org/faq/, Son Erişim Tarihi: 08.05.2022.

63. İnternet: H. M. Peters, Defense Acquisitions: DOD's Cybersecurity Maturity Model Certification Framework. URL: https://crsreports.congress.gov, Son Erişim Tarihi: 17.05.2022.

64. İnternet: The basics of CMMC 2.0 and preparation recommendations - Microsoft Tech Community. URL: https://techcommunity.microsoft.com/t5/public-sector-blog/the-basics-of-cmmc-2-0-and-preparation-recommendations/ba-p/3057526, Son Erişim Tarihi: 09.05.2022.

65. Sağıroğlu, Ş., Aktaş, O. ve Alkan, O. (2019) *Siber Güvenlik ve Savunma-Standartlar ve Uygulamalar*. Ankara, 51-85.

66. İnternet: About NIST | NIST. URL: https://www.nist.gov/about-nist, Son Erişim Tarihi: 23.05.2022.

67. İnternet: Questions and Answers | NIST. URL: https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework, Son Erişim Tarihi: 23.05.2022.

68. N. Institute of Standards (2014). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*.

69. İnternet: ETSI - Standards, mission, vision, direct member participation. URL: https://www.etsi.org/about, Son Erişim Tarihi: 23.05.2022.

70. İnternet: About ENISA - The European Union Agency for Cybersecurity — ENISA. URL: https://www.enisa.europa.eu/about-enisa, Son Erişim Tarihi: 24.05.2022.

71. EU. (2013). Regulatıon (Eu) No 526/2013 Of The European Parliament and of the Council. *Official Journal of the European Union*, L 165 (41).

72. İnternet: ISO - About us. URL: https://www.iso.org/about-us.html, Son Erişim Tarihi: 25.05.2022.

73. İnternet: History | IEC. URL: https://iec.ch/history, Son Erişim Tarihi: 25.05.2022.

74. Office of the Government Chief Information Officer (OGCIO). (2022). *An Overview of ISO/IEC 27000 family of Information Security Management System Standards*. Hong Kong: OGCIO, 1-4.

75. İnternet: NATO - Declassified: A short history of NATO. URL: https://www.nato.int/cps/en/natohq/declassified_139339.htm, Son Erişim Tarihi: 24.05.2022.

76. İnternet: NATO Cyber Defence. URL: www.nato.int, Son Erişim Tarihi: 24.05.2022.

77. İnternet: CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/, Son Erişim Tarihi: 24.05.2022.

78. İnternet: IEEE - History of IEEE. URL: https://www.ieee.org/about/ieee-history.html?utm_source=linkslist_text&utm_medium=lp-about&utm_campaign=history, Son Erişim Tarihi: 25.05.2022.

79. İnternet: IEEE SA - About Us. URL: https://standards.ieee.org/about/, Son Erişim Tarihi: 25.05.2022.

80. İnternet: Kurumsal - SASAD - Savunma Sanayii İmalatçılar Derneği. URL: https://www.sasad.org.tr/kurumsal, Son Erişim Tarihi: 22.05.2022.

81. Odabaşı, Y. (1999). Anket yöntemi. *Sosyal Bilimlerde Araştırma Yöntemleri içinde ed. Ali Atf Bir. Eskişehir: TC Anadolu Üniversitesi Yaynlar*, 1081, 81-97.

82. Büyüköztürk, Ş. (2005). Anket geliştirme. *Türk Eğitim Bilimleri Dergisi*, 3 (2), 133-151.

83. Coşar, İ. Y., & Tüfekci, A. CMMC v1. 02 ile ISO IEC 27001 Standardının Karşılaştırılması ve CMMC'ye Geçiş İçin Yapılması Gerekli Temel Faaliyetler. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7 (2), 60-73.

84. Ersoy, E. ve Alkan, M. (2007, 13-14 Aralık). *Bilgi Güvenliğinin Kurumsal Bazda Uygulanması*. Bilgi Güvenliği ve Kriptoloji Konferansında sunuldu, Ankara.

EKLER

EK-1. Uzman görüşü formu

"TÜRK SAVUNMA SANAYİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMALARI İLE CMMC GEREKSİNİMLERİNİN DEĞERLENDİRİLMESİ" KONULU TEZE AİT SAVUNMA SANAYİ KURULUŞLARI İÇİN HAZIRLANAN SORU LİSTESİ[1] DEĞERLENDİRME FORMU

Aşağıda yer alan 1 ila 6. sorular ülkemizin savunma sanayi kuruluşlarının mevcut siber güvenlik uygulamalarının ne olduğuna, 6 ila 9. sorular kuruluşların son bir yılda en çok rastlanan siber saldırı türlerine maruz kalıp kalmadığına, 10 ve 11. sorular ise kuruluşların CMMC hakkındaki farkındalığına ve CMMC'yi uygulamaya yönelik planlarının olup olmadığına dair veri toplamaya yönelik hazırlanmıştır. Bu bakımdan soruların her birinin kapsamını ve geçerliliğini "Uygun" veya "Uygun değil" şeklinde değerlendirebilir ve isteğe bağlı olarak önerilerde bulunabilirsiniz.

1) Kuruluşunuzda ait yazılı bir bilgi güvenliği politikası mevcut mudur? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
2) Kuruluşunuz tarafından düzenli olarak bilgi güvenliği politikalarının uygunluğu denetlenmekte midir? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
3) Kuruluşunuza ait iş süreçlerine özgü en uygun siber güvenlik tedbirlerinin belirlenmesi nasıl yapılmaktadır? *Kurumsal organizasyona bağlı yapılar ile iç değerlendirmeler yapılarak.* *Sektördeki diğer kuruluşlarla ortak değerlendirmeler yapılarak.* *Sektörden bağımsız diğer kuruluşlarla ortak değerlendirmeler yapılarak.* *Sektöre özel yaygın olarak kullanılan yöntemler göz önünde bulundurularak.* *Sektörden bağımsız yaygın olarak kullanılan yöntemler göz önünde bulundurularak.* ** Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*

[1] T.C. Ulaştırma ve Altyapı Bakanlığı Kurumlar İçin Siber Güvenlik Önlemlerini Ölçme Testi Dokümanından faydalanılarak hazırlanmıştır.

EK-1.(devam) Uzman görüşü formu

4) Kuruluşunuzda 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde belirtilenlerden farklı olarak uyguladığınız ilave tedbirler bulunmakta mıdır? *Evet / Hayır * Evet ise isimleri nelerdir?*	*Uygun / Uygun Değil*
5) Kuruluşunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgesi bulunuyor mu? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
6) Kuruluşunuzda bilgi güvenliği alt yapısı oluşturulurken referans alınan ulusal veya uluslararası ölçekte kabul görmüş diğer bir standart ve/veya uygulama modeli / rehber doküman bulunmakta mıdır? Varsa isimleri nelerdir? *Evet / Hayır * Evet ise isimleri nelerdir?*	*Uygun / Uygun Değil*
7) Kuruluşunuza ait web sitesi veya ağlar son bir yıl içinde DDoS veya herhangi bir siber saldırıya maruz kalmış mıdır? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
8) Kuruluşunuza ait bilgisayarlarda ve/veya ağlarda, son bir yıl içinde tespit edilen zararlı yazılım(lar) oldu mu? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*

EK-1.(devam) Uzman görüşü formu

9) Kuruluş ağlarından, son bir yıl içerisinde yetkisiz kullanıcılar tarafından bilgi kaçırılmasına yönelik herhangi bir olay gerçekleşti mi? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
10) Amerika Birleşik Devletleri Savunma Bakanlığının savunma sanayine yönelik bilgi güvenliği alt yapısını güçlendirmek için oluşturduğu CMMC adı verilen bilgi güvenliği yönetimi modeli hakkında bilginiz var mı? *Evet / Hayır * Evet ise;* S1) İsmini duydum. *S2) İsmini duydum ve tanımını biliyorum.* *S3) Tanımıyla birlikte modelin uygulanma gerekçesini ve kapsamını biliyorum.* *S4) S3'e ilave olarak modelin uygulama yöntemi ve seviyeleri hakkında bilgi sahibiyim.* *S5) S4'e ilave olarak modelin ne şekilde uygulanacağını, içerdiği tanımları ve seviyelerine bağlı gereksinimleri hakkında da bilgi sahibiyim.* ** Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
11) Yakın gelecekte ABD Savunma Bakanlığı, tüm tedarikçi ve onların alt tedarikçileri için CMMC kapsamında belgeli olma şartını getirmeyi planlamaktadır. Bu bağlamda kuruluşunuzun ilerleyen herhangi bir tarihte CMMC belgesine sahip olması gerektiğini düşünüyor musunuz? *Evet / Hayır * Uygunsa açıklama yazılabilir.*	*Uygun / Uygun Değil*
Değerlendirenin Adı-Soyadı	

EK-2. Soru listesi formu

"TÜRK SAVUNMA SANAYİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMALARI İLE CMMC GEREKSİNİMLERİNİN DEĞERLENDİRİLMESİ" KONULU TEZE AİT SAVUNMA SANAYİ KURULUŞLARI İÇİN HAZIRLANAN SORU LİSTESİ[1]

Aşağıdaki sorular kuruluşunuzda uygulanan genel bilgi güvenliği tedbirleri, kuruluşunuza ait bilgi teknolojileri alt yapılarının son bir yıl içinde yaygın olarak gerçekleşen siber saldırı türlerine maruz kalıp kalmadığı ve kuruluşunuzdaki CMMC farkındalığı hakkında bilgi almak üzere hazırlanmıştır. Gizlilik ve kurumsal diğer nedenlerden dolayı açıklama kısımlarını doldurmak isteğe bağlıdır. Vereceğiniz cevaplar kurum ve kişi ismi olmaksızın anonim olarak saklanacak ve kullanılacaktır.

1) Kuruluşunuzda ait yazılı bir bilgi güvenliği politikası mevcut mudur?

Evet / Hayır ** Uygunsa açıklama yazılabilir.*

2) Kuruluşunuz tarafından düzenli olarak bilgi güvenliği politikalarının uygunluğu denetlenmekte midir?

Evet / Hayır ** Uygunsa açıklama yazılabilir.*

3) Kuruluşunuza ait iş süreçlerine özgü en uygun siber güvenlik tedbirlerinin belirlenmesi nasıl yapılmaktadır?

Kurumsal organizasyona bağlı yapılar ile iç değerlendirmeler yapılarak.
Sektördeki diğer kuruluşlarla ortak değerlendirmeler yapılarak.
Sektörden bağımsız diğer kuruluşlarla ortak değerlendirmeler yapılarak.
Sektöre özel yaygın olarak kullanılan yöntemler göz önünde bulundurularak.
Sektörden bağımsız yaygın olarak kullanılan yöntemler göz önünde bulundurularak.
** Uygunsa açıklama yazılabilir.*

[1] T.C. Ulaştırma ve Altyapı Bakanlığı Kurumlar İçin Siber Güvenlik Önlemlerini Ölçme Testi Dokümanından faydalanılarak hazırlanmıştır.

EK-2.(devam) Soru listesi formu

4) Kuruluşunuzda 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde belirtilenlerden farklı olarak uyguladığınız ilave tedbirler bulunmakta mıdır?
Evet / Hayır ** Evet ise isimleri nelerdir?*

5) Kuruluşunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgesi bulunuyor mu?
Evet / Hayır ** Uygunsa açıklama yazılabilir.*

6) Kuruluşunuzda bilgi güvenliği alt yapısı oluşturulurken referans alınan ulusal veya uluslararası ölçekte kabul görmüş diğer bir standart ve/veya uygulama modeli / rehber doküman bulunmakta mıdır? Varsa isimleri nelerdir?
Evet / Hayır ** Evet ise isimleri nelerdir?*

7) Kuruluşunuza ait web sitesi veya ağlar son bir yıl içinde DDoS veya herhangi bir siber saldırıya maruz kalmış mıdır?
Evet / Hayır ** Uygunsa açıklama yazılabilir.*

8) Kuruluşunuza ait bilgisayarlarda ve/veya ağlarda, son bir yıl içinde tespit edilen zararlı yazılım(lar) oldu mu?
Evet / Hayır ** Uygunsa açıklama yazılabilir.*

EK-2. **(**devam**)** Soru listesi formu

9) Kuruluş ağlarından, son bir yıl içerisinde yetkisiz kullanıcılar tarafından bilgi kaçırılmasına yönelik herhangi bir olay gerçekleşti mi? *Evet / Hayır* ** Uygunsa açıklama yazılabilir.*
10) Amerika Birleşik Devletleri Savunma Bakanlığının savunma sanayine yönelik bilgi güvenliği alt yapısını güçlendirmek için oluşturduğu CMMC adı verilen bilgi güvenliği yönetimi modeli hakkında bilginiz var mı? *Evet / Hayır* ** Evet ise;* *S1) İsmini duydum.* *S2) İsmini duydum ve tanımını biliyorum.* *S3) Tanımıyla birlikte modelin uygulanma gerekçesini ve kapsamını biliyorum.* *S4) S3'e ilave olarak modelin uygulama yöntemi ve seviyeleri hakkında bilgi sahibiyim.* *S5) S4'e ilave olarak modelin ne şekilde uygulanacağını, içerdiği tanımları ve seviyelerine bağlı gereksinimleri hakkında da bilgi sahibiyim.* ** Uygunsa açıklama yazılabilir.*
11) Yakın gelecekte ABD Savunma Bakanlığı, tüm tedarikçi ve onların alt tedarikçileri için CMMC kapsamında belgeli olma şartını getirmeyi planlamaktadır. Bu bağlamda kuruluşunuzun ilerleyen herhangi bir tarihte CMMC belgesine sahip olması gerektiğini düşünüyor musunuz? *Evet / Hayır* ** Uygunsa açıklama yazılabilir.*

EK-3. Eşleştirme değerlendirme formu

"TÜRK SAVUNMA SANAYİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMALARI İLE CMMC GEREKSİNİMLERİNİN DEĞERLENDİRİLMESİ" KONULU TEZE AİT CMMC v2.0 ve ISO/IEC 27001 GEREKSİNİM KARŞILIKLARINI DEĞERLENDİRME FORMU

Aşağıda yer alan tablonun ilk iki sütununda CMMC v2.0 uygulamalarının ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardında karşılıkları olduğu düşünülen gereksinimler eşleştirilmiştir. Üçüncü sütunda ise yapılan eşleştirmeler ile ilgili olarak uzman görüşlerinin alınmasına yönelik "DEĞERLENDİRME" başlıklı sütuna yer verilmiştir. Eşleştirme yapılırken CMMC v2.0 uygulamalarının ISO/IEC 27001 Standardında ve ISO/IEC 27002 Bilgi Güvenliği Kontrolleri İçin Uygulama Prensiplerinde doğrudan ifade edildiği gereksinimler dikkate alınmıştır. Bu bakımdan eşleştirmelerin her birini "Uygun" veya "Uygun değil" şeklinde değerlendirebilir ve isteğe bağlı olarak önerilerde bulunabilirsiniz.

CMMC v2.0		ISO/IEC 27001		DEĞERLENDİRME
AC-Erişim Kontrolü				
Seviye 1	Seviye 2	Seviye 1 Karşılığı	Seviye 2 Karşılığı	
AC. L1-3.1.1 *Yetkili Erişim Kontrolü* Yetkili kullanıcılara, yetkili kullanıcılar adına hareket eden süreçlere veya cihazlara (diğer bilgi sistemleri dahil) bilgi sistemi erişimini sınırlayın.	**AC.L2-3.1.3** *CUI Akış Kontrolü* Onaylanmış yetkilendirmelere göre CUI akışını kontrol edin.	A.9.2 Kullanıcı erişim yönetimi A.9.2.2 Kullanıcı erişimine izin verme	**YOK**	*Uygun / Uygun Değil* **Öneri/Açıklama yazılabilir.*
AC.L1-3.1.2 *İşlem ve İşlev Kontrolü* Yetkili kullanıcıların yürütmesine izin verilen işlem türleri ve işlevlere bilgi sistemi erişimini sınırlayın.	**AC.L2-3.1.4** *Görevlerinin ayrılması* Örtülü niyetler olmaksızın kötü niyetli faaliyet riskini azaltmak için bireylerin görevlerini ayırın.	A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.1 Bilgiye erişimin kısıtlanması	A.6.1 İç organizasyon A.6.1.2 Görevlerin ayrılığı	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

AC.L1-3.1.20 *Dış Bağlantılar* Harici bilgi sistemlerine bağlantıları ve bunların kullanımını doğrulayın ve kontrol edin/sınırlayın.	**AC.L2-3.1.5** *En Az Ayrıcalık* Belirli güvenlik işlevleri ve ayrıcalıklı hesaplar dahil olmak üzere en az ayrıcalık ilkesini kullanın.	A.13.2 Bilgi transferi A.13.2.1 Bilgi transfer politikaları ve prosedürleri	A.9.2 Kullanıcı erişim yönetimi A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi	*Uygun / Uygun Değil*
AC.L1-3.1.22 *Kamu Bilgilerini Kontrol Et* Kamuya açık bilgi sistemlerinde yayınlanan veya işlenen bilgileri kontrol edin.	**AC.L2.-3.1.6** *Ayrıcalıksız Hesap Kullanımı* Güvenlikle ilgili olmayan işlevlere erişirken ayrıcalıklı olmayan hesapları veya rolleri kullanın.	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması	**YOK**	*Uygun / Uygun Değil*
	AC.L2-3.1.7 *Ayrıcalıklı İşlevler* Ayrıcalıklı olmayan kullanıcıların ayrıcalıklı işlevleri yürütmesini önleyin ve bu tür işlevlerin yürütülmesini denetim günlüklerinde yakalayın.		A.9.2 Kullanıcı erişim yönetimi A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi	*Uygun / Uygun Değil*
	AC.L2-3.1.8 *Başarısız Oturum Açma Denemeleri* Başarısız oturum açma girişimlerini sınırlayın.		**YOK**	*Uygun / Uygun Değil*
	AC.L2-3.1.9 *Gizlilik ve Güvenlik Bildirimleri* Geçerli CUI kurallarıyla tutarlı gizlilik ve güvenlik bildirimleri sağlayın.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	AC.L2-3.1.10 *Oturum Kilidi* Belirli bir süre işlem yapılmadığında verilere erişimi ve verilerin görüntülenmesini önlemek için desen gizleme ekranlarıyla oturum kilidini kullanın.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.2 Güvenli oturum açma prosedürleri	*Uygun / Uygun Değil*
	AC.L2-3.1.11 *Oturum Sonlandırma* Tanımlanmış bir koşuldan sonra bir kullanıcı oturumunu (otomatik olarak) sonlandırın.		**YOK**	*Uygun / Uygun Değil*
	AC.L2-3.1.12 *Uzaktan Erişimi Kontrol Et* Uzaktan erişim oturumlarını izleyin ve kontrol edin.		A.6.2 Mobil cihazlar ve uzaktan çalışma A.6.2.2 Uzaktan çalışma	*Uygun / Uygun Değil*
	AC.L2-3.1.13 *Uzaktan Erişim Gizliliği* Uzaktan erişim oturumlarının gizliliğini korumak için kriptografik mekanizmalar kullanın.		**YOK**	*Uygun / Uygun Değil*
	AC.L2-3.1.14 *Uzaktan Erişim Yönlendirme* Yönetilen erişim kontrol noktaları aracılığıyla uzaktan erişimi yönlendirin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	AC.L2-3.1.15 *Ayrıcalıklı Uzaktan Erişim* Ayrıcalıklı komutların uzaktan yürütülmesine ve güvenlikle ilgili bilgilere uzaktan erişime yetki verin.		**YOK**	*Uygun / Uygun Değil*
	AC.L2-3.1.16 *Kablosuz Erişim Yetkilendirmesi* Bu tür bağlantılara izin vermeden önce kablosuz erişimi yetkilendirin.		A.9.1 Erişim kontrolünün iş gereklilikleri A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1 Ağ güvenliği yönetimi A.13.1.1 Ağ kontrolleri	*Uygun / Uygun Değil*
	AC.L2-3.1.17 *Kablosuz Erişim Koruması* Kimlik doğrulama ve şifreleme kullanarak kablosuz erişimi koruyun.		A.13.1 Ağ güvenliği yönetimi A.13.1.2 Ağ hizmetlerinin güvenliği	*Uygun / Uygun Değil*
	AC.L2-3.1.18 *Mobil Cihaz Bağlantısı* Mobil cihazların bağlantısını kontrol edin.		A.6.2 Mobil cihazlar ve uzaktan çalışma A.6.2.1 Mobil cihaz politikası	*Uygun / Uygun Değil*
	AC.L2-3.1.19 *Mobil Cihazda CUI'yi Şifreleyin* CUI'yi mobil cihazlarda ve mobil bilgi işlem platformlarında şifreleyin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	AC.L2-3.1.21 *Taşınabilir Depolama Kullanımı* Harici sistemlerde taşınabilir depolama cihazlarının kullanımını sınırlayın.		A.8.3 Ortam işleme A.8.3.1 Taşınabilir ortam yönetimi	*Uygun / Uygun Değil*
	AT.L2-3.2.1 *Rol Bazlı Risk Farkındalığı* Yöneticilerin, sistem yöneticilerinin ve kurumsal sistemlerin kullanıcılarının, faaliyetleriyle ilişkili güvenlik risklerinden ve bu sistemlerin güvenliğiyle ilgili geçerli politikalar, standartlar ve prosedürlerden haberdar olmalarını sağlayın.		A.7.2 Çalışma esnasında A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi	*Uygun / Uygun Değil*
	AT.L2-3.2.2 *Rol Bazlı Eğitim* Personelin, kendilerine atanan bilgi güvenliği ile ilgili görev ve sorumluluklarını yerine getirmek için eğitildiğinden emin olun.		A.7.2 Çalışma esnasında A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	AT.L2-3.2.3 *İçeriden Tehdit Farkındalığı* İçeriden gelen tehdidin potansiyel göstergelerini tanıma ve raporlama konusunda güvenlik bilinci eğitimi sağlayın.		A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.3 Bilgi güvenliği açıklıklarının raporlanması	*Uygun / Uygun Değil*
	AU.L2-3.3.1 *Sistem Denetimi* Yasa dışı veya yetkisiz sistem etkinliğinin izlenmesini, analizini, araştırılmasını ve raporlanmasını sağlamak için gereken ölçüde sistem denetim günlüklerini ve kayıtlarını oluşturun ve saklayın.		A.12.4 Kaydetme ve izleme A.12.4.1 Olay kaydetme	*Uygun / Uygun Değil*
	AU.L2-3.3.2 *Kullanıcı Sorumluluğu* Bireysel sistem kullanıcılarının eylemlerinin bu kullanıcılara benzersiz bir şekilde izlenebildiğinden emin olun, böylece eylemlerinden sorumlu tutulabilirler.		A.12.4 Kaydetme ve izleme A.12.4.3 Yönetici ve operatör kayıtları	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	AU.L2-3.3.3 *Etkinlik İncelemesi* Günlüğe kaydedilen olayları gözden geçirin ve güncelleyin.		A.12.4 Kaydetme ve izleme A.12.4.1 Olay kaydetme	*Uygun / Uygun Değil*
	AU.L2-3.3.4 *Denetim Hatası Uyarısı* Denetim günlüğü işlemi hatası durumunda uyar.		**YOK**	*Uygun / Uygun Değil*
	AU.L2-3.3.5 *Denetim Korelasyonu* Soruşturma ve yasa dışı, yetkisiz, şüpheli veya olağandışı faaliyet belirtilerine yanıt için denetim kaydı incelemesi, analizi ve raporlama süreçleri arasında ilişki kurun.		**YOK**	*Uygun / Uygun Değil*
	AU.L2-3.3.6 *Azaltma ve Raporlama* İsteğe bağlı analiz ve raporlamayı desteklemek için denetim kayıtlarını azaltma ve rapor oluşturmayı sağlayın.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	AU.L2-3.3.7 *Yetkili Zaman Kaynağı* Denetim kayıtları için zaman damgaları oluşturmak üzere dahili sistem saatlerini yetkili bir kaynakla karşılaştıran ve senkronize eden bir sistem yeteneği sağlayın.		A.12.4 Kaydetme ve izleme A.12.4.4 Saat senkronizasyonu	*Uygun / Uygun Değil*
	AU.L2-3.3.8 *Denetim Koruması* Denetim bilgilerini ve denetim günlüğü araçlarını yetkisiz erişime, değiştirmeye ve silmeye karşı koruyun.		A.12.4 Kaydetme ve izleme A.12.4.2 Kayıt bilgisinin korunması	*Uygun / Uygun Değil*
	AU.L2-3.3.9 *Denetim Yönetimi* Denetim günlüğü işlevselliğinin yönetimini ayrıcalıklı kullanıcıların bir alt kümesiyle sınırlayın.		**YOK**	*Uygun / Uygun Değil*
	CM.L2-3.4.1 *Sistem Temeli Belirleme* İlgili sistem geliştirme yaşam döngüleri boyunca kurumsal sistemlerin (donanım, yazılım, bellenim ve belgeler dahil) temel yapılandırmalarını ve envanterlerini oluşturun ve sürdürün.		A.8.1 Varlıkların sorumluluğu A.8.1.1 Varlıkların envanteri	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	CM.L2-3.4.2 *Güvenlik Yapılandırma Uygulaması* Kurumsal sistemlerde kullanılan bilgi teknolojisi ürünleri için güvenlik yapılandırma ayarlarını oluşturun ve uygulayın.		A.12.1 İşletim prosedürleri ve sorumlulukları A.12.1.1 Yazılı işletim prosedürleri	*Uygun / Uygun Değil*
	CM.L2-3.4.3 *Sistem Değişiklik Yönetimi* Organizasyonel sistemlerde yapılan değişiklikleri takip edin, gözden geçirin, onaylayın veya onaylamayın ve günlüğe kaydedin.		A.12.1 İşletim prosedürleri ve sorumlulukları A.12.1.2 Değişiklik yönetimi	*Uygun / Uygun Değil*
	CM.L2-3.4.4 *Güvenlik Etki Analizi* Uygulamadan önce değişikliklerin güvenlik etkisini analiz edin.		A.12.1 İşletim prosedürleri ve sorumlulukları A.12.1.2 Değişiklik yönetimi	*Uygun / Uygun Değil*
	CM.L2-3.4.5 *Değişiklik için Erişim Kısıtlamaları* Kurumsal sistemlerdeki değişikliklerle ilişkili fiziksel ve mantıksal erişim kısıtlamalarını tanımlayın, belgeleyin, onaylayın ve uygulayın.		A.14.2 Geliştirme ve destek süreçlerinde güvenlik A.14.2.2 Sistem değişiklik kontrolü prosedürleri	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	CM.L2-3.4.6 *En Az İşlevsellik* Yalnızca temel yetenekleri sağlamak için organizasyonel sistemleri yapılandırarak en az işlevsellik ilkesini kullanın.		**YOK**	*Uygun / Uygun Değil*
	CM.L2-3.4.7 *Gereksiz İşlevsellik* Gerekli olmayan programların, işlevlerin, bağlantı noktalarının, protokollerin ve hizmetlerin kullanımını kısıtlayın, devre dışı bırakın veya önleyin.		**YOK**	*Uygun / Uygun Değil*
	CM.L2-3.4.8 *Uygulama Yürütme Politikası* Yetkisiz yazılımların kullanımını önlemek için özel durumla reddet (kara listeye alma) ilkesini veya yetkili yazılımın yürütülmesine izin vermek için tümünü reddet, özel durumla izin ver (beyaz listeye alma) ilkesini uygulayın.		A.12.2 Kötücül yazılımlardan koruma A.12.2.1 Kötücül yazılımlara karşı kontroller	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	CM.L2-3.4.9 *Kullanıcı Tarafından Yüklenen Yazılım* Kullanıcı tarafından yüklenen yazılımı kontrol edin ve izleyin.		A.12.6 Teknik açıklık yönetimi A.12.6.2 Yazılım kurulumu kısıtlamaları	*Uygun / Uygun Değil*
IA.L1-3.5.1 *Tanılama* Bilgi sistemi kullanıcılarını, kullanıcılar adına hareket eden süreçleri veya cihazları tanımlayın.	IA.L2-3.5.3 *Çok Faktörlü Kimlik Doğrulama* Ayrıcalıklı hesaplara yerel ve ağ erişimi için ve ayrıcalığı olmayan hesaplara ağ erişimi için çok faktörlü kimlik doğrulamayı kullanın.	A.9.2 Kullanıcı erişim yönetimi A.9.2.1 *Kullanıcı kaydetme ve kayıt silme*	**YOK**	*Uygun / Uygun Değil*
IA.L1-3.5.2 *Kimlik doğrulama* Kurumsal bilgi sistemlerine erişime izin vermek için bir ön koşul olarak bu kullanıcıların, süreçlerin veya cihazların kimliklerini doğrulayın.	IA.L2-3.5.4 *Tekrara Dayanıklı Kimlik Doğrulama* Ayrıcalıklı ve ayrıcalıklı olmayan hesaplara ağ erişimi için tekrara dayanıklı kimlik doğrulama mekanizmalarını kullanın.	A.9.2 Kullanıcı erişim yönetimi A.9.2.2 Kullanıcı erişimine izin verme	A.9.3 Kullanıcı sorumlulukları A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı	*Uygun / Uygun Değil*
	IA.L2-3.5.5 *Tanımlayıcı Yeniden Kullanımı* Tanımlayıcıların belirli bir süre boyunca yeniden kullanılmasını önleyin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	IA.L2-3.5.6 *Tanımlayıcı İşleme* Belirli bir hareketsizlik süresinden sonra tanımlayıcıları devre dışı bırakın.		**YOK**	*Uygun / Uygun Değil*
	IA.L2-3.5.7 *Şifre Karmaşıklığı* Yeni parolalar oluşturulduğunda minimum parola karmaşıklığı ve karakter değişikliği uygulayın.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.3 Parola yönetim sistemi	*Uygun / Uygun Değil*
	IA.L2-3.5.8 *Şifre Yeniden Kullanımı* Belirli sayıda dönem için parolanın yeniden kullanılmasını yasaklayın.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.3 Parola yönetim sistemi	*Uygun / Uygun Değil*
	IA.L2-3.5.9 *Geçici Şifreler* Kalıcı bir parolayla anında değişiklik yaparak sistem oturumları için geçici parola kullanımına izin verin.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.3 Parola yönetim sistemi	*Uygun / Uygun Değil*
	IA.L2-3.5.10 *Kriptografik Olarak Korunan Şifreler* Yalnızca kriptografik olarak korunan parolaları saklayın ve iletin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	IA.L2-3.5.11 *Belirsiz Geri Bildirim* Kimlik doğrulama bilgileri ile ilgili belirsiz geri bildirim yap.		A.9.4 Sistem ve uygulama erişim kontrolü A.9.4.2 Güvenli oturum açma prosedürleri	*Uygun / Uygun Değil*
	IR.L2-3.6.1 *Olay Yönetimi* Hazırlık, tespit, analiz, muhafaza, kurtarma ve kullanıcı müdahale faaliyetlerini içeren kurumsal sistemler için operasyonel bir olay işleme yeteneği oluşturun.		A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.1 Sorumluluklar ve prosedürler	*Uygun / Uygun Değil*
	IR.L2-3.6.2 *Olay Raporlama* Olayları takip edin, belgeleyin ve kuruluş içindeki ve dışındaki belirlenmiş görevlilere ve/veya yetkililere bildirin.		A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.2 Bilgi güvenliği olaylarının raporlanması	*Uygun / Uygun Değil*
	IR.L2-3.6.3 *Olay Müdahale Testi* Kurumsal olay yanıt yeteneğini test edin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	MA.L2-3.7.1 *Bakım Yap* Organizasyonel sistemlerde bakım gerçekleştirin.		A.11.2 Teçhizat A.11.2.4 Teçhizat bakımı	*Uygun / Uygun Değil*
	MA.L2-3.7.2 *Sistem Bakım Kontrolü* Sistem bakımını yürütmek için kullanılan araçlar, teknikler, mekanizmalar ve personel üzerinde kontroller sağlayın.		A.11.2 Teçhizat A.11.2.4 Teçhizat bakımı	*Uygun / Uygun Değil*
	MA.L2-3.7.3 *Ekipman Sanitasyonu* Tesis dışı bakım için kaldırılan ekipmanın herhangi bir CUI'den arındırıldığından emin olun.		A.11.2 Teçhizat A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği	*Uygun / Uygun Değil*
	MA.L2-3.7.4 *Medya Denetimi* Medya kurumsal sistemlerde kullanılmadan önce, tanılama ve test programlarını içeren medyayı kötü amaçlı kod açısından kontrol edin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	MA.L2-3.7.5 Yerel Olmayan Bakım Harici ağ bağlantıları aracılığıyla yerel olmayan bakım oturumları oluşturmak ve yerel olmayan bakım tamamlandığında bu tür bağlantıları sonlandırmak için çok faktörlü kimlik doğrulaması gerektir.		**YOK**	*Uygun / Uygun Değil*
	MA.L2-3.7.6 *Bakım Personeli* Gerekli erişim yetkisi olmayan bakım personelinin bakım faaliyetlerini denetleyin.		A.11.2 Teçhizat A.11.2.4 Teçhizat bakımı	*Uygun / Uygun Değil*
MP.L1-3.8.3 *Medya İmhası* Federal Sözleşme Bilgilerini (FCI) içeren bilgi sistemi ortamını atmadan veya yeniden kullanım için serbest bırakmadan önce sanitize veya imha edin.	MP.L2-3.8.1 *Medya Koruması* Hem kâğıt hem de dijital olarak CUI içeren sistem ortamını koruyun (örn. fiziksel olarak kontrol edin ve güvenli bir şekilde saklayın).	A.11.2 Teçhizat A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı	A.8.3 Ortam işleme 8.3.1 Taşınabilir ortam yönetimi	*Uygun / Uygun Değil*
	MP.L2-3.8.2 *Medya Erişimi* Sistem ortamındaki CUI'ye erişimi yetkili kullanıcılarla sınırlayın.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	MP.L2-3.8.4 *Medya İşaretleri* Medyayı gerekli CUI işaretleri ve dağıtım sınırlamaları ile işaretleyin.		A.8.2 Bilgi sınıflandırma A.8.2.2 Bilgi etiketlemesi	*Uygun / Uygun Değil*
	MP.L2-3.8.5 *Medya Sorumluluğu* CUI içeren medyaya erişimi kontrol edin ve kontrollü alanların dışına taşıma sırasında medya için hesap verebilirliği sağlayın.		**YOK**	*Uygun / Uygun Değil*
	MP.L2-3.8.6 *Taşınabilir Depolama Şifrelemesi* Alternatif fiziksel güvenlik önlemleriyle korunmadığı sürece, taşıma sırasında dijital ortamda depolanan CUI'nin gizliliğini korumak için kriptografik mekanizmalar uygulayın.		A.8.3 Ortam işleme A.8.3.3 Fiziksel ortam aktarımı	*Uygun / Uygun Değil*
	MP.L2-3.8.7 *Çıkarılabilir Medya* Sistem bileşenlerinde çıkarılabilir medya kullanımını kontrol edin.		A.8.3 Ortam işleme A.8.3.1 Taşınabilir ortam yönetimi	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	MP.L2-3.8.8 *Paylaşılan Medya* Bu tür cihazların tanımlanabilir bir sahibi olmadığında taşınabilir depolama cihazlarının kullanımını yasaklayın.		**YOK**	*Uygun / Uygun Değil*
	MP.L2-3.8.9 *Yedeklemeleri Koruyun* Depolama konumlarında yedek CUI'nin gizliliğini koruyun.		A.12.3 Yedekleme A.12.3.1 Bilgi yedekleme	*Uygun / Uygun Değil*
	PS.L2-3.9.1 *Bireyleri Tarayın* CUI içeren kurumsal sistemlere erişim yetkisi vermeden önce bireyleri tarayın.		A.7.1 İstihdam öncesi A.7.1.1 Tarama	*Uygun / Uygun Değil*
	PS.L2-3.9.2 *Personel İşlemleri* Sonlandırma ve transferler gibi personel eylemleri sırasında ve sonrasında CUI içeren kurumsal sistemlerin korunmasını sağlayın.		A.7.3 İstihdamın sonlandırılması ve değiştirilmesi A.7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

PE.L1-3.10.1 *Fiziksel Erişimi Sınırla* Kurumsal bilgi sistemlerine, ekipmana ve ilgili işletim ortamlarına fiziksel erişimi yetkili kişilerle sınırlandırın.	PE.L2-3.10.2 *Tesisi İzle* Fiziksel tesisi koruyun ve izleyin ve organizasyonel sistemler için altyapıyı destekleyin.	A.11.1 Güvenli alanlar A.11.1.1 Fiziksel güvenlik sınırı	A.11.1 Güvenli alanlar A.11.1.1 Fiziksel güvenlik sınırı	*Uygun / Uygun Değil*
PE.L1-3.10.3 *Ziyaretçilere Eşlik Et* Ziyaretçilere eşlik edin ve ziyaretçi etkinliğini izleyin.	PE.L2-3.10.6 *Alternatif Çalışma Sahaları* Alternatif çalışma sahalarında CUI için koruma önlemleri uygulayın.	A.11.1 Güvenli alanlar A.11.1.2 Fiziksel giriş kontrolleri	**YOK**	*Uygun / Uygun Değil*
PE.L1-3.10.4 *Fiziksel Erişim Günlükleri* Fiziksel erişimin denetim günlüklerini koruyun.		A.11.1 Güvenli alanlar A.11.1.2 Fiziksel giriş kontrolleri		*Uygun / Uygun Değil*
PE.L1-3.10.5 *Fiziksel Erişimi Yönet* Fiziksel erişim cihazlarını kontrol edin ve yönetin.		A.11.2 Teçhizat A.11.2.1 Teçhizat yerleştirme ve koruma		*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	RA.L2-3.11.1 *Risk Değerlendirmesi* Kurumsal sistemlerin işleyişinden ve ilgili işleme, depolama veya CUI iletiminden kaynaklanan kurumsal operasyonlara (misyon, işlevler, imaj veya itibar dahil), kurumsal varlıklara ve bireylere yönelik riski periyodik olarak değerlendirin.		6 Planlama 6.1 Risk ve fırsatları ele alan faaliyetler 8 İşletim 8.1 İşletimsel planlama ve kontrol	*Uygun / Uygun Değil*
	RA.L2-3.11.2 *Güvenlik Açığı Taraması* Düzenli aralıklarla ve bu sistemleri ve uygulamaları etkileyen yeni güvenlik açıkları belirlendiğinde, kurumsal sistemlerdeki ve uygulamalardaki güvenlik açıklarını tarayın.		A.12.6 Teknik açıklık yönetimi A.12.6.1 Teknik açıklıkların yönetimi	*Uygun / Uygun Değil*
	RA.L2-3.11.3 *Güvenlik Açığı Giderme* Güvenlik açıklarını risk değerlendirmelerine göre giderin.		A.12.6 Teknik açıklık yönetimi A.12.6.1 Teknik açıklıkların yönetimi	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	CA.L2-3.12.1 *Güvenlik Kontrol Değerlendirmesi* Kontrollerin uygulamalarında etkili olup olmadığını belirlemek için kurumsal sistemlerdeki güvenlik kontrollerini periyodik olarak değerlendirin.		9 Performans değerlendirme 9.1 İzleme, ölçme, analiz ve değerlendirme A.18.2 Bilgi güvenliği gözden geçirmeleri A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirmesi	*Uygun / Uygun Değil*
	CA.L2-3.12.2 *Eylem Planı* Kurumsal sistemlerdeki eksiklikleri gidermek ve güvenlik açıklarını azaltmak veya ortadan kaldırmak için tasarlanmış eylem planları geliştirin ve uygulayın.		6 Planlama 6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama	*Uygun / Uygun Değil*
	CA.L2-3.12.3 *Güvenlik Kontrol İzleme* Kontrollerin etkinliğinin devam etmesini sağlamak için güvenlik kontrollerini sürekli olarak izleyin.		8 İşletim 8.1 İşletimsel planlama ve kontrol	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	CA.L2-3.12.4 *Sistem Güvenlik Planı* Sistem sınırlarını, sistem çalışma ortamlarını, güvenlik gereksinimlerinin nasıl uygulandığını ve diğer sistemlerle ilişkileri veya diğer sistemlerle olan bağlantıları açıklayan sistem güvenlik planlarını geliştirin, belgeleyin ve periyodik olarak güncelleyin.		8 İşletim 8.1 İşletimsel planlama ve kontrol	*Uygun / Uygun Değil*
SC.L1-3.13.1 Sınır Koruması Bilgi sistemlerinin dış sınırlarında ve temel iç sınırlarında kurumsal iletişimleri (örn. kurumsal bilgi sistemleri tarafından iletilen veya alınan bilgiler) izleyin, kontrol edin ve koruyun.	SC.L2-3.13.2 *Güvenlik Mühendisliği* Kurumsal sistemlerde etkin bilgi güvenliğini destekleyen mimari tasarımları, yazılım geliştirme tekniklerini ve sistem mühendisliği ilkelerini kullanın.	A.13.1 Ağ güvenliği yönetimi A.13.1.1 Ağ kontrolleri	A.14.2 Geliştirme ve destek süreçlerinde güvenlik A.14.2.5 Güvenli sistem mühendisliği prensipleri	*Uygun / Uygun Değil*
SC.L1-3.13.5 *Genel Erişim Sistemi Ayrımı* Dahili ağlardan fiziksel veya mantıksal olarak ayrılmış, genel olarak erişilebilir sistem bileşenleri için alt ağlar uygulayın.	SC.L2-3.13.3 *Rol Ayrımı* Kullanıcı işlevselliğini sistem yönetimi işlevselliğinden ayırın.	A.13.1 Ağ güvenliği yönetimi A.13.1.3 Ağlarda ayrım	A.6.1 İç organizasyon A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	SC.L2-3.13.4 *Paylaşılan Kaynak Kontrolü* Paylaşılan sistem kaynakları aracılığıyla yetkisiz ve istenmeyen bilgi aktarımını önleyin.		**YOK**	*Uygun / Uygun Değil*
	SC.L2-3.13.6 *İstisnaya Göre Ağ İletişimi* Varsayılan olarak ağ iletişim trafiğini reddet ve ağ iletişim trafiğine istisnaya göre izin ver (örn. hepsini reddet, istisnaya göre izin ver).		A.13.1 Ağ güvenliği yönetimi A.13.1.2 Ağ hizmetlerinin güvenliği	*Uygun / Uygun Değil*
	SC.L2-3.13.7 *Bölünmüş Tünelleme* Uzak cihazların aynı anda kurumsal sistemlerle uzaktan olmayan bağlantılar kurmasını ve harici ağlardaki kaynaklara başka bir bağlantı aracılığıyla iletişim kurmasını (örn. bölünmüş tünelleme) önleyin.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	SC.L2-3.13.8 *Aktarılan Veriler* Alternatif fiziksel güvenlik önlemleriyle korunmadığı sürece, iletim sırasında CUI'nin yetkisiz ifşasını önlemek için kriptografik mekanizmalar uygulayın.		A.13.2 Bilgi transferi A.13.2.1 Bilgi transfer politikaları ve prosedürleri	*Uygun / Uygun Değil*
	SC.L2-3.13.9 *Bağlantı Sonlandırma* Oturumların sonunda veya belirli bir etkinlik dışı kalma süresinden sonra iletişim oturumlarıyla ilişkili ağ bağlantılarını sonlandırın.		A.11.2 Teçhizat A.11.2.8 Gözetimsiz kullanıcı teçhizatı	*Uygun / Uygun Değil*
	SC.L2-3.13.10 *Anahtar Yönetimi* Kurumsal sistemlerde kullanılan kriptografi için kriptografik anahtarlar oluşturun ve yönetin.		A.10.1 Kriptografik kontroller A.10.1.2 Anahtar yönetimi	*Uygun / Uygun Değil*
	SC.L2-3.13.11 *CUI Şifrelemesi* CUI'nin gizliliğini korumak için kullanıldığında FIPS onaylı şifreleme kullanın.		**YOK**	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

	SC.L2-3.13.12 *Ortak Cihaz Kontrolü* Ortak bilgi işlem cihazlarının uzaktan etkinleştirilmesini yasaklayın ve cihazda bulunan kullanıcılara kullanımda olan cihazların göstergesini sağlayın.		**YOK**	*Uygun / Uygun Değil*
	SC.L2-3.13.13 *Mobil Kod* Mobil kodun kullanımını kontrol edin ve izleyin.		**YOK**	*Uygun / Uygun Değil*
	SC.L2-3.13.14 *İnternet Protokolü Üzerinden Ses* İnternet Üzerinden Ses Protokolü (VoIP) teknolojilerinin kullanımını kontrol edin ve izleyin.		A.13.2 Bilgi transferi A.13.2.1 Bilgi transfer politikaları ve prosedürleri	*Uygun / Uygun Değil*
	SC.L2-3.13.15 *İletişim Güvenilirliği* İletişim oturumlarının güvenilirliğini koruyun.		A.13.1 Ağ güvenliği yönetimi A.13.1.1 Ağ kontrolleri	*Uygun / Uygun Değil*
	SC.L2-3.13.16 *Duran Veriler* Bekleyen CUI'nin gizliliğini koruyun.		A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum A.18.1.3 Kayıtların korunması	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

SI.L1-3.14.1 *Kusur Giderme* Bilgi ve bilgi sistemi kusurlarını zamanında tespit edin, raporlayın ve düzeltin.	SI.L2-3.14.3 *Güvenlik Uyarıları ve Önerileri* Sistem güvenlik uyarılarını ve önerilerini izleyin ve karşılık vermek üzere harekete geçin.	A.12.6 Teknik açıklık yönetimi A.12.6.1 Teknik açıklıkların yönetimi	A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.1 Sorumluluklar ve prosedürler	*Uygun / Uygun Değil*
SI.L1-3.14.2 *Kötü Amaçlı Kod Koruması* Kurumsal bilgi sistemleri içinde uygun yerlerde kötü amaçlı kodlara karşı koruma sağlayın.	SI.L2-3.14.6 *Saldırılar için İletişimi İzleyin* Saldırıları ve olası saldırıların göstergelerini tespit etmek için gelen ve giden iletişim trafiği dahil olmak üzere kurumsal sistemleri izleyin.	**YOK**	A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi A.16.1.1 Sorumluluklar ve prosedürler	*Uygun / Uygun Değil*
SI.L1-3.14.4 *Kötü Amaçlı Kod Korumasını Güncelle* Yeni sürümler çıktığında kötü amaçlı kod koruma mekanizmalarını güncelleyin.	SI.L2-3.14.7 *Yetkisiz Kullanımı Tanımlayın* Organizasyonel sistemlerin yetkisiz kullanımını tanımlayın.	**YOK**	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.1.1 Erişim kontrol politikası	*Uygun / Uygun Değil*

EK-3.(devam) Eşleştirme değerlendirme formu

SI.L1-3.14.5 *Sistem ve Dosya Tarama* Dosyalar indirilirken, açılırken veya yürütülürken, bilgi sisteminin periyodik taramalarını ve harici kaynaklardan gelen dosyaların gerçek zamanlı taramalarını gerçekleştirin.		A.12.2 Kötücül yazılımlardan koruma A.12.2.1 Kötücül yazılımlara karşı kontroller		*Uygun / Uygun Değil*

Değerlendirenin Adı-Soyadı	:

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	:	COŞAR, İsmail Yiğit
Uyruğu	:	T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Yılı
Yüksek Lisans	Gazi Üniversitesi/Bilişim Enstitüsü Yönetim Bilişim Sistemleri Anabilim Dalı	Devam Ediyor
Yüksek Lisans	Hacettepe Üniversitesi/Sosyal Bilimler Enstitüsü Maliye Anabilim Dalı	2012
Lisans	Gazi Üniversitesi/Mühendislik Mimarlık Fakültesi Makine Mühendisliği Bölümü	2006
Lise	Gazi Anadolu Lisesi	2001

İş Deneyimi

Yıl	Kuruluş	Görev
2022-Halen	ASELSAN	Mühendis
2006-2022	Türk Standardları Enstitüsü	Mühendis
2006-2006	İstanbul Ulaşım A.Ş.	Mühendis

Yabancı Dili

İngilizce

Yayınlar

1. Coşar, İ. Y., & Tüfekci, A. CMMC v1. 02 ile ISO IEC 27001 Standardının Karşılaştırılması ve CMMC'ye Geçiş İçin Yapılması Gerekli Temel Faaliyetler. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *7*(2), 60-73.

Hobiler

Bilişim teknolojileri ve otomobiller.



GAZİLİ OLMAK AYRICALIKTIR…