CMMC v1.02 ile ISO IEC 27001 Standardının Karşılaştırılması ve CMMC'ye Geçiş İçin Yapılması Gerekli Temel Faaliyetler

İsmail Yiğit Coşar *[1, 2] ,Aslıhan Tüfekci[3]

[1] Gazi Üniversitesi Bilişim Enstitüsü, Ankara, Türkiye
[2] TSE Eğitim Dairesi Başkanlığı Program Geliştirme Müdürlüğü, Ankara, Türkiye
[3] Gazi Üniversitesi Bilişim Enstitüsü, Ankara, Türkiye
yigitcsr@gmail.com, asli@gazi.edu.tr

ÖZET

Gelişen teknoloji ile birlikte bilgi güvenliğinin önemi hem bireysel hem de kurumsal ölçekte her geçen gün artmaktadır. Özellikle bilgi güvenliği yönetimine sistemsel bakış açısının kazandırılması açısından ISO/IEC 27001 standardının önemi oldukça fazladır. Ancak zamanla gelişen teknoloji artan veri miktarını ve çeşitliliğini de beraberinde getirmiş, bilgi güvenliğine yönelik tehditler çoğalmış ve bunlara bağlı olarak bazı sektörler için sektöre özel farklı bilgi güvenliği yönetimi modelleri ortaya çıkmıştır. Bunlardan biri de ABD Savunma Bakanlığı tarafından savunma sanayi sektörüne özel olarak geliştirilen ve İngilizce adıyla "Cybersecurity Maturity Model Certification-CMMC" olarak belirtilen süreçte yer alan siber güvenlik olgunluk modelidir. Bu çalışmada ülkemiz savunma sanayinde bilgi güvenliği farkındalığının arttırılması amacıyla söz konusu uygulamalar hakkında temel bilgiler verilmiş, bakış açısının geliştirilmesine katkı sağlayan CMMC v1.02 ile ISO/IEC 27001'e kapsam, gereksinim ve sertifikasyon süreçleri bakımından karşılaştırılmış, yeni bakış açısının dikkate alınması için önerilerde bulunulmuş ve gerçekleştirilmesi gerekli temel faaliyetler açıklanmıştır. Sonuç olarak, elde edilen bilgiler ve bulgular çerçevesinde bilgi güvenliği uygulamalarının gelecekte ne yönde ilerleyeceği ve yapılması gerekenler konusunda değerlendirmeler sunulmuştur.

Anahtar Kelimeler- Siber Güvenlik, Siber Saldırı, Siber Savaş, Bilgi Güvenliği, CMMC.

Comparison of CMMC v1.02 and ISO IEC 27001 Standard and Basic Activities to be Performed for Transition to CMMC

ABSTRACT

With the developing technology, the importance of information security on both an individual and corporate scale is increasing day by day. Especially in terms of bringing a systemic perspective to information security management the importance of ISO/IEC 27001 standard is quite high. However, over time, the developing technology has brought the increasing amount and diversity of data, the threats to information security have increased and according so, different sector-specific information security management models have emerged for some sectors. One of them is the cyber security maturity model, which is developed by the US Department of Defense specifically for the defense industry sector and is included in the process specified as "Cybersecurity Maturity Model Certification-CMMC". In this study, basic information about the applications in question was given in order to increase the awareness of information security in our country's defense industry. CMMC v1.02, which contributes to the development of the perspective, and ISO/IEC 27001 were compared in terms of scope, requirements and certification processes and suggestions were made to take the new perspective into account and the main activities to be carried out were explained. As a result, within the framework of the information and findings obtained, evaluations were presented on how information security practices will progress in the future and what needs to be done.

Keywords- Cyber Security, Cyber Attack, Cyberwarfare, Information Security, CMMC.

I. GİRİŞ (INTRODUCTION)

Gelişen teknoloji ile birlikte hayatımızın her alanında etkisini gösteren "dijitalleşme", bilgi varlıklarının çeşidini ve büyüklüğünü arttırırken kişilerin ve kurumların bilgi güvenliği konusunda tedbir almalarını da zorunlu hale getirmiştir.

Son 50 yılda özellikle teknoloji alanında yaşanan büyük gelişmelerle birlikte artık gerçek dünyanın kontrolü önemli ölçüde siber dünyaya aktarılmış böylece her alanda öne çıkan "bilgi" kavramı günümüzde neredeyse "güç" kavramıyla eş anlamda kullanılmaya başlanmıştır [1]. Buradan da anlaşılacağı üzere güvenliğin sağlanması için gerekli olan gücün temelinde artık bilgi yer almaktadır ve bilgi varlıklarının korunmasında yaşanabilecek

herhangi bir zafiyet varlıkların sürdürülebilirliği için önemli bir tehdit oluşturacaktır. Bu bakımdan günümüzde özellikle bilgi ve bilgi işlem güvenliğine önem vermemenin bizlere, işlerimize ve ülkemize maliyeti düşünülenden oldukça fazladır [2].

Örneğin 2018 yılında Amerika Birleşik Devletleri'nde yapılan bir çalışmaya göre zararlı siber aktivitelerin 2016 yılında yalnızca ABD ekonomisine zararının 57 ila 109 milyar dolar arasında olduğu belirtilmektedir [3]. Dünyaya bakıldığında ise bu miktarın 2016 yılında dünya ülkelerinin toplam gayrisafi yurtiçi hasılasının %1 'ine yani 600 milyar dolar seviyelerine kadar çıktığı görülmektedir [4].

Bu bakımdan oldukça yüksek zarar verme potansiyeline sahip olan siber saldırıların gerekçeleri çok çeşitli olmakla birlikte bu tip saldırıların boyutları kişisel, kurumsal veya ulusal ölçekte olabilmektedir. Hatta birçok durumda arkalarında gelişmiş ülkelerin bulunduğu uluslararası saldırılarla da karşılaşılabilmektedir. Buradan hareketle geçmişin ülkelerarası soğuk savaşlarının günümüzde siber ortamda cereyan ettiği de söylenebilir [5].

Bilgi güvenliği alt yapılarını korumak için gelişmiş ülkeler siber ortamda risklerin azaltılması ve güvenliğin sağlanmasına yönelik çalışmalarını özellikle bilgi güvenliği alanında standart hazırlanması faaliyetleri ile başlatarak 90'lı yıllardan itibaren devam ettirmektedir. Bu alanda ilk olarak 1995 yılında İngiltere'de BSI (British Standards Institution) BS 7799-1:1995 numaralı bilgi güvenliği yönetimi standardını yayınlayarak günümüzde yaygın olarak kullanılan bilgi güvenliği yönetim sistemi standardı olan ISO/IEC 27001'in temellerini atmıştır [6]. O zamandan günümüze bilgi güvenliği alanında uluslararası birçok kuruluş (AQAP, IEEE, ETSI, ITU, NIST, ISACA vd.) çok sayıda standart veya uygulama modeli yayınlayarak kişi ve kurumların hizmetine sunmuştur [7].

Günümüze gelindiğinde ise benzer şekilde ABD Savunma Bakanlığı'nın da tedarikçilerinin bilgi güvenliği altyapılarını güçlendirmek için İngilizce adıyla "Cybersecurity Maturity Model Certification-CMMC v1.02" olarak bilinen "Siber Güvenlik Olgunluk Modeli Sertifikasyonu" uygulama modelini geliştirdiği görülmektedir. Savunma sanayine özel olarak geliştirilen bu uygulama modeli ile birlikte savunma sanayi projelerinde tedarikçi ve alt tedarikçilerden kaynaklanan bilgi güvenliği riskinin en aza indirilmesi hedeflenmektedir.

Makalenin amacı yukarıda belirtilen genel ve özel (savunma sanayi) kapsamlı bu iki örnek çerçevesinde bilgi güvenliği yönetimi uygulamalarının geçmişten günümüze ne yönde ilerlediğini ortaya koymak, bu hususta savunma sanayimizin farkındalığını arttırarak yeni yaklaşımlarla ilgili olarak kuruluşlara yol göstermek ve ortaya konan bilgiler ışığında gelecekteki uygulamalara yönelik okuyucunun perspektifine katkı sağlamaktır.

Bu makalede;

- Kurumsal bilgi güvenliğinin günümüzdeki öneminden bahsedilerek yukarıda ifade edilen duruma örnek olarak gösterilebilecek iki ayrı bilgi güvenliği yönetimi uygulaması; savunma sanayine yönelik geliştirilen Siber Güvenlik Olgunluk Modeli Sertifikasyonu (CMMC v1.2) ile organizasyonların genel faaliyetleri göz önünde bulundurularak hazırlanan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı hakkında bilgi verilmiş,
- CMMC v1.02 ile ISO/IEC 27001 standardı kapsam, gereksinim ve belgelendirme süreçleri bakımından karşılaştırılarak CMMC'ye geçiş için kuruluşlarca gerçekleştirilmesi gerekli temel faaliyetler belirtilmiş,
- Söz konusu uygulamaların özellikleri ile gelecekte bilgi güvenliği uygulamalarının ne yönde ilerleyeceğine ve bu kapsamda ülkemizde yapılması gerekenlere dair değerlendirmeler sunulmuştur.

Buna uygun olarak;

Bölüm 2'de ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı hakkında temel bilgilere,

Bölüm 3'de Siber Güvenlik Olgunluk Modeli Sertifikasyonu (CMMC) hakkında temel bilgilere,

Bölüm 4'de ISO/IEC 27001 Standardı ile CMMC'nin kapsam, gereksinimler ve belgelendirme süreçleri bakımından karşılaştırılması neticesinde elde edilen bulgulara,

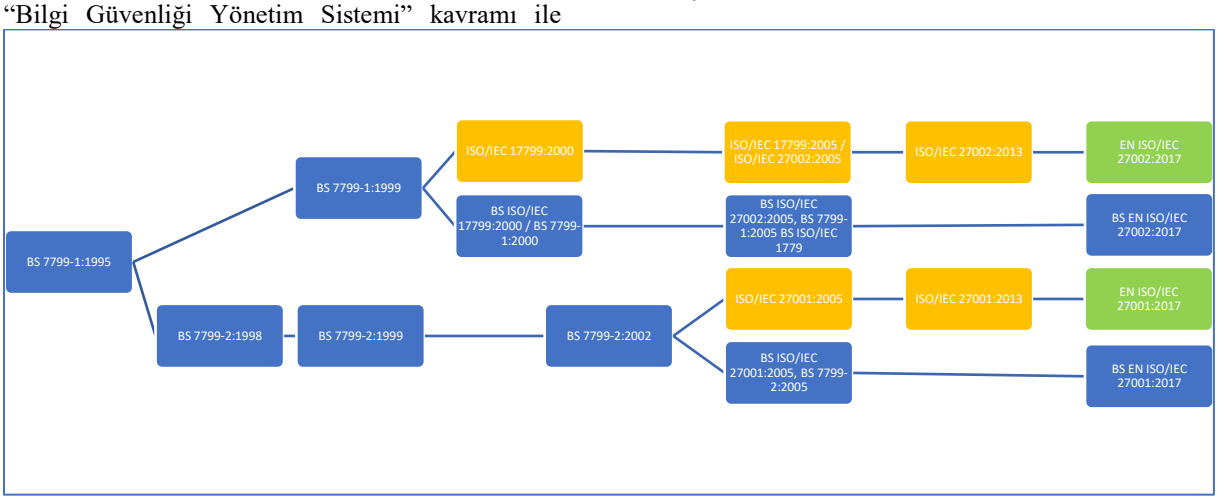
Bölüm 5'de kuruluşların CMMC'ye geçiş için gerçekleştirmesi gerekli faaliyetlere dair açıklamalara,

Sonuç ve Değerlendirme bölümünde ise elde edilen bilgi ve bulgular çerçevesinde bilgi güvenliği uygulamalarında geleceğe dair öneri ve değerlendirmelere yer verilmiştir.

II. ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ STANDARDI (ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD)

Bilgi teknolojilerinin yaygınlaşmasıyla artan bilgi sistemlerine yönelik tehditlere karşı tedbir alınması sorumluluğu 1990'lı yıllara kadar yalnızca organizasyonların bilgi teknolojileri birimleri üzerindeyken, 1995 yılında BSI tarafından yayınlanan BS 7799-1 standardında ön görülen "Bilgi Güvenliği Yönetim Sistemi" kavramı ile birlikte bilgi güvenliğinin sağlanması sorumluluğu ve ilgili görevler organizasyonun tümüne yayılmıştır [8].

Bu standart aynı zamanda Şekil 1'de gösterilen gelişme aşamalarında da görüleceği üzere ISO (International Organization for Standardization) tarafından yayınlanan ve kuruluşlarda faaliyet konularından bağımsız olarak oluşturulabilecek bir bilgi güvenliği yönetim sisteminin sağlaması gereken şartları tanımlayan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardının da temelini oluşturmaktadır.



Şekil 1. ISO/IEC 27001 Gelişim Aşamaları [9]

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardının ilk hali 2005 yılında ISO bünyesinde bulunan Bilgi Teknolojileri Ortak Teknik Komitesi JTC1'e (Joint Technical Committee 1) bağlı Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruma Alt Komitesi SC27 (Sub Committee 27) tarafından hazırlanmıştır [10].

EN ISO/IEC 27001:2017 numaralı EN standardı ise ISO'nun yayınladığı ISO/IEC 27001:2013 standardının 2017 yılında CEN (European Committee for Standardization) tarafından yayınlanan güncel versiyonudur [11]. CEN tarafından yayınlanan bu son versiyon ile ISO tarafından yayınlanan bir önceki versiyon arasında gereksinimler yönünden herhangi bir fark bulunmamaktadır.

CEN tarafından yayınlanan versiyon ayrıca TSE tarafından 2017 yılında "Türk Standardı" olarak kabul edilmiş, Türkçe 'ye çevrilerek 2018 yılında TS EN ISO/IEC 27001 "Bilgi teknolojisi- Güvenlik teknikleri- Bilgi güvenliği yönetim sistemleri- Gereksinimler" başlığıyla ülkemizde de yayınlanmıştır [12]. Bu çalışmada ISO/IEC 27001:2017 standardındaki ifadelerin Türkçe karşılıkları için TS EN ISO/IEC 27001:2017 standardından faydalanılmıştır.

III. SİBER GÜVENLİK OLGUNLUK MODELİ SERTİFİKASYONU (CYBERSECURITY MATURITY MODEL CERTIFICATION)

Siber Güvenlik Olgunluk Modeli Sertifikasyonu veya İngilizce adıyla "Cybersecurity Maturity Model Certification-CMMC" Amerika Birleşik Devletleri Savunma Bakanlığı'nın (Department of Defense-DoD) yürütmekte olduğu savunma sanayi projelerinde bilgi güvenliği alt yapısını güçlendirmek için tedarikçilerinden gerçekleştirmesini beklediği ve modele ait gereksinimlerin uygulamaya bağlı olarak 5 ayrı olgunluk seviyesi ile ifade edildiği bir bilgi güvenliği yönetim modelidir.

ABD savunma sanayi sektörünün çok büyük ve kapsamlı olması dolayısıyla ABD Savunma Bakanlığı tarafından, savunma sanayi sektöründe bulunan ve "Kontrollü Gizli Olmayan Bilgi" (CUI-Controlled Unclassified Information) ve "Federal Sözleşme Bilgisi" (FCI- Federal Contract Information) olarak ifade edilen bilgilerin güvenliğinin gerektiği şekilde sağlanamaması durumunda önemli ulusal güvenlik risklerinin oluşacağı değerlendirilmektedir [13].

Burada sözü 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 sınıflandırılmış olanlar hariç olmak üzere hükümetin oluşturduğu veya sahip olduğu veya bir kuruluşun hükümet adına veya hükümet için oluşturduğu veya sahip olduğu gizli olmayan ancak yürürlükteki yasalar, düzenlemeler ve hükümet genelindeki politikalar uyarınca ve bunlarla tutarlı olarak koruma veya yaygınlaştırma kontrolü gerektiren bilgiler olarak tanımlanırken "Federal Sözleşme Bilgisi-FCI"; bir ürün veya hizmetin hükümete sunulması veya geliştirilmesi için bir sözleşme kapsamında hükümet tarafından sağlanan veya hükümet için oluşturulan, kamuya açıklanması amaçlanmayan bilgileri ifade etmektedir.

Bu bilgilerin güvenliğinin zafiyete uğrama riskini azaltmak için ABD Savunma Bakanlığı'na bağlı Tedarik ve İdame Ofisi (The Office of the Under Secretary of Defense for Acquisition and Sustainment- OUSD(A&S)), gizli olmayan iletişim ağlarında bilgi güvenliğini sağlamak için ABD Savunma Bakanlığı paydaşları, üniversitelere bağlı araştırma merkezleri (UARC), federal olarak finanse edilen araştırma ve geliştirme merkezleri (FFRDC) ve sektör ile birlikte ortak çalışmalar gerçekleştirmiş ve bu çalışmaların sonucunda ortak bilgi güvenliği kriterlerini tanımlamak amacıyla NIST SP 800-171, NIST SP 800-53 ve NAS9933 gibi bir çok bilgi güvenliği rehber ve standardından da faydalanarak CMMC adı verilen bilgi güvenliği yönetim modelini geliştirmiştir.

IV. ISO/IEC 27001 VE CMMC v.1.02 KAPSAM, GEREKSİNİMLER VE BELGELENDİRME SÜREÇLERİ (ISO/IEC 27001 AND CMMC v.1.02 SCOPE, REQUIREMENTS AND CERTIFICATION PROCESSES)

4.1 Kapsam

Söz konusu bilgi güvenliği uygulamaları kapsam yönüyle ele alındığında EN ISO/IEC 27001:2017 standardı kapsamında, organizasyonun bağlamına uygun bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereksinimlerin tanımlandığı görülmektedir. Standart kapsamında sektör ayrımı yapılmamış olduğundan gereksinimler genel niteliğe sahip ve tüm sektörlere uygulanabilir olacak şekilde oluşturulmuştur.

Standardın uygulanması için herhangi bir zorunluluk bulunmamakla birlikte, mevzuat, sözleşme vb. diğer özel şartlar dolayısıyla organizasyonlarda standardın uygulanmasının gerekli olacağı durumlar ortaya çıkabilmektedir.

EN ISO/IEC 27001:2017 standardı aynı zamanda Avrupa'da 34 ülkenin üye olduğu CEN ve dünyada 165 ülkenin üye olduğu bağımsız bir organizasyon olan ISO tarafından kabul edilmiş olması nedeniyle uluslararası alanda en geniş ölçekte kabul gören bilgi güvenliği yönetim sistemi standardı olma özelliğine de sahiptir [14].

CMMC kapsamında ise ISO/IEC 27001'den farklı olarak, savunma sanayi sektörü kuruluşlarına özel, 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 koymak için gerekli gereksinimler tanımlanmıştır. Böylece ilgili savunma sanayi kuruluşunun hassas bilgileri yeteri kadar koruyabileceği konusunda ABD Savunma Bakanlığı'na daha fazla güvence sağlanması hedeflenmektedir [15].

Sektörde CMMC uygulamalarına ilişkin ise "Savunma Federal Satın Alma Yönetmeliği Eki: Yüklenicinin Siber Güvenlik Gereksinimlerini Uygulamasının Değerlendirilmesi" (DFARS Case 2019-D041) mevzuatı 30/11/2020 tarihinde geçerli olmak üzere 19/09/2020 tarihinde ABD resmî gazetesinde (Federal Register) yayınlanmıştır.

Bu mevzuat uyarınca 1/10/2025 tarihinden önce ABD Savunma Bakanlığı yüklenici ve alt yüklenicilerinin bilgi güvenliği alt yapılarını CMMC şartlarına uygun hale getirmeleri gerekmektedir. Söz konusu tarihten sonra teklif sahibi veya yüklenici, gerekli CMMC seviyesi için geçerli (yani üç yıldan daha eski olmayan) sertifikaya sahip değilse ABD Savunma Bakanlığı ihalelerine katılamayacaktır. Buna ilaveten, CMMC sertifikasyon gereksinimlerinin, her bir alt yükleniciye aktarılan gizli olmayan bilgilerin hassasiyetine bağlı olarak, tüm kademelerde alt yüklenicilere de aktarılması beklenmektedir [16]

Buradan da anlaşılacağı üzere her ne kadar CMMC uygulamaları mevzuat yönüyle ulusal nitelik taşıyor olsa da belirtilen tarih itibariyle dünya çapında ABD Savunma Bakanlığı ile tedarikçi statüsünde çalışan tüm savunma sanayi kuruluşları ve onların alt tedarikçileri için CMMC modelinin uygulanmasının zorunluluk arz edeceği görülmektedir.

4.2. Gereksinimler

ISO/IEC 27001 Standardına göre gereksinimlerin yer aldığı standart içeriğine ulaşabilmek için organizasyonların ücreti karşılığında standart dokümanını satın almaları gerekmektedir. Standardın Türkçe ve İngilizce versiyonu TSE tarafından satılmakta olup diğer yabancı dillerdeki versiyonlarına ISO ve CEN 'in internet siteleri üzerinden dijital olarak ulaşılabilmektedir.

Standart içeriğinde bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesine dair gereksinimler ve diğer hususlar toplam 11 ana başlık altında ifade edilmiştir.

Bu başlıklar, yönetim sistemi standartlarında uygulanan "yüksek seviyeli yapı" HLS (High Level

Structure) gereği ISO tarafından diğer yönetim sistemi standartlarında da kullanılan genel ifadelerden oluşmaktadır [17].

Söz konusu "yüksek seviyeli yapı" gereği standart kapsamında sağlanması gereken gereksinimler 4 ila 10. Maddede belirtilen başlıklarda tanımlanmaktadır. Bu maddeler ile tanımlanmış olan gereksinimler herhangi bir kritere, seviyeye veya sektöre bağlı olmaksızın her tipteki organizasyona ve bilgi varlığına uygulanabilir nitelik taşımaktadır.

Buna göre kuruluşlar standarda göre 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 oluşturmalı ve kurumsal rolleri tanımlama,
- "6. Planlama" başlığı uyarınca risk ve fırsatları belirlemeli, riskleri değerlendirmeli, risk işleme sürecini tanımlamalı ve bilgi güvenliği yönetim sisteminin amaçlarını belirleyerek nasıl başarılacağını planlama,
- "7. Destek" başlığı uyarınca bilgi güvenliği yönetim sistemi için kaynakları, yeterlilikleri tanımlamalı, 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 gerçekleştirmeli ve bilgi güvenliği yönetim sistemini sürekli iyileştirme,

faaliyetlerini sürdürülebilir ve etkin şekilde uygulayabilmelidir [18].

Standart ekinde bulunan tabloda ise "6. Planlama" maddesinde yer alan ve seçilen bilgi güvenliği risk işleme faaliyetlerinin uygulanmasında referans olarak kullanılacak kontrol amaçları ve kontroller doğrudan ISO/IEC 27002:2013 standardı madde 5 ila 18. Maddelerinde belirtilen ifadeler referans alınarak listelenmiştir [19].

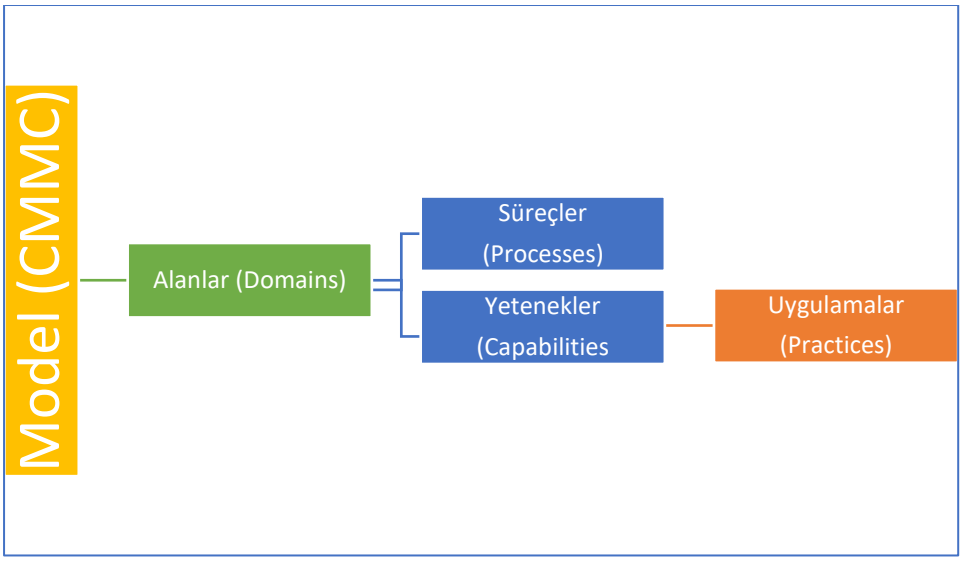
Buna göre kuruluşlar EN ISO/IEC 27001:2017 Ek A ile verilen listede yer alan; "A.5 Politika", "A.6 Bilgi güvenliği organizasyonu", "A.7 İnsan kaynakları güvenliği", "A.8 Varlık yönetimi", "A.9 Erişim kontrolü", "A.10 Kriptografi", "A.11 Fiziksel ve çevresel güvenlik", "A.12 İşletim güvenliği", "A.13 Haberleşme güvenliği", "A.14 Sistem temini, geliştirme ve bakımı", "A.15 Tedarikçi ilişkileri", "A.16 Bilgi güvenliği ihlal yönetimi", "A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları", "A.18 Uyum" maddelerinde yer alan kontrol faaliyetlerini standardın "6. Planlama" maddesinde belirtilen esaslara uygun olacak şekilde gerçekleştirmelidir.

CMMC v1.02 için ise bilgi güvenliği yönetim sistemi standartlarından farklı olarak gereksinimlerin yer aldığı çerçeve doküman CMMC V1.02 (CMMC_ModelMain_V1.02_20200318) ve diğer yardımcı dokümanlar ABD Savunma Bakanlığı'na bağlı Tedarik ve İdame Ofisi'ne ait internet adresinde genel kullanıma açık şekilde yayınlanmaktadır [20].

Modele ait ana dokümanda siber güvenlik olgunluk modeli 5 ayrı seviyede ele alınmaktadır. Burada sözü geçen olgunluk modeli; kuruluşun iş sürecini yönetmedeki performanslarını değerlendirmek için bir takım kilit süreç alanları ve farklı olgunluk seviyelerinden oluşan bir değerlendirme yaklaşımıdır [21] ve buna göre her bir seviye için dokümanda, korunması gereken ve tehdide konu olan bilginin tipine ve hassasiyetine göre ayrı süreçlere ve uygulamalara yer verilmiştir [22].

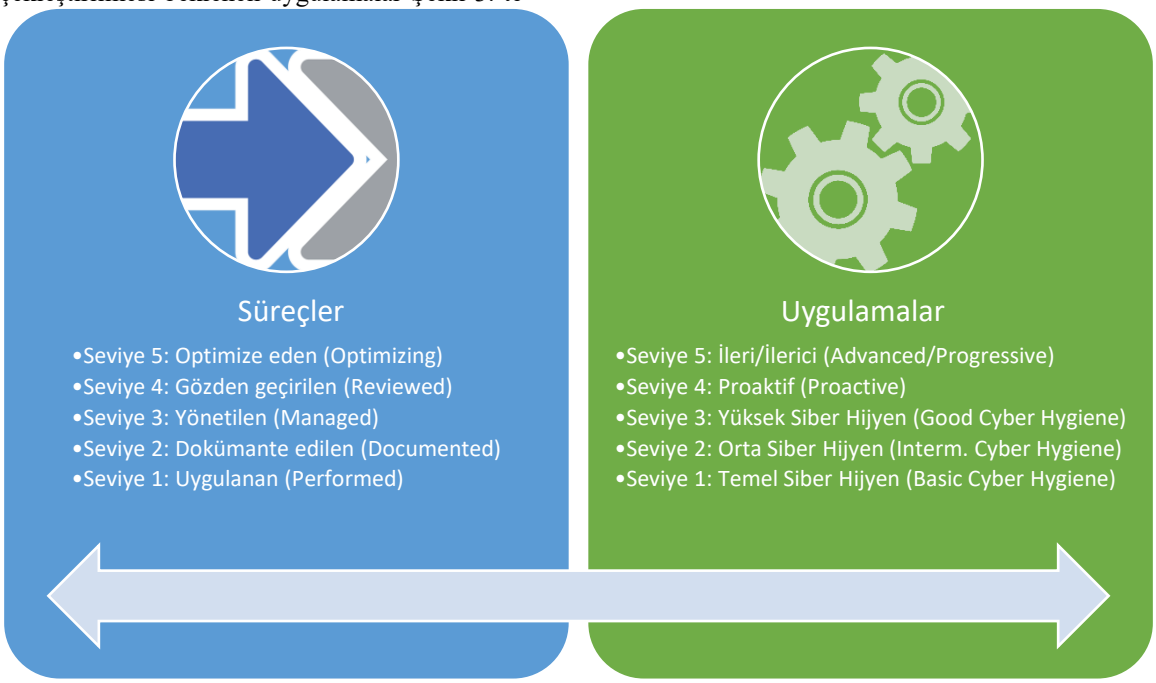
Dokümanda FCI için "temel koruma", CUI için ise daha ileri seviye "güvenlik" gereksinimleri tanımlanmaktadır. Savunma sanayi kuruluşu CMMC uygulamalarını organizasyonunun tamamında veya yalnızca korunması gereken bilginin kullanıldığı ve saklandığı biriminde/bölümünde gerçekleştirebilir.

CMMC modeli çerçevesinde "süreç" ve "uygulamalar" Şekil 2'de gösterildiği üzere belirli sayıda "alan" içerisinde tanımlanmıştır.



Şekil 2. CMMC Çerçeve Modeli

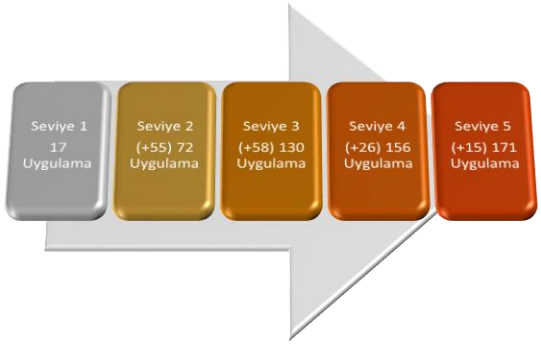
Buna göre model kapsamında her bir alan için süreç olgunlukları ile yetenekler kapsamında gerçekleştirilmesi beklenen uygulamalar Şekil 3.'te gösterildiği gibi 5 ayrı seviye içerisinde gruplandırılmıştır.



Şekil 3. CMMC Seviyeleri

Bu doğrultuda organizasyon hedeflediği seviye gereksinimlerini sağlamak için, tüm alanlarda hedeflenen seviyede ön görülen süreç olgunluk gereksinimini sağlamalı bununla birlikte hedeflenen seviyede ve altındaki seviyelerde tanımlanan uygulamaları da gerçekleştirmelidir. Süreç olgunluk seviyesi ve gerçekleştirilen uygulamaların seviyelerinin farklı olması durumunda alt seviyedeki gereksinimlerin sağlandığı kabul edilmektedir.

Burada yer alan her bir seviye uygulamalara ait özellikleri belirlerken aynı zamanda süreçlerin ne ölçüde kurumsallaştırıldığını da ifade etmektedir. Burada süreçlerin kurumsallaşma ölçüsü arttıkça organizasyonun gerekli faaliyetleri sürdürülebilir, etkin ve yüksek kalitede gerçekleştireceği ön görülmektedir. Bunlarla birlikte CMMC modelinde her bir seviye için ilgili alanda uygulanmak üzere toplam 171 uygulama tanımlanmıştır. Bu uygulamaların her bir seviye için dağılımları Şekil 4'te gösterilmiştir.



Şekil 4. Uygulamaların Dağılımı

4.3. Belgelendirme Süreçleri

Belgelendirme süreçlerine bakıldığında hem ISO/IEC 27001 hem de CMMC v1.02'ye göre belgelendirmenin üçüncü taraf kuruluşlarca gerçekleştirildiği görülmektedir. ISO yapısı ve amaçları dolayısıyla belgelendirme faaliyeti yapmamakta ISO standartlarına göre belgelendirme faaliyetleri bağımsız belgelendirme kuruluşlarınca gerçekleştirilmektedir. ISO/IEC 27001 standardı gereksinimleri doğrultusunda bilgi güvenliği yönetim sistemini oluşturan kuruluşların üçüncü taraf denetimlerinin gerçekleştirilmesi ve sistemlerinin belgelendirilmesi için bu belgelendirme kuruluşlarına başvurmaları gerekmektedir.

Burada başvurulan belgelendirme kuruluşunun uygunluk değerlendirme kapsamında yönetim sistemlerinin tetkikini ve belgelendirmesini sağlayan kuruluşlar için şartları tanımlayan (TS) (EN) ISO/IEC 17021-1:2015 standardına göre IAF (International Accreditation Forum) üyesi bir akreditasyon kuruluşundan akredite olması önemlidir. Bu sayede edinilen belgenin ulusal ve uluslararası geçerliliği güvence altına alınmış olacaktır [23].

Benzer şekilde ABD Savunma Bakanlığı veya bünyesinde bulunan Tedarik ve İdame Ofisi 'de CMMC modeli kapsamında herhangi bir belgelendirme faaliyeti gerçekleştirmemektedir.

Bununla birlikte ABD Savunma Bakanlığı CMMC modeli kapsamında tanımlanan iş ve işlemlerin yürütülmesinde düzenleyici otorite olarak görev yapmak üzere bağımsız bir organizasyon olan ve uygunluk değerlendirmesi yapan kuruluşları akredite eden kuruluşlar için şartları tanımlayan ISO/IEC 17011 standardına göre akredite edilen CMMC Akreditasyon Kuruluşu'nu (CMMC-AB) yetkilendirmiştir [24].

CMMC-AB düzenleyici otorite olarak, üçüncü taraf denetimi ve belgelendirme gibi görevleri yürütmek üzere CMMC üçüncü taraf denetleme organizasyonlarını (C3PAO) ve CMMC denetçilerinin ve eğitimcilerinin belgelendirilmesi için CMMC denetçi ve eğitimci belgelendirme organizasyonlarını (CAICO) yetkilendirmekte ve akredite etmektedir.

Yukarıda ifade edilenler doğrultusunda CMMC modeli gereksinimlerini yerine getiren kuruluşlar üçüncü taraf denetimlerinin gerçekleştirilmesi ve belgelendirme için CMMC-AB tarafından yetkilendirilen C3PAO kuruluşlarından birine başvurmalıdır. C3PAO kuruluşlarının listesi CMMC-AB internet sitesi üzerinden yayınlanmaktadır.

V. ISO/IEC 27001'DEN CMMC'YE GEÇİŞ VE ÖNERİLER (TRANSITION TO ISO/IEC 27001 TO CMMC AND SUGGESTIONS)

Günümüzde birçok kuruluş hem yüksek tanınırlık seviyesine sahip olması hem de geniş kapsamdaki uygulama alanları dolayısıyla ISO/IEC 27001 standardına göre belgelendirilmiş bir bilgi güvenliği yönetim sistemine sahiptir. Ancak yukarıda da ifade edildiği üzere gelişen teknoloji ile birlikte artan bilgi güvenliği riskleri doğrultusunda özellikle savunma sanayinde daha derin ve kapsamlı yeni bilgi güvenliği modellerinin oluşturulmasına ihtiyaç duyulmuş ve bu kapsamda ilk örneklerden biri olan CMMC modeli ABD Savunma Bakanlığı tarafından oluşturulmuştur.

Buna bağlı olarak da CMMC mevzuatında yer alan uygulama takvimine göre 1/10/2025 tarihinden itibaren ABD Savunma Bakanlığı'na bağlı projelerde ana veya alt tedarikçi statüsünde olan tüm kuruluşların CMMC modelini uygulamaları zorunluluk arz etmektedir.

Savunma sanayinde faaliyet gösteren kuruluşların önemli bir kısmı halihazırda ISO/IEC 27001 standardına göre oluşturulmuş bir bilgi güvenliği yönetim sistemine sahiptir. ABD savunma sanayinin uluslararası ölçekte en büyük paya sahip olması dolayısıyla yakın gelecekte bu kuruluşların neredeyse tamamının mevcut bilgi güvenliği yönetimi alt yapılarını CMMC modeline uygun hale getirmelerinin gerekeceği değerlendirilmektedir.

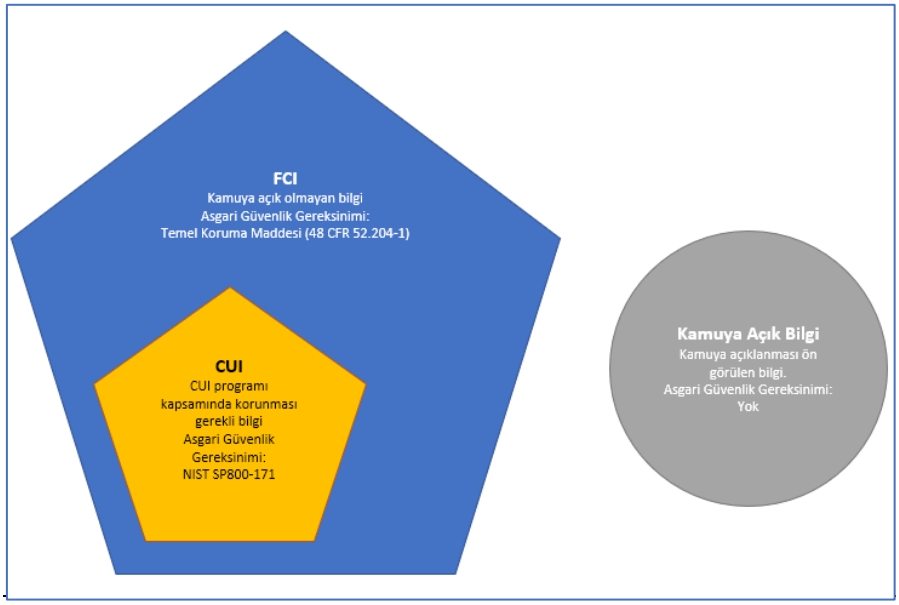
Bu bağlamda her iki bilgi güvenliği yönetim modelinin özellikleri, gereksinimleri ve birbirleriyle olan farklılıkları dikkate alındığında, hali hazırda ISO/IEC 27001 kapsamında bir bilgi güvenliği yönetim sistemine sahip olan bir savunma sanayi kuruluşunun CMMC modeline göre geçiş için temel olarak;

1) Bilgi varlıklarının sınıflandırılması
2) İhtiyaç duyulan olgunluk seviyesinin belirlenmesi
3) ISO/IEC 27001 şartları, bilgi güvenliği kontrolleri ve CMMC uygulamaları
4) Bilgi güvenliği politikası
5) Dokümantasyon

konularını ele alarak birtakım faaliyetleri gerçekleştirmesi gerekmektedir.

5.1. Bilgi Varlıklarının Sınıflandırılması

ISO/IEC 27001 standardı kapsamında bilgi güvenliği yönetim sistemine sahip kuruluşlar bilgi varlıklarını standardın gereksinimlerine uygun olarak kuruluş bağlamları ve kendi risk değerlendirme sonuçlarına göre sınıflandırmaktadır. CMMC modelinde ise uygulanacak olan olgunluk seviyesinin tespit edilebilmesi ve buna göre uygulamaların belirlenebilmesi için kuruluşa ait bilgi varlıklarının "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 sınıflandırılması gerekmektedir.
İki ayrı şekilde tanımlanan bilgi türünün birbirleriyle ve halka açık bilgi ile olan ilişkileri Şekil 5'de gösterilmiştir [25].



Şekil 5. 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.
Örnek vermek gerekirse; sözleşme kapsamında yer alan ve kamuya açıklanması ön görülmeyen performans raporları, süreç dokümanları, organizasyon ve program çizelgeleri FCI olarak tanımlanırken [26], yasal materyaller, sağlık belgeleri, teknik çizimler ve planlar, fikri mülkiyetler, ITAR kontrollü belgeler/ürünler CUI kapsamında tanımlanmaktadır [27] .
Bu doğrultuda kuruluş öncelikle;

- 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 güncellemelidir.

Devamında ise kuruluş ISO/IEC 27001'den farklı olarak oluşturulan güncel ve CMMC modeline uygun bilgi envanterini kapsamına alacak şekilde uygulanacak olgunluk seviyesine göre faaliyetleri planlanmalıdır.

5.2. İhtiyaç Duyulan Olgunluk Seviyesinin Belirlenmesi

CMMC modelinde bulunan seviyeler korunması gerekli bilginin türüne, hassasiyetine, maliyetlere, tabii olunan mevzuata, uygulamanın ve değerlendirmenin karmaşıklığı gibi birtakım faktörlere bağlı olarak kademelendirilmiştir. Buna göre seviyelerin odaklandığı bilgi varlığı türleri Tablo 1'de ifade edildiği gibi tanımlanmaktadır.

Tablo 1. CMMC Seviyeleri ve Odaklandığı Alanlar

Seviye	Alan
1	Federal Sözleşme Bilgilerinin (FCI) korunması
2	Kontrollü Gizli Olmayan Bilgilerin (CUI) korunması aşamasına (Seviye 3) geçiş
3	CUI güvenliğinin sağlanması
4-5	CUI güvenliği ile gelişmiş ısrarcı tehdit (APT) riskinin azaltılması

Kuruluş, CMMC kapsamında yer alan projelere ait bilgi envanterini CMMC modelinde yer alan tanımlar uyarınca yeniden gözden geçirmesinin ardından elde ettiği sonuçlara göre ABD Savunma

Bakanlığının Bilgi Taleplerinde (Requests for Information-RFI) ve Teklif Taleplerinde (Requests for Proposals-RFP) ön gördüğü gereksinimlere uygun olarak olgunluk seviyesini belirlemelidir.
Buna göre CMMC modelinde "kamuya açık bilgi" kapsamında yer alan bilgi varlıkları için herhangi bir tedbir ön görülmemekte, "kamuya açık olmayan federal sözleşme bilgisi (FCI)" kapsamında yer alanlar için en düşük seviye 1, "kontrollü gizli olmayan bilgi (CUI) programı kapsamında korunması gerekli bilgi" kapsamında yer alan bilgi varlıkları için ise en düşük seviye 3 olgunluk seviyesinin sağlanması gerekmektedir.
Bunlara ek olarak bilgi varlıklarının hassasiyetinin yüksek olması ve bilgi varlıklarının gelişmiş ısrarcı tehdit (Advanced Persistent Threats-APT) olarak nitelendirilen tehditlere karşı da korunması ön görülüyorsa güvenlik gereksinimlerini karşılayacak şekilde olgunluk seviyesinin 4'e veya 5'e çıkarılması gerekmektedir.
Örneğin kritik alt yapılara bağlı programlara ait bilgiler ile kuruluş için misyonunu yerine getirme veya iş yapma kabiliyeti üzerinde ciddi etkiye sahip kritik işlemlerde kullanılan hassas kontrollere ait veriler, talimatlar veya benzersiz veri koleksiyonları olarak tanımlanan Yüksek Değerli Varlıklar (HVA) CMMC seviye 4 veya 5 gerektiren bilgi varlıklarıdır [28].

5.3. ISO/IEC 27001 Şartları, Bilgi Güvenliği Kontrolleri ve CMMC Uygulamaları

Önceki bölümlerde ifade edildiği üzere ISO/IEC 27001 standardında gereksinimler standardın 4 ila 10. Maddelerinde yer alan ve CMMC v1.02'den farklı olarak risk işleme faaliyetlerini de içeren şartlar ile yine standard Ek A'da yer alan 114 kontrol faaliyeti ile tanımlanmakta iken CMMC v1.02'de gereksinimler standartta belirtilen kontrol faaliyetlerine benzer şekilde farklı konu alanlarında toplam 171 uygulama tanımlanmıştır. Burada standarttan farklı olarak uygulamaların sayıları ve ayrıntıları hedeflenen olgunluk seviyesiyle birlikte artmaktadır.
Böylece CMMC modeline geçişi için kuruluş öncelikle ISO/IEC 27001 standardına göre gerçekleştirmiş olduğu risk işleme faaliyetlerini gözden geçirmeli, standart Ek A'da ifade edilen kontrollere ilave olarak planladığı diğer kontrolleri de göz önünde bulundurarak mevcut kontrollerini hedeflenen CMMC olgunluk seviyesinde bulunan konu alanlarında yer alan uygulamalarla eşleştirmelidir.
Bu bağlamda CMMC güvenlik alanlarına ve yeteneklerine bağlı uygulamaların ISO/IEC 27001'de belirtilen karşılıkları ISO/IEC 27002 ve CMMC yardımcı dokümanında belirtilen amaçları, içerikleri ve örneklerine göre gözden geçirilerek Tablo 2 ile ifade edilmiştir.

Tablo 2. CMMC v1.02 Uygulamalarının ISO/IEC 27001 Karşılıkları [29], [30]

CMMC v1.02		**ISO/IEC 27001**	
Alan	**Yetenek**	**TS EN ISO/IEC 27001 Ana Madde**	**TS EN ISO/IEC 27001 Alt Madde**

Erişim Kontrolü	· Sistem erişim gereksinimleri oluştur · İç sistem erişimini kontrol et · Uzaktan erişimi kontrol et · Veri erişimi için yetkili kullanıcıları ve süreçleri kısıtla	A.9. Erişim kontrolü	A.9.1. Erişim kontrolünün iş gereklilikleri A.9.2. Kullanıcı erişim yönetimi A.9.3. Kullanıcı sorumlulukları A.9.4. Sistem ve uygulama erişim kontrolü
Varlık Yönetimi	· Varlıkları tanımla ve dokümante et	A.8.Varlık yönetimi	A.8.1. Varlıkların sorumluluğu A.8.2. Bilgi sınıflandırma A.8.3. Ortam işleme
Denetim ve Hesap Verebilirlik	· Denetim gereksinimlerini belirle · Denetimi gerçekleştir · Denetim bilgilerini tanımla ve koru · Denetim günlüklerini gözden geçir ve yönet	9.2 İç tetkik	-
Farkındalık ve Eğitim	· Güvenlik bilinci faaliyetlerini yürüt · Eğitim gerçekleştir	7.3. Farkındalık	-
		A.7. İnsan kaynakları güvenliği	A.7.2. Çalışma esnasında A.7.2.2. Bilgi güvenliği farkındalığı eğitim ve öğretimi
Yapılandırma Yönetimi	· Yapılandırma temellerini oluştur · Yapılandırma ve değişim yönetimini uygula	A.12. İşletim güvenliği	A.12.1. İşletim prosedürleri ve sorumlulukları A.12.5. İşletimsel yazılımının kontrolü
		A.14 Sistem temini, geliştirme ve bakımı	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2. Geliştirme ve destek süreçlerinde güvenlik
Tanımlama ve Kimlik Doğrulama	· Doğrulanmış kişilere erişim izni ver	A.9. Erişim Kontrolü	A.9.2. Kullanıcı erişim yönetimi
Olay Müdahalesi	· Olay karşılıklarını planla · Olayları algıla ve raporla · Bildirilen bir olaya yanıt geliştir ve uygula · Olay sonrası değerlendirmeyi uygula · Olay karşılıklarını dene	A.16. Bilgi güvenliği ihlal olayı yönetimi	A.16.1. Bilgi güvenliği ihlal olaylarının ve iyileştirmelerin yönetimi

Bakım	· Bakımı yönet	A.11. Fiziksel ve çevresel güvenlik	A.11.2. Teçhizat A.11.2.4. Teçhizat bakımı
Medya Koruma	· Medyayı tanımla ve işaretle · Medyayı koru ve kontrol et · Medyayı sterilize et · Taşıma sırasında medyayı koru	A.8. Varlık yönetimi	A.8.1. Varlıkların sorumluluğu A.8.2. Bilgi sınıflandırma A.8.3. Ortam işleme
Kişisel Güvenlik	· Personeli denetle · Personel işlemleri sırasında CUI'yi koru	A.7. İnsan kaynakları güvenliği	A.7.1. İstihdam öncesi A.7.2. Çalışma esnasında A.7.3. İstihdamın sonlandırılması ve değiştirilmesi
Fiziksel Koruma	· Fiziksel erişimi sınırla	A.11. Fiziksel ve çevresel güvenlik	A.11.1. Güvenli alanlar A.11.2. Teçhizat
Kurtarma	· Yedeklemeyi yönet	A.12. İşletim güvenliği	A.12.3. Yedekleme
Risk Yönetimi	· Riski tanımla ve değerlendir · Riski yönet	6. Planlama	6.1. Risk ve fırsatları ele alan faaliyetler
		8. İşletim	8.2. Bilgi güvenliği risk değerlendirme 8.3. Bilgi güvenliği risk işleme
Güvenlik Değerlendirmesi	· Bir sistem güvenlik planı geliştir ve yönet · Kontrolleri tanımla ve yönet · Kod incelemeleri gerçekleştir	A.17. İş sürekliliği yönetiminin bilgi güvenliği hususları	A.17.1 Bilgi güvenliği sürekliliği
Durumsal Farkındalık	· Tehdit izlemeyi uygula	A.6 Bilgi güvenliği organizasyonu	A.6.1 İç organizasyon A.6.1.4 Özel ilgi grupları ile iletişim
Sistemler ve İletişim Koruması	· Sistemler ve iletişim için güvenlik gereksinimlerini tanımla · Sistem sınırlarında iletişimi kontrol et	A.13. Haberleşme güvenliği	A.13.1. Ağ güvenliği yönetimi A.13.2. Bilgi transferi
Sistem ve Bilgi Bütünlüğü	· Bilgi sistemi kusurlarını tanımla ve yönet · Kötü amaçlı içeriği tanımla · Ağ ve sistem izlemeyi gerçekleştir · Gelişmiş e-posta korumaları uygula	A.12 İşletim güvenliği	A.12.6 Teknik açıklık yönetimi

		A.13 Haberleşme güvenliği	A.13.1 Ağ güvenliği yönetimi A.13.2 Bilgi transferi
		A.14. Sistem temini, geliştirme ve bakımı	A.14.2 Geliştirme ve destek süreçlerinde güvenlik

Buna göre kuruluş hali hazırda ISO/IEC 27001 kapsamındaki uygulamalarını CMMC alan ve yeteneklerine bağlı belirtilen uygulamalar ile karşılaştırarak boşluk analizi yapmalı ve eksik uygulamaları tespit ederek gerekli tedbirleri almalıdır.
Örneğin bu faaliyetlerde özellikle "Denetim ve Hesap Verebilirlik" veya "Farkındalık ve Eğitim" gibi CMMC 'de ayrıntılı uygulamalarına yer verilen ancak ISO/IEC 27001'de alt maddeler ile kontrol faaliyetlerine yönelik detay verilmeyen konu alanlarının öncelikle ele alınması daha uygun olacaktır.

5.4. Bilgi Güvenliği Politikası

ISO/IEC 27001 standardına göre kuruluşun üst yönetimi bir bilgi güvenliği politikası belirlemeli, yazılı hale getirmeli ve kuruluş içerisinde belirlenen politikaya dair yeterli farkındalığı sağlamalıdır. CMMC modeli için ise politika seviye 2 olgunluk kriterlerinden biri olup her bir alan için ayrı ayrı oluşturulmalıdır.
Buna bağlı olarak kuruluşlar her bir kontrol alanı için politikalarını belirlemeli ISO/IEC 27001 uygulamalarında olduğu gibi yazılı hale getirmeli ve gerekli farkındalığı sağlamalıdır. Ayrıca alan kapsamında tanımlanan uygulamalar da belirlenen politikayı sağlayacak şekilde oluşturulmalı ve dokümante edilmelidir.

5.5. Dokümantasyon

ISO/IEC 27001 uygulamalarında standart gereği dokümante edilmesi gerekli bilgiler standardın içerisinde belirtilmektedir. Bununla birlikte bazı hususlarda dokümantasyon gerekliliği kuruluşun inisiyatifine bırakılmıştır. Örneğin ISO/IEC 27001'den farklı olarak CMMC modelinde olgunluk seviyesi 2'den itibaren politikanın sağlanması için tüm uygulamaların dokümante edilmesi gerekmektedir.
Buna benzer durumlara karşı tedbir alınması bakımından kuruluş uygulanacak olgunluk seviyesine göre CMMC modelinin gerektirdiği dokümantasyon şartlarını da mutlaka gözden geçirilmeli, eksik dokümanların oluşturulmasını sağlamalıdır.

VI. SONUÇ VE DEĞERLENDİRME (RESULT AND EVALUATION)

Bilginin öneminin artması ile birlikte bilgi güvenliğine yönelik tehditler de artmaktadır. Buna bağlı olarak mevcut bilgi güvenliği savunma alt yapılarının da etkinliklerinin korunması için sürekli güncellenerek geliştirilmesi ve yeni güvenlik modellerinin oluşturulması gerekmektedir.
Bu makale çalışmasında bu gelişim sürecinin farklı aşamalarına örnek oluşturabilecek iki farklı bilgi güvenliği yönetimi modeli olan ISO/IEC 27001 standardı ile CMMC uygulamaları ele alınmış, her iki model karşılaştırılarak buradan elde edilen bilgiler ile bir kuruluşun ISO/IEC 27001 standardına göre oluşturduğu bilgi güvenliği yönetim sistemini CMMC modeline uygun hale getirmesi için temel olarak yapması gerekenler ortaya konmuştur.
Makalede de özetlendiği üzere ilk bilgi güvenliği standardı olan ve 1995 yılında İngiliz BSI tarafından yayınlanan BS 7799 standardı ile başlayan kurumsal ölçekte bilgi güvenliğine yönelik çalışmalar [31], 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 ve bu standart ise zaman zaman ihtiyaçlara ve karşılaşılan risklere göre güncellenmeye de devam etmektedir.
ISO/IEC 27001 standardı ile sektöründen bağımsız her tip organizasyon ve her türde bilgi varlığı için yeterli seviyede koruma sağlayabilecek bir bilgi güvenliği yönetim sisteminin oluşturulması ve belgelendirilmesine yönelik gerekli gereksinim ve şartların ortaya konması hedeflenmiştir. Bu doğrultuda standardın uygulama ve belgelendirme kapsamının çok geniş olduğu bununla beraber gereksinim bakımından günümüzde artık temel kabul edilebilecek genel tedbirleri içerdiği görülmektedir. Ancak günümüzde bilgi güvenliğine yönelik tehditler eskiye oranla çok daha hızlı değişmekte ve gelişmekte buna bağlı olarak potansiyel hedefler de çoğalmaktadır. Bu durum bilgi güvenliği yönetimi

noktasında önceki uygulamalardan farklı olarak hem bilgi varlıklarının türüne hem de sektöre göre özelleştirilen daha ileri seviyede, daha ayrıntılı ve daha etkili bilgi güvenliği tedbirlerinin alınmasını gerektirmektedir.

Buradan hareketle ABD Savunma Bakanlığı başta ulusal güvenliği korumak için diğer paydaşlarıyla birlikte kendi tedarikçi kuruluşlarına yönelik bir bilgi güvenliği yönetim modeli geliştirmiştir. CMMC adı verilen bu model EN ISO/IEC 27001 standardından farklı olarak kapsam yönüyle yalnızca belirli bir sektöre ve belirli bilgi türlerine odaklanmaktadır. Bu bağlamda CMMC 'de tanımlı gereksinimlerin ilgili olduğu sektöre ve bilgi türlerine özel olacak şekilde ve ISO/IEC 27001'de yer alan kontrol sayısından daha çok sayıda uygulama ile daha ayrıntılı olarak ifade edildiği görülmektedir.

Yapılan bu çalışma sonucunda;

- CMMC 'nin gelecekte zorunluluk arz edeceği görüldüğünden özellikle ülkemizin göz bebeği olan savunma sanayi firmalarımızın uluslararası düzeyde rekabet edebilme kabiliyetinin sekteye uğramaması bakımından CMMC modeli kapsamında hazırlık çalışmalarına başlamasının büyük önem arz edeceği,
- Gelecekte bilgi güvenliği alanında mevcut güvenlik seviyelerini arttırmak veya korumak amacıyla yapılan çalışmaların genel ve geniş kapsamlı yönetim modellerinden çok sektöre ve bilgi türlerine özel kademeli yönetim modellerine odaklanacağı buna bağlı olarak temel bilgi güvenliği yönetimi standartlarının etkinliklerinin zamanla azalacağı,
- Özellikle kamu ve savunma sanayi sektöründe CMMC'ye benzer şekilde sektöre ve bilgi türlerine özel kademelendirilmiş gereksinimlere sahip bilgi güvenliği yönetimi modellerinin oluşturularak ivedilikle uygulanmaya başlanmasının ülkemizin ulusal güvenliğine yönelik siber tehditlerin bertaraf edilmesi bakımından kritik öneme sahip olduğu,
- Bu bakımdan mevcut 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında savunma sanayine özel herhangi bir çalışmanın yer almadığından bir sonraki strateji ve eylem planı için gerekli çalışmalara ivedilikle başlanmasının uygun olacağı,
- Bu kapsamda ülkemizin milli standart kuruluşu TSE'nin de mevcut uluslararası standartlardan faydalanarak ülkemiz savunma sanayine yönelik standart çalışması yapmasının faydalı olacağı,

değerlendirilmektedir.

KAYNAKLAR (REFERENCES)

[1] A. Akçoraoğlu, G. Üniversitesi, and İ. Bilimler, " 'Yeni Kapitalizm' Teorileri, Dijital Devrim ve Türkiye Kapitalizmi," Mülkiye Dergisi, vol. 43, no. 3, pp. 525–575, 2019.

[2] G. Canbek and Ş. Sağıroğlu, Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri. Ankara: Grafiker Yayıncılık, 2006.

[3] McAfee, "The Economic Impact of Cybercrime—No Slowing Down Executive Summary," 2018.

[4] The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," 2018.

[5] Ş. Sağıroğlu, M. Alkan, and R. Samet, Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık. Ankara: Grafiker Yayıncılık, 2018.

[6] E. Humphreys, "Information security management system standards," Datenschutz und Datensicherheit -DuD, vol. 35, no. 1, pp. 7–11, 2011, doi: 10.1007/s11623-011-0004-3.

[7] Ş. Sağıroğlu, O. Aktaş, and O. Alkan, Siber Güvenlik ve Savunma-Standartlar ve Uygulamalar. Ankara, 2019.

[8] E. Humphreys, "Information security management standards: Compliance, governance and risk management," Information Security Technical Report, vol. 13, no. 4, pp. 247–255, Nov. 2008, doi: 10.1016/j.istr.2008.10.010.

[9] "ISO/IEC 27001 International Information Security Standard published," BSI, 2005. https://www.bsigroup.com/en-GB/about-si/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/ (Erişim: Kas. 16, 2021).

[10] ISO Technical Committees. https://www.iso.org/technical-committees.html (Erişim Haz.. 05, 2021).

[11] CEN, "CEN/CLC/JTC 13 - Cybersecurity and Data Protection," Cen, 2021. https://standards.cen.eu/ (Erişim Haz. 05, 2021).

[12] TSE, "TSE.NET Standard Detayı TS EN ISO/IEC 27001:2017,"2018.https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073083043047076078043057108043104101 (Erişim Haz. 05, 2021).

[13] National Archives, "About CUI." https://www.archives.gov/cui/about (Erişim Haz. 06, 2021).

[14] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five," International Journal of Electrical & Computer Sciences IJECS-IJENS, 2011.

[15] OUSD(A&S), "CMMC Home Page."https://www.acq.osd.mil/cmmc/index.html (Erişim Haz. 06, 2021).

[16] Deparmant of Defense, "DFARS Case 2019-D041," Federal Register, vol. 29/09/2020, pp. 61505–61522, 2020.
[17] ISO, "ISO Management System Standards."https://www.iso.org/management-system-standards.html (Erişim Haz. 05, 2021).
[18] TSE, "TS EN ISO/IEC 27001." TSE, Ankara, 2018.
[19] ISO, "ISO/IEC 27002." ISO, 2013.
[20] OUSD(A&S), "CMMC Model and Assessment Guides." 2020.
[21] X. Meng, M. Sun, and M. Jones, "Maturity Model for Supply Chain Relationships in Construction," Journal of Management in Engineering, vol. 27, no. 2, pp. 97–105, Apr. 2011, doi: 10.1061/(asce)me.1943-5479.0000035.
[22] OUSD(A&S), "CMMC v1.02 Model Main Document." OUSD(A&S), 2020.
[23] ISO,"Certification."https://www.iso.org/certification.html (Erişim Haz. 06, 2021).
[24] CMMC-AB, "CMMC-AB Home Page." https://cmmcab.org/ (Erişim Haz. 12, 2021).
[25] National Archives, "FCI and CUI, what is the difference?," 2020. https://isoo.blogs.archives.gov/2020/06/19/fci-and-cui-what-is-the-difference/ (Erişim Haz. 06, 2021).
[26] Shawn Hays, "What is FCI? and How to Meet CMMC Level 1?" https://info.summit7.us/blog/fci (Erişim Ara. 06, 2021).
[27] North Carolina Interagency Cybersecurity Coordinating Committee (I3C), "FCI/CUI." https://www.cybernc.us/fci-cui/ (Erişim Ara. 06, 2021).
[28] CISA, "Secure High Value Assets." https://www.cisa.gov/publication/secure-high-value-assets (Erişim Ara. 06, 2021).
[29] OUSD(A&S), "CMMC Appendices v1.02." 2020.
[30] TSE, "TS EN ISO/IEC 27002." 2017.
[31] E. Ersoy and M. Alkan, "Bilgi Güvenliğinin Kurumsal Bazda Uygulanması," Bilgi Güvenliği ve Kriptoloji Konferansı, vol. Ankara, no. 13-14 Aralık 2007, pp. 200–207, 2007.