DOI: dpcram24-03-tr

Dijital Koruma Koalisyonu Hızlı Değerlendirme Modeli (DPC RAM)

İçindekiler

Düzenleme Geçmişi

Versiyon	Tarih	Notlar
1	1 Eylül 2019	DPC RAM'ın duyurulması
2	31 Mart 2021	Geri bildirimler neticesinde DPC RAM'ın gözden geçirilmesi
3	Ocak-Mart 2022	Türkçe'ye çevrildi
4	22 Mart 2024	Geri bildirimler neticesinde DPC RAM'ın gözden geçirilmesi (Versiyon 3)
5	6 Ocak 2025	Versiyon 3, Türkçe'ye çevrildi

Kısaltma Listesi

AOR: Assessing Organizational Readiness (Kurumsal Hazıroluşluk Değerlendirme Seti)
DPC: Digital Preservation Coalition (Dijital Koruma Koalisyonu)
DPCMM: Digital Preservation Capability Maturity Model (Dijital Koruma Yetenek Olgunluk Modeli)
GLAM: Galleries, Libraries, Archives and Museums (Galeriler, Kütüphaneler, Arşivler ve Müzeler)
ISO: International Organization for Standardization (Uluslararası Standartlar Teşkilatı)
IT: Information Technology (Bilgi Teknolojileri)
RAM: Rapid Assessment Model (Hızlı Değerlendirme Modeli)
NDSA: National Digital Stewardship Alliance (Ulusal Dijital Savunuculuk Birliği)

Genel Bakış

Dijital Koruma Koalisyonu Hızlı Değerlendirme Modeli, bir kurumun dijital koruma yeteneğinin hızlı bir şekilde değerlendirilmesini sağlarken geliştirilen çözüm ve stratejilere karşı bilinmezlik içerisinde kalınmaması için tasarlanmış bir olgunluk modelleme aracıdır. Model, yalın ve tutarlı olgunluk seviyelerine göre sınıflandırılmış olan bir dizi idari ve hizmet düzeyinde yetenekler sunar. Böylece kurumların koruma yetenekleri ve altyapılarını geliştirip iyileştirirken ilerlemelerini takip etmelerini ve gelecekteki olgunluk hedeflerini belirlemelerini sağlar.

Dijital koruma, gerek duyulduğu süre boyunca dijital malzemelere sürekli erişim için ihtiyaç duyulan yönetilebilir etkinlikler dizisi olarak tanımlanır. Dijital malzemenin bulunduğu ortamın bozulması veya teknolojik ve kurumsal değişim gibi sınırlılıkların ötesinde dijital malzemelere erişimi sürdürmek için gerekli olan tüm eylemleri ifade eder[1].

Model, kullanım için herkesin erişimine ücretsiz olarak açıktır. Ancak, DPC üyelerine tecrübelerini paylaşma ve ilerlemelerini diğer üyelerle karşılaştırma fırsatı da sunulmaktadır. Bu süreç, aynı

[1] Tanım, Dijital Koruma El Kitabı'ndan uyarlanmıştır: https://www.dpconline.org/handbook/glossary#D

zamanda DPC çalışanlarına üyelerin ihtiyaçları ve sorunları hakkında bilgi elde etmeye yönelik verimli, sürekli ve standartlaştırılmış bir yaklaşım sağlayarak DPC Üye Destekleme etkinliklerinin kolaylaşmasına yardımcı olacaktır.

Başlangıç ve Teşekkür

Model, mevcut olgunluk modellerinden yararlanmakta ve esasında Adrian Brown'un Dijital Koruma Olgunluk Modeli'ne dayanmaktadır[2]. Bununla birlikte, Ulusal Dijital Savunuculuk Birliği (National Digital Stewardship Alliance - NDSA) Koruma Düzeyleri[3], Dijital Koruma Yetenek Olgunluk Modeli (Digital Preservation Capability Maturity Model - DPCMM)[4], Kurumsal Hazıroluşluk Değerlendirme Seti (Assessing Organizational Readiness - AOR) ve CoreTrustSeal[5]'dan da yararlanılmıştır. Bu çalışmaların zenginliği, dijital koruma yeteneklerinin değerlendirilmesi için geniş bir kapsama alanı sunarak referans noktaları sağlamıştır. Bunun neticesinde elimizdeki Hızlı Değerlendirme Modeli, Araştırma ve Uygulama Alt Komitesini oluşturanlar da dâhil olmak üzere DPC üyelerinin bildirimleriyle geliştirilip, test edilerek hazırlanmıştır. Bu model için bir başlangıç noktası sağlayıp, ileriye taşınmasındaki desteğinden dolayı Adrian Brown'a özellikle teşekkür ederiz. Bu model üzerindeki ilk çalışma, Nükleer Santral Devre Dışı Bırakma İdaresi tarafından desteklenen ortak bir dijital koruma projesinin parçası olarak gerçekleştirilmiştir.

DPC RAM'ın 2. versiyonu Mart 2021'de yayınlanmıştır. Modeldeki güncellemeler, dijital koruma topluluğunun geri bildirimleri ve bu alandaki iyi uygulama örnekleri ışığında gerçekleştirilmiştir. Hervé L'Hours ve Simon Wilson'a ayrıntılı geri bildirimleri, DPC Araştırma ve Uygulama Alt Komitesi ile Adrian Brown'a önerilen değişiklikleri gözden geçirdikleri için hassaten teşekkür ederiz.

DPC RAM'in üçüncü sürümü Mart 2024'te yayımlanmıştır. Model'de yapılan revizyonlarla bir kez daha topluluktan alınan geri bildirimlere ve iyi dijital koruma uygulamalarının devam eden gelişimine yanıt verilmesi hedeflenmiştir. DPC'nin İyi Uygulamalar Alt Komitesi, önerilen değişiklikler hakkında değerli geri bildirimler sunmuştur. Tui Raven, Kirsten Thorpe, Lauren Booker ve Sharon Webb'in de aralarında bulunduğu bir dizi uzmana RAM'de yapılan etik meselerle ilgili değişikliklere yönelik geri bildirimleri için teşekkürlerimizi iletiriz.

Çeviri Notu

DPC RAM, İngilizce aslından Türkçe'ye Dr. Özhan Sağlık (Bursa Uludağ Üniversitesi Prof. Dr. Fuat Sezgin Merkez Kütüphanesi) tarafından çevrilmiştir[6].

Yol Gösterici İlkeler

Mevcut olgunluk modelleri belirli koruma yaklaşımlarını öncelemektedir. Örneğin CoreTrustSeal'da veri depoları gibi belirli alanlara öncelik verilmekte, NDSA Koruma Düzeyleri'nde kapsam, teknik

2 Brown, A (2013) Practical Digital Preservation: a how-to guide for organizations of any size, Facet Publishing: London.

3 https://ndsa.org/publications/levels-of-digital-preservation/ Türkçesi için bkz. https://osf.io/fje6v/

4 https://web.archive.org/web/20230309120649/http://www.securelyrooted.com/dpcmm

5 https://www.coretrustseal.org

6 Çeviri, Mustafa Ergül (Koç Üniversitesi Suna Kıraç Kütüphanesi) ve Nathalie Defne Gier (Koç Üniversitesi Anadolu Medeniyetleri Araştırma Merkezi Kütüphanesi) tarafından gözden geçirilmiştir. 2024'e kadar dijitalin Türk Dil Kurumu Sözlüğündeki karşılığı olan sayısal terimi kullanılmaktaydı (Sayısal Koruma Koalisyonu, Sayısal Savunuculuk Birliği gibi). Ancak Türkiye'deki dijital koruma topluluğundan gelen dijital kelimesinin daha yaygın kullanıldığı önerisi üzerine, dijital kavramı tercih edilmiştir.

hususlar gibi dijital korumanın özel bir alt alanıyla sınırlandırılmakta ve DPCMM'de teknolojik göç odaklı yaklaşımlar ve açık dosya formatları gibi hususlar incelenmektedir.

DPC üyeleri, galeri, kütüphane, arşiv ve müze (Galleries, Libraries, Archives and Museums - GLAM) sektöründen finans, bilim, üretim ve ötesine kadar uzanan bir çeşitliliktedir. Hâliyle dijital koruma olgunluklarının kolayca değerlendirilmesi, kıyaslanması ve tezatlıkların tespit edilmesi için Koalisyon üyelerinin hedef, ölçek ve yaklaşımlarından bağımsız olarak farklı türdeki kurumlarda uygulanabilecek bir modelin geliştirilmesine ihtiyaç duyulmuştur. Bunun neticesinde belirlenen olgunluk düzeyleri, iyi uygulama örneklerine dayalıdır ve belli koruma stratejileri ya da yaklaşımlarından bağımsızdır. Kurumlar, nerede bulunduklarını değerlendirmek ve ileride nerede olabilecekleri üzerinde düşünmek için modeli kolaylıkla kullanabilmelidir.

Bu model şunları amaçlamaktadır:

- Sektör ve ölçek ayırt etmeksizin her kurum için uygulanabilir olmak
- Uzun-dönemli koruma değerine sahip her içerik için geçerli olmak
- Belirli bir koruma stratejisi ve çözüm önerisinden bağımsız olmak
- Mevcut iyi uygulama örneklerine dayalı olmak
- Kolayca anlaşılabilir ve hızlıca uygulanabilir olmak

Bu Model Nasıl Kullanılır

Bu model, kurum genelinde asgari çaba ve müzakereyle sıklıkla uygulanabilen süratli ve yalın bir değerlendirme sağlayan hızlı bir kıyaslama aracı olarak kullanılmalıdır[7]. Ancak model, derinlemesine bir değerlendirme sağlayabilecek katı ve kapsamlı hususlar içeren bir sertifika aracı değildir.

Model, dijital korumanın kilit alanlarını kapsayan 11 yetenekten oluşmaktadır. İlk 6'sı bir kurumun dijital koruma faaliyetlerini yönetmek (kaynak bulma, politika oluşturma ve destek gibi) için ne kadar iyi kurulduğunu tanımlayan "Kurumsal yetenekler"dir. Geriye kalan 5 tanesi ise bir kurumda yürürlükte olan koruma süreçlerini (sağlama, bit akışı koruma ve erişim gibi) tanımlayan "Hizmet yetenekleri"dir. Her bir yetenek için kurumlar, kendisini 0 ila 4 arasında bir ölçekte değerlendirmelidir. 0, ilgili alanda vurgulanan konulara ilişkin en düşük farkındalığı; 4 ise kurumun en iyi düzeyde çalıştığını gösterir.

Her ölçüt düzeyi için bir yol gösterici açıklama hazırlanmıştır. 2'den 4'e kadar olan düzeyler için madde işaretli örnek listeleri verilmiştir. Bu listeler, ilgili düzeye ulaşılmadan önce **karşılanması gereken ihtiyaçlar değil, açıklayıcı örnekler** olarak sunulmuştur. Bir RAM değerlendirmesi yapılırken bazı örnekler kurumun kendi bağlamıyla ilgili olmayabilir, ancak kurumları benzer bir RAM seviyesine taşıyacak başka eylemler uygulanabilir. Bu aracı kullanan kurumlar, mevcut yeteneklerine hangi düzeyin uygun olduğunu değerlendirmelidir. Bu değerlendirme, mevcut duruma en yakın olacak şekilde **dürüst ve gerçekçi** bir şekilde yapılmalıdır. Kurum, bir düzeyi kısmen karşıladığını değerlendiriyor ancak bu alanda daha fazla çabanın gösterilmesi gerektiğini düşünüyorsa o düzeyden daha düşük bir puanlama yapılmalıdır. Yarım puan elde edilememektedir.

Bu adımlar sonrasında kurum gelecekte hangi düzeye ulaşmak istediklerine karar vermelidir. Bir hedef düzeyin belirlenmesi, o hedefe ilerleyebilmek için giderilmesi gereken noktalar ve önceliklerin

[7] Ön testler, dijital koruma ve bunun kurumda nasıl uygulanacağını bilen uzman biri tarafından yapılan analiz neticesinde modelin 2 saatten kısa bir süre içerisinde temel bir değerlendirme sunabileceğini göstermektedir. Özellikle birden fazla paydaşa danışılması gibi durumlar söz konusuysa bu süre uzayabilir. Gelecekteki hedef ve önceliklerin belirlenmesi muhtemelen daha uzun bir süreç gerektirecektir.

anlaşılmasını artıracaktır. Kurumların DPC RAM'ın her bölümü için optimum düzeylere ulaşma hususunda çaba göstermesine gerek yoktur. Bazı kurumlar için bir veya birden fazla bölümde temel ya da yönetilebilir düzeyleri hedeflemek daha uygun olabilir. Gerçekçi ve kurumsal kaynağın ve önceliklerin açıkça anlaşılması üzerine belirlenen hedeften en üst düzeyde yarar sağlanır. Bundan dolayı, hedeflenen düzeylere ulaşmak için bir zaman tayin edilmelidir. Mesela bazı kurumlar için gelecek 12 ay içerisinde tamamlanacak kısa vadeli hedefler daha uygunken, bazıları beş ya da on yıllık zaman dilimi içerisinde nerede olmak istediklerini değerlendirmeyi daha faydalı bulabilir.

DPC RAM'in özünde sürekli iyileştirme vardır. Bu nedenle RAM'ı tek seferlik bir uygulama olarak görmek mümkün olsa da ilerlemeyi vurgulamak veya daha fazla kaynağa ihtiyaç duyulduğunu göstermek için daha düzenli bir şekilde kullanılmalıdır.

Kurumların olgunluk seviyelerini diğer bağlamsal bilgilerle birlikte kaydetmelerini sağlayan bir Excel tablosu mevcuttur[8]. Bu tablo, aynı zamanda sonuçların basit görselleştirmelerini de oluşturmaktadır. Ayrıca, RAM sonuçlarını kaydetmek için temel bir çalışma sayfası bu belgenin sonunda bulunabilir.

Modelin kullanımı hakkında daha fazla bilgi DPC RAM web sitesinde bulunabilir. Özellikle, "DPC RAM ile Seviye Atlama" her bir RAM yeteneği ile ilerlemeye yönelik ipuçları, faydalı kaynaklar ve vaka çalışmaları yer almaktadır[9].

Faydalar

Bu modeli uygulayan kurum, bu modelle zaman içerisinde yetenekleri ve olgunlukları hakkında kanıta dayalı veri üretebilecekken aşağıdaki gibi sorulara da cevap verebilecektir:

- Kurumumuz nerede?
- Kurumumuzun dijital koruma yeteneklerinde geliştirilmesi gereken yerler mevcut mudur?
- Gelecekte nerede olmak istiyoruz?
- Kurumumuz ulaşmak istediği dijital koruma olgunluk düzeyine ne kadar yakın?
- Kurumumuzun dijital koruma yeteneklerini geliştirmek için önceliklerimiz neler olmalı?
- Kurumumuzun ilerlemesine yardımcı olmak için hangi destek ve kaynaklara ihtiyaç var?
- Kurumun yetenekleri zaman içerisinde nasıl gelişti?

DPC Üyeleri için Faydalar

DPC üyeleri, temel olarak DPC RAM'dan şu hususlar bakımından yararlanabilir:

- Mevcut yeteneklerin hızlıca değerlendirilmesi ve desteğe en çok ihtiyaç duyulan alanların belirlenmesini mümkün kılarak tam üyeler için üye destekleme etkinliklerini hedeflemek.
- Kurumların durumlarını, DPC üyeleri veya DPC üyesi benzer kurumlardaki sonuçlarla karşılaştırmasını mümkün kılarak olgunluk düzeyleri hakkında bilgi paylaşımını kolaylaştırmak.
- DPC'nin üyeliklerini bir bütün olarak daha iyi anlamasına yardımcı olmak ve ortaya çıkan bu bilgiyi üyelik öncelikleri doğrultusunda devam eden araştırma, eğitim ve kaynak geliştirme programlarını şekillendirmek için kullanmak.

8 Bu Excel tablosu, DPC RAM websitesi üzerinden indirilebilir. Türkçe'ye de çevrilen bu Excel dosyası, DPC RAM websitesinden indirilebilir. (ç.n.) https://www.dpconline.org/digipres/implement-digipres/dpc-ram

9 https://www.dpconline.org/digipres/implement-digipres/dpc-ram/level-up

DPC, üyelerini RAM olgunluk seviyelerini yıllık olarak paylaşmaya teşvik edecektir. DPC üyelerin anonimliğini koruyarak bu bilgileri harmanlayıp analiz edecek, eğilimleri ve örüntüleri üyelere raporlayacaktır. Bu model, DPC çalışanları ve Koalisyon üyeleri arasındaki etkileşimleri daha da artıracak ve üye destekleme faaliyetlerinde önemli bir araç olacaktır.

Bir önceki bölümde listelenen ve tüm taraflar için geçerli olan faydalara ek olarak DPC RAM, DPC üyelerinin şu soruları cevaplandırmasını mümkün kılacaktır:

- Kurumumun dijital koruma olgunluğu, DPC üyeleriyle nasıl karşılaştırılabilir?
- Kurumumun dijital koruma olgunluğu, DPC'deki benzer üyelerle nasıl karşılaştırılabilir?
- DPC desteğinden en çok hangi noktada faydalanabiliriz?
- İlerleyebilmek için hangi DPC kaynaklarına ihtiyacımız var?

Terimler

"Dijital Arşiv" kavramı, DPC RAM'da kalıcı değeri olan dijital formdaki bir içeriğin uzun vadeli koruma için saklandığı ve yönetildiği bir tesisi ifade eder.

Kurum (organizasyon)[10] terimi ise, analiz yapılan her bir idari birim anlamında kullanılmaktadır. Bu birim, alışageldiğimiz gibi bir organizasyonda dijital içeriği yönetmek ve korumakla görevli olabileceği gibi, bazı durumlarda kurumun tamamını da kapsayabilir. Bu modeli kullanan her kuruluş, öncelikle kurumlarının hangi bölümlerini analiz edeceğine karar vermelidir. Burada tek bir doğru yaklaşım yoktur ve modelin kullanıcıları kendi ihtiyaçlarını en iyi karşılayabilecek şekilde kurumsal kapsamlarını belirlemeye teşvik edilmektedir.

Kapsam Notu

Bu model, özellikle bilgi teknolojileriyle ilgili (BT - Information Technology [IT]) güvenlik hususlarını hariç tutmaktadır. Bu hususlar, yetenek ve tutarlılık açısından oldukça önemli görülse de, mevcut BT güvenlik rehberliği tarafından iyi hizmet verilen bir alandır (bkz. ISO/IEC 27000 ailesi standartları[11]). Aynı zamanda söz konusu hususlara göre yapılacak değerlendirme sonuçlarının hassas veya gizli bilgi içerebileceği değerlendirilmiştir.

Yorumlar, Geri Bildirimler ve Düzeltmeler

Her ne kadar pek çok kuruluşta dijital koruma faaliyetleri, yaklaşık 20 yıldır yürütülüyor olsa da bu disiplin bir bütün olarak dış etkenler ve yeni gelişmeler karşısında değişimini ve ilerlemesini sürdürecektir. Yeni çözümler, çalışma biçimleri ve iyi uygulama örnekleri ortaya çıkacaktır. Bu modelin ilerlemeyi gösterebilmek açısından yararlı olması için olgunluk düzeylerinin her birinin temel dayanağının aynı kalacağı tahmin edilmektedir. Ancak her bölümdeki örnekler, sahadaki gelişmeler ve DPC üyeleriyle dijital koruma topluluğundan gelen geri bildirimler neticesinde zaman içerisinde güncellenebilir ve geliştirilebilir. Güncellemeler ya da eklemeler için bir öneriniz varsa lütfen DPC ile iletişime geçiniz[12].

10 DPC RAM'ın Türkçe çevirisinde kurum, kuruluş ve organizasyon aynı anlamlarda kullanılmaktadır (ç.n.)

11 https://www.iso.org/isoiec-27001-information-security.html

12 https://www.dpconline.org/about/contact-us

DOI: dpcram24-03-tr

Model

Kurumsal yetenekler		
A	Kurumsal uygulanabilirlik	Dijital koruma faaliyetlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması.
B	Politika ve strateji	Dijital arşivin işleyişi ve yönetimini yönlendiren politikalar, stratejiler ve prosedürler.
C	Yasal ve etik	Dijital içeriğin sağlanması, korunması ve erişimiyle ilgili yasal, toplumsal ve kültürel hak ve sorumlulukların ilgili mevzuat ve etik kurallara uyumlu olarak yönetilmesi.
D	Bilgi İşlem yeteneği	Dijital koruma faaliyetlerini desteklemek için bilgi teknolojileri yetenekleri.
E	Sürekli iyileştirmeler	Mevcut dijital koruma yeteneklerinin değerlendirilmesi, hedeflerin belirlenmesi ve ilerlemenin takip edilmesine yönelik süreçler.
F	Topluluk	Dijital koruma topluluğuyla daha geniş etkileşim ve katkı.
Hizmet yetenekleri		
G	Sağlama, transfer ve sisteme dâhil etme	İçeriğin sağlanması ya da transferi ve dijital arşive dâhil edilmesine yönelik süreçler.
H	Bit akışının korunması	Korunacak dijital içeriğin depolanması ve bütünlüğünün sağlanmasına yönelik süreçler.
I	İçeriğin korunması	Zaman içerisinde dijital içeriğin muhteviyatı, kullanılabilirliği ve işlevselliğini korumaya yönelik süreçler.
J	Üstveri yönetimi	Arşivlenen dijital içeriğin, koruma, keşif ve kullanımına ilişkin yeterli üstverinin üretilmesi ve muhafazasına yönelik süreçler.
K	Keşif ve erişim	Dijital içeriğin keşfini mümkün kılmak ve kullanıcıların erişimini sağlamaya yönelik süreçler.

DOI: dpcram24-03-tr

Kurumsal yetenekler

A - Kurumsal uygulanabilirlik Dijital koruma faaliyetlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması.	
0 - Düşük farkındalık	Kurum, dijital koruma faaliyetlerinin desteklenmesi ihtiyacı konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, dijital koruma faaliyetlerinin desteklenmesi ihtiyacının farkındadır.
2 – Temel	Dijital koruma faaliyetleri, kurum içerisinde temel düzeyde desteklenir ve kaynak sağlanır. Örneğin: ● Üst yönetimin kısmi katılımı vardır. ● Personele sorumluluklar tanınmış ve bunları gerçekleştirebilmeleri bir zaman kararlaştırılmıştır. ● Zaman sınırlı olabilse de dijital koruma için bir bütçe ayrılmıştır. ● Personel gelişim gereksinimleri belirlenmiştir.
3 – Yönetilebilir	Kurumda dijital koruma faaliyetleri yönetilir ve desteklenir. Örneğin: ● Üst yönetimin kararlılığı vardır. ● Dijital koruma için sorumluluklar açıkça tevdi edilmiştir. ● Personel dijital koruma faaliyetlerini yürütmek için ihtiyaç duyduğu becerilere sahiptir ve gerektiğinde ilgili uzmanlığa erişebilir. ● Dijital koruma için özel bir bütçe tahsis edilmiştir. ● Bütçeler, personel rolleri ve geliştirmeler düzenli olarak değerlendirilir. ● Raporlama, planlama ve yönetime yardımcı olmak için dijital arşivle ilgili analizler ve raporlar hazırlanabilir. ● Personel gelişim gereksinimleri için yeterli kaynak ayrılır. ● Dijital koruma, stratejik bir öncelik olarak belirlenmiştir.
4 – Optimum	Dijital koruma faaliyetleri kurumda proaktif olarak yönetilir, iyileştirilir ve geliştirilir. ● Dijital korumanın faydaları bilinir, desteklenir ve kurum geneline yayılmıştır. ● Birimler arasında bir dijital koruma paydaş grubu kurulmuştur. ● Bir ya da daha fazla personelin alanında uzman olması beklenir. ● Bütçeler, personel rolleri, kapasite ve gelişim ihtiyaçları gelecekteki değişikliklere karşı proaktif olarak değerlendirilir. ● Proaktif olarak raporlama, planlama ve yönetime yardımcı olmak için dijital arşivle ilgili analiz ve raporlar, gelecekteki ihtiyaçlara yönelik tahminlerle ilişkilendirilir. ● Personel gelişiminin etkinliği düzenli olarak takip edilir.

	● Kurumun dijital koruma faaliyetlerini gerçekleştirememesi durumunda malzemelerin sürekli korunmasını sağlamak için süreklilik ve haleflik (devir) planlaması[13] mevcuttur.

B - Politika ve strateji Dijital arşivin işleyişi ve yönetimini yönlendiren politikalar, stratejiler ve prosedürler.	
0 - Düşük farkındalık	Kurum, dijital koruma için çerçeve bir politika ihtiyacı konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, çerçeve bir politikanın geliştirilmesi ihtiyacının farkında olup bununla ilişkili politikalara sahiptir. Ancak, kurumda dijital koruma politika ya da stratejisi mevcut değildir.
2 – Temel	Kurumun temel bir çerçeve politikası mevcuttur. Örneğin: ● Üst düzeyde bir dijital koruma politikası ya da stratejisi bulunur. ● Dijital korumayla ilgili başka politikalar mevcut olsa da kapsamında boşluklar bulunabilir. ● Dijital içeriği yönetmek ve erişimi sağlamak için prosedürler uygulanmaktadır ve bunlar dokümante edilebilir. ● Koleksiyonun kapsamı tanımlanmış ve anlaşılmıştır (Örnek: Koleksiyon geliştirme politikası, saklama planı gibi). ● Politika ve prosedürün geliştirilmesinde temel kullanıcı ihtiyaçlarının anlaşılmasına dikkat edilir.
3 – Yönetilebilir	Kurumda kapsamlı ve yönetilebilir politikalar, stratejiler ve prosedürler mevcuttur. Örneğin: ● Dijital koruma politikası/stratejisi diğer kurumsal politikalarla ilişkilidir ve kararlaştırılan takvime göre gözden geçirilir. ● İlgili etik hususlar (çevresel etki, eşitlilik ve çeşitlilik, mahremiyet, kültürel kurallar gibi) tanımlanarak politika ve prosedürlerde açıklanır. ● Dijital arşivdeki içeriği yönetmek ve erişim sağlamak için dokümante edilmiş süreçler ve prosedürler bulunur. ● İlgili tüm personel, dijital koruma politikaları, stratejileri ve prosedürleri hakkında bilgi sahibidir. ● İçeriğin mevcut kullanımı ve kullanımla ilgili gelecek tahminleri, derleme, koruma yaklaşımları, üstveri ve erişim gibi politika ve prosedürlerin geliştirilmesine yardımcı olur.

[13] Haleflik (devir) planı, kurum faaliyetlerini sonlandırdığı takdirde hangi kuruluşlara nasıl devredileceğini içerir.

4 – Optimum	Kurum, proaktif olarak politika, strateji ve prosedürlerini yönetir ve süreç iyileştirmelerinin sürekliliğini taahhüt eder. Örneğin: ● Dijital içeriğin korunması ve erişimiyle ilgili politikalar, stratejiler ve prosedürler eksiksiz bir şekilde mevcuttur. ● Politika ve strateji tam olarak uygulanır ve personel bununla etkin bir biçimde ilgilenir. ● Politika, strateji ve prosedürler, iç ve diğer politikalardaki değişikliklere, kullanıcı ihtiyaçlarına veya diğer dış etkenlere karşı cevap verebilmek için proaktif olarak izlenir ve güncellenir. ● İçeriğin sahipliği ya da aidiyet zincirinin sorgulanması gibi durumlar karşısında değerlendirme, planlama ve içeriği iade etme için bir süreç oluşturulmuştur.

C - Yasal ve etik Dijital içeriğin sağlanması, korunması ve erişimiyle ilgili yasal, toplumsal ve kültürel hak ve sorumlulukların ilgili mevzuat ve etik kurallara uyumlu olarak yönetilmesi.	
0 - Düşük farkındalık	Kurum, yasal, toplumsal, kültürel ve etik hak ve sorumlulukların yönetilmesine yönelik temel ilkelerle ilgili ihtiyaçlar konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, yasal, toplumsal, kültürel ve etik hak ve sorumlulukların yönetilmesiyle ilgili ihtiyaçlar konusunda farkındalığa sahiptir.
2 – Temel	Dijital içerikle ilgili yasal, toplumsal, kültürel ve etik haklar ve sorumlulukların yönetiminde temel hususlar gerçekleştirilir. Örneğin: ● Yasal, toplumsal, kültürel ve etik haklar ve sorumluluklarla ilgili taraflar tanımlanır ve kayıt altına alınır (Yerli halkların hakları veya topluluk sahipliği gibi). ● Gerekli yasal anlaşma ve sözleşme taslakları mevcuttur. ● Mesleki etik kurallarına bağlı kalınır.
3 – Yönetilebilir	Dijital içerikle ilgili yasal, toplumsal, kültürel ve etik hak ve sorumluluklar yönetilebilir. Örneğin:

	● Lisanslama, yasal haklar ve sözleşmelerle ilgili bilgiler gerektiğinde kolayca bulunabilir ve erişilebilir. ● Yasal ve etik sorunlar ve riskler yönetilerek düzenli aralıklarla gözden geçirilir. ● Yasal ve etik sorunlar ve risklerin yönetimiyle ilgili yetkiler ve sorumluluklar açıkça belirlenmiştir. ● Gerek duyulduğunda hukuk, etik meseleler, satın alma, sözleşme yönetimi veya bilgi edinme uyumluluğu[14] gibi uzman görüşüne başvurulabilir. ● Yasal ve etik haklar ve sorumluluklarla ilgili gerçekleştirilen faaliyetlerin dokümantasyonu yapılır. ● Farklı yasal, etik ya da mevzuatsal gereksinimlerin söz konusu olduğu içerikler için ayrı koruma ve erişim iş akışları mevcuttur. ● İçerik, yürürlükteki mevzuata uygun olarak engelli kullanıcılar için erişilebililirdir.
4 – Optimum	Dijital içerikle ilgili yasal, toplumsal, kültürel ve etik haklar ve sorumluluklar proaktif olarak yönetilir. Örneğin: ● Yasal ve etik sorunlar ve riskler proaktif olarak izlenir ve hafifletilir. ● Kurum, etik sorumluluklar ve/veya düzenleme oluşturan yasal ve adli süreçlerle ilgili diyalog kurar. ● Yerli halkların veya topluluklara ait içeriğin emanetçileriyle güvenilir ve işbirlikçi ilişkiler tesis edilir. ● Çevresel sürdürülebilirlik, yerli halkların veri hâkimiyeti, eşitlik ve çeşitlilik gibi kritik etik meselelerin ele alınması için uygun bir forum oluşturulur.

D - Bilgi İşlem yeteneği Dijital koruma faaliyetlerini desteklemek için bilgi teknolojileri yetenekleri.	
0 - Düşük farkındalık	Kurum, dijital arşivi destekleyecek bilgi işlem yeteneğine duyulan ihtiyaç veya bu yeteneğin uygulanmasına yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, dijital arşivi destekleyecek bilgi işlem yeteneğine duyulan ihtiyacın farkındadır ve bu yeteneğe yönelik temel ilkeleri anlamıştır.
2 – Temel	Kurum, teknik altyapı ve destek gibi temel bilgi işlem faaliyetlerine ulaşabilir. Örneğin: ● Dijital arşiv için temel seviyede bilgi işlem desteği mevcuttur. ● Bilgi işlem faaliyetlerinden sorumlu olan çalışan, dijital korumayı desteklemedeki rolü konusunda temel bilgiye sahiptir. ● Bilgi işlem sistemleri, temel düzeyde dokümante edilir.
3 – Yönetilebilir	Kurum, kapsamlı bir şekilde yönetilen teknik altyapı ve destek gibi temel bilgi işlem faaliyetlerine ulaşabilir. Örneğin:

14 Information compliance olarak geçen kavram, bilgi edinme hakkı ve kişisel verilerin korunması gibi yasal süreçlerle ilgilidir. Daha sarih bir ifade olabileceği düşüncesiyle söz konusu kavram, bilgi edinme uyumluluğu olarak kullanılmıştır. (ç.n.)

	● Dijital arşiv için yeterli bilgi işlem desteği mevcuttur. ● Dijital korumayla ilgili bilgi işlem rol ve sorumlulukları dokümante edilerek düzenli aralıklarla gözden geçirilir. ● Bilgi işlem sistemleri düzenli aralıklarla bakıma alınır ve güncellenir. ● Gerek duyulduğunda yeni araçlar ve sistemler kullanılır. ● Bilgi işlem sistemlerinin dokümantasyonu kapsamlı bir şekilde yapılır. ● Bulut bilişim gibi üçüncü taraf hizmet sağlayıcılarla yapılan anlaşmalar ve hizmet alımları iyi yönetilerek dokümante edilir.
4 – Optimum	Kurum, sürekli olarak ilerleyen ve gelişen, proaktif olarak yönetilen bilgi işlem faaliyetlerine ulaşabilir. Örneğin: ● Dijital arşiv için iyi seviyede bir bilgi işlem desteği mevcuttur. ● Bilgi işlem, dijital korumayla ilgili konulara hâkimdir ve bunlarla etkileşim içerisindedir. ● Bilgi işlem sistemlerinin geleceğe yönelik iyileştirmeleri için ayrıntılı bir yol haritası mevcuttur. ● Muhtemel yeni araçlar ve sistemler proaktif olarak belirlenir ve test edilir. ● Dijital koruma gereklilikleri, uzun dönem saklanması gereken belgeler içeren gibi diğer bilgi işlem sistemleri tedarik edilirken dikkate alınır.

E - Sürekli iyileştirmeler Mevcut dijital koruma yeteneklerinin değerlendirilmesi, hedeflerin belirlenmesi ve ilerlemenin takip edilmesine yönelik süreçler.	
0 - Düşük farkındalık	Kurum, mevcut yetenekler veya hedefler hakkında düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, mevcut yetenekleri anlama ve hedefleri belirleme ihtiyacı konusunda farkındalığa sahiptir.
2 – Temel	Kurum, mevcut dijital koruma yetenekleri ve geliştirilecek alanlar konusunda temel bir anlayışa sahiptir. Örneğin: ● Bir yetenek değerlendirmesi yapılmıştır. ● Dijital koruma yetenekleri konusunda geliştirilmesi gereken hususlar belirlenmiştir.
3 – Yönetilebilir	Kurum, yetenek değerlendirme ve hedefleri belirleme konusunda yönetilebilir süreçlere sahiptir. Örneğin: ● Hedefler kararlaştırılmış ve üst yöneticiler tarafından onaylanmıştır. ● Hedeflere ulaşmak için yol haritası hazırlanmıştır. ● Yetenek değerlendirmeleri belirli aralıklarla tekrarlanır. ● Yetenek değerlendirmeleri meslektaşlarla paylaşılır. ● Kurum, diğerlerine göre nerede olduğuna dair bir anlayışa sahiptir.
4 – Optimum	Kurum, proaktif yönetim biçimiyle süreç iyileştirmeyi sürekli kılar. Örneğin: ● Kurum genelindeki ilgili paydaşlar yetenek değerlendirmesine katılır ve sonraki adımlar için plan yapar.

	● Sertifikasyon/dış değerlendirme ihtiyacı tanımlandıysa bu gerçekleştirilmiştir. ● İyileştirme önerileri dikkate alınarak uygulanmıştır. ● Hedefler ve yol haritası belirli aralıklara gözden geçirilir.

F - Topluluk Dijital koruma topluluğuyla daha geniş katılım ve katkı.	
0 - Düşük farkındalık	Kurum, dijital koruma topluluğuyla daha geniş bir katılım konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, dijital koruma topluluğuyla daha geniş bir işbirliği yapmanın faydaları konusunda farkındalığa sahiptir.
2 – Temel	Kurum, daha geniş bir biçimde dijital koruma topluluğuyla temel düzeyde ilişki kurar. Örneğin: ● İlgililerle bir ağ kurulmuştur. ● İlgili toplulukların etkinliklerine iştirak edilir. ● Başkalarının tecrübelerinden faydalanmak için çaba gösterilir.
3 – Yönetilebilir	Dijital koruma topluluğuyla daha geniş bir ilişki kurulması desteklenerek bu ilişki yönetilir. Örneğin: ● İlgili ağlar ve topluluklar davet edilir. ● Dijital koruma topluluğunda daha etkin bir rol üstlenilir. ● Gerektiğinde dijital koruma konusunda uzman görüşüne başvurulur. ● Kendi iş süreçlerinden elde ettiği başarı ve çıkarılan dersler toplulukla paylaşılır. ● Dijital koruma topluluğu ile etkileşim yönetim tarafından desteklenerek teşvik edilir ve bu süreç, politika veya stratejilere dâhil edilir.
4 – Optimum	Kurum, dijital koruma topluluğunda liderlik rolü üstlenir ve bu katılımı proaktif bir şekilde yönetir. Örneğin: ● Topluluk üyeleri arasında işbirliği, ortak faaliyetler veya etkinlikler düzenlenmesinde proaktif bir rol alır. ● Uzman grupları, komiteler veya çalışma gruplarına katkıda bulunulur.

DOI: dpcram24-03-tr

Hizmet yetenekleri

G - Sağlama, transfer ve sisteme dâhil etme İçeriğin sağlanması ya da transferi ve dijital arşive dâhil edilmesine yönelik süreçler.	
0 - Düşük farkındalık	Kurum, dijital arşive içerik sağlamak ya da transfer etmek ihtiyacı ile bunu gerçekleştirmeye yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurumun dijital arşive dijital bir içeriği sağlamak veya transfer etmek ihtiyacı konusunda farkındalığı ve bu içeriği sisteme dâhil ederken uygulanacak temel ilkeler konusunda bilgisi vardır.
2 – Temel	Kurum, sağlama, transfer ve sisteme dâhil etme için temel süreçleri uygulamaya almıştır. Örneğin: ● Sisteme dâhil etme süreci dokümante edilmektedir. ● Gerektiğinde bağışçılar, belge sahipleri ve üreticileri için temel bir kılavuz mevcuttur. ● Dokümantasyon ve üstveriler çoğu zaman sağlama veya transfer sürecinin bir parçası olarak alınır veya kaydedilir. ● Gerektiğinde dijital içeriğin seçimi ve kaydedilmesine ilişkin süreç belgelenebilir (örneğin web ve e-posta arşivleri, dijitalleştirilmiş içerikler, EBYS'deki belgeler). ● Bazı içerik, dijital koruma politikalarıyla uyumlu olarak elle işletilen (manuel) bir süreç kapsamında değerlendirilebilir. ● Virüs kontrolü ve dosya tanımlama gibi sisteme dâhil etme ve öncesindeki faaliyetler için fiziki ya da sanal farketmeksizin bir çalışma alanı mevcuttur.
3 – Yönetilebilir	Kurum, sağlama, transfer ve sisteme dâhil etme için kapsamlı ve yönetilebilir süreçleri uygulamaya almıştır. Örneğin: ● Gerektiğinde bağışçılar, saklama hizmeti sunanlar, belge sahipleri, veri özneleri ve belge üreticileriyle ilişkiler sürekli iletişim, rehberlik ve destek verme aracılığıyla yürütülür. ● Değerlendirme, sisteme dâhil etme iş akışının standart bir parçasıdır. ● İş akışları verimli ve amaçlarla uyumludur. ● Sisteme dâhil etme sürecinin parçaları otomatikleştirilmiştir. ● İçeriğin başarıyla transferi, bütünlük kontrolüyle doğrulanır.
4 – Optimum	Kurum, sağlama, transfer ve sisteme dâhil etme sürecini proaktif olarak yönetir ve geliştirir. Örneğin: ● Kurum, muhtemel bağışçılar, saklama hizmeti sunanlar, belge sahipleri, veri özneleri ve belge üreticileriyle malzemelerin

	optimum yaşam döngüsü yönetimini desteklemek için işbirliği yapar. ● Arşive transfer edilecek dijital içeriği üreterek bünyesinde saklayan kurumdaki bilgi sistemleri, gelecekteki koruma gereksinimlerinin bilinciyle işletilir ve yapılandırılır. ● Sisteme dâhil etme süreci, gerektiğinde el ile işletilmesi mümkün olmak kaydıyla, yararlı görüldüğünde otomatikleştirilir. ● İçeriğin varlık yönetimi veya belge yönetimi sistemlerinden otomatik olarak aktarılmasını sağlamak için entegrasyonlar mevcuttur. ● Hassas bilgiye dikkat çekmek veya değerlendirme kararları hakkında bilgi sunmak gibi süreci otomatikleştirmek ve iyileştirmek için yazılım araçları kullanılır. ● İçeriğin arşivlik değeri, kullanım ölçütleri ve hem mali hem de çevresel olarak koruma maliyetleri gibi etmenler göz önünde bulundurularak belirli aralıklarla yeniden değerlendirirlir.

H - Bit akışının korunması Korunacak dijital içeriğin depolanması ve bütünlüğünün sağlanmasına yönelik süreçler.	
0 - Düşük farkındalık	Kurum, bit akışının korunması ihtiyacı veya bunu gerçekleştirmeye yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurumun bit akışının korunması ihtiyacıyla ilgili farkındalığı ve buna yönelik temel ilkeler hakkında bilgisi vardır.
2 – Temel	Kurum, bit akışının korunması için temel süreçleri uygulamaya almıştır. Örneğin: ● Mevcut koruma ihtiyaçlarını karşılamak için dijital bir depo mevcuttur. ● İçeriğin konumu, kayıt defterine kaydedilmiştir. ● Basit bir yedekleme rejimi, artık veriler sağlar. ● Tüm içerik için sağlama toplamı oluşturulur. ● İçeriğe hangi çalışanın erişim yetkisine sahip olduğu bilinir.

3 – Yönetilebilir	Kurum, içeriğinin replikasyon ve bütünlük kontrollerini en iyi koruma uygulamalarıyla yönetilebilir bir şekilde saklamaktadır. Örneğin: ● İçerik, bir veya daha fazla konumda replikasyon ve bütünlük kontrolünün birleşimiyle yönetilir. ● Depolama risklerini ve kopya sayısı, konum, kullanılan teknolojiler, bütünlük kontrolünün sıklığı gibi uygun önlemleri değerlendirmek için bir risk değerlendirme süreci tesis edilir. ● Depolama mimarisi, siber saldırı, insan hatası, bit bozulması ve doğal veya insan kaynaklı felaketler gibi belirlenen riskleri uygun şekilde azaltmak için tasarlanırken içeriğin değeri, finansal maliyetler ve çevresel etki gibi diğer gereklilikler de dikkate alınır. ● İçeriğin bütünlük kontrolünde karşılaşılan başarısız sonuçlar giderilir. ● Çalışanların içeriğe erişimi için yetkilendirmeler yapılır ve bunlar dokümante edilir. ● Yedeklemeler, replikasyon ve bütünlük kontrolünün etkinliğini teyit etmek için rutin testler gerçekleştirilir. ● Dijital içerik, politika sınırlamalarına, yasal kısıtlamalara ve veri hâkimiyeti gereksinimlerine uygun olacak bir coğrafi konumda depolanır.
4 – Optimum	Kurum, proaktif risk yönetimiyle birlikte iyi derecede yönetilebilir depolama usullerini uygulamaya almıştır. Örneğin: ● Depolama için yapılan risk değerlendirmesi kayıt altına alınır ve düzenli aralıklarla gözden geçirilir. ● Gelecekteki depolama ihtiyaçları, düzenli aralıklarla hesaplanarak güncellenir; buna göre depolama kapasitesi izlenir ve gözden geçirilir. ● İçeriğin bütünlüğü ve bunu sağlamaya yönelik süreçler, bağımsız bir şekilde denetlenir. ● İçeriğe tüm erişimler, log kayıtlarına kaydedilir ve hangi içerik, ne zaman ve kim tarafından erişildi gibi sorular sorularak yetkisiz bir kullanım ve/veya değişimin olup olmadığı kontrol edilir.

I - İçeriğin korunması Dijital içeriğin zaman içerisinde anlamını, kullanılabilirliğini ve işlevselliğini korumaya yönelik süreçler.	
0 - Düşük farkındalık	Kurum, içeriğin korunması ihtiyacı veya bunu gerçekleştirmeye yönelik temel ilkelerin uygulanması konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum içeriğin korunması ihtiyacının farkındadır ve buna yönelik temel ilkeler konusunda bilgisi vardır.
2 – Temel	Kurum, sahip olduğu içeriği anlayabilmek için temel süreçleri uygulamaya almıştır. Örneğin: ● Dosya formatları belirlenmiştir. ● İçerik, şifreleme, bozulmuş ya da eksik içerik ve geçersiz dosyalar gibi nitelik kriterleri ve koruma hususiyetleri açısından değerlendirilmiştir. ● Mevcut ve gelecekteki kullanıcılar ile içeriğin kullanımı hakkında temel bilgi vardır.

3 – Yönetilebilir	Kurum, zaman içerisinde içeriğin anlamı, kullanılabilirliği ve erişilebilirliğinin korunmasını izlemek ve planlamak için yönetilebilir süreçleri uygulamaya almıştır. Örneğin: ● Koruma izleme uygulamaları yapılır ve risk altındaki içerik belirlenir. ● Teknik bağımlılıklar tespit edilir ve kayıt altına alınır. ● İş akışının meydana gelişi ya da kayıt altına alınması için göç ettirme, öykünme ve değiştirme gibi içeriğin korunması ve kalite kontrolüne yönelik faaliyetler zaman zaman gerçekleştirilir. ● Koruma faaliyetleri, mevcut ve gelecekteki kullanımları destekleyecek biçimde dijital malzemelerin özellikleri göz önünde bulundurularak yapılır. ● Ne zaman, ne, nasıl, neden ve kim gibi ayrıntılarla dijital içerikte değişime sebep olan her işlem kayıt altına alınır.
4 – Optimum	Kurum, içeriğin zaman içerisinde anlamı, kullanılabilirliği ve işlevselliğinin korunması için korumayla ilgili riskleri önceliklendirmek ve gidermek için proaktif bir yaklaşım benimser. Örneğin: ● Belirli format ve türdeki içeriğe ilişkin riskler layıkıyla anlaşılmıştır. ● Riskleri hafifletmek için gereken uygun koruma faaliyetleri, titiz bir koruma planlaması neticesinde belirlenmiştir. ● Uygulanacak koruma faaliyetleri, riskler, içeriğin arşivlik değeri, hem mali hem çevresel maliyetler ve kullanım biçimleri dikkate alınarak kararlaştırılır. ● Format göçü, düzeltmeler, öykünme ve diğer dijital koruma faaliyetleri, koruma planlarına uygun olarak gerçekleştirilir. ● Kalite kontrolü, koruma faaliyetleri neticesinde içeriğin anlamını ve/veya işlevselliğini olması gerektiği gibi muhafaza edilmesini sağlamak için yapılır ve kayıt altına alınır. ● Gerektiğinde dijital içerik ve üstverilerin versiyon kontrolü sağlanır.

J - Üstveri yönetimi Arşivlenen dijital içeriğin, koruma, keşif ve kullanımına ilişkin yeterli üstverinin üretilmesi ve muhafazasına yönelik süreçler.	
0 - Düşük farkındalık	Kurum, üstverilerin yönetilmesi ihtiyacı veya bunu gerçekleştirmeye yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, üst verilerin yönetilmesi ihtiyacının farkındadır ve buna yönelik yemel ilkeler konusunda bilgisi vardır.
2 – Temel	Kurum, temel seviyede koruma, keşif ve kullanım için üstveri oluşturur ve bunları muhafaza eder. Örneğin: ● İçerik, bir dijital varlık sisteminde koleksiyon düzeyinde tanımlanmıştır. ● Asgari düzeyde uygun bir tanımlayıcı üstveri koşulu mevcuttur. ● İçerikle birlikte sağlanan üstveriler ve dokümantasyon saklanır ve korunur. ● Temel seviyedeki koruma üstverileri her bir tekil malzeme düzeyinde oluşturulur.

3 – Yönetilebilir	Kurum, koruma, keşif ve kullanım için üstveri oluşturmak ve muhafaza etmek için yönetilebilir süreçleri uygulamaya almıştır. Örneğin: ● Uygun üstveri standartları belirlenmiştir. ● Oluşturulan üstverilerin tutarlılığı için kurum içi kılavuzlar ve kontrollü sözlükler mevcuttur. ● Dijital içerik için kalıcı tek biçim tanımlayıcılar atanmış ve bunlar muhafaza edilmiştir. ● Dijital malzemeyi oluşturan veri ile üstveri elemanları arasındaki yapısal ilişki korunmuştur.
4 – Optimum	Kurum, koruma, keşif ve kullanım için üstverilerin proaktif yönetimini üstlenerek süreçlerin iyileştirilmesi ve geliştirilmesi için yollar arar. Örneğin: ● Mümkün olduğunca dijital içerik için zengin üstveriler bulunur. ● Uygun üstveri standartları kullanılır. ● Belirli aralıklarla üstveri standartları tercihi gözden geçirilir ve değerlendirilir. ● Malzemenin ömrü boyunca üstveriler ve dokümantasyon iyileştirilebilir. ● Üstveriler, kullanıcı için daha zengin bir kullanım deneyimi sunar. ● Üstveriler harmanlanabilir ve tekrar kullanılabilir. ● Yerli halklar veya ötekileştirilmiş topluluklarla ilgili ya da onlara ait olan içeriğin tanımlaması onlarla işbirliği içerisinde yapılır. ● Mevcut koruma stratejisinin yönetimi, standartlaştırılmış içerik paketleri ve üstveriler aracılığıyla kolaylaştırılır.

K - Keşif ve erişim Dijital içeriğin keşfini mümkün kılmak ve kullanıcıların erişimini sağlamaya yönelik süreçler.	
0 - Düşük farkındalık	Kurum, kendi kullanıcı topluluğu için keşif ve erişimi mümkün kılmak veya bunu gerçekleştirmeye yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurumun kendi kullanıcı topluluğu için keşif ve erişimi mümkün kılmakla ilgili farkındalığı ve buna yönelik temel ilkeler konusunda bilgisi vardır.
2 – Temel	Kurum, erişim haklarının izin verdiği ölçüde, temel bir keşif ve erişim mekanizmasını uygulamaya almıştır. Örneğin: ● Bazı dijital içerikler için temel kaynak keşif aracı mevcuttur. ● Kullanıcılar, kurum içinden ya da dışından dijital içerik ve üstverileri görebilir veya erişebilir. ● Kullanıcıların dijital içeriğe erişimi kayıt altına alınır. ● Dijital içeriğin kullanıcılarına destek sunulur. ● Dijital içeriğin erişilebilirliğine ilişkin bilgi, kullanıcılara sunulur.

3 – Yönetilebilir	Kurum, erişim haklarının izin verdiği ölçüde, kapsamlı ve yönetilebilir keşif ve kullanım süreçlerini uygulamaya almıştır. Örneğin: ● Her dijital içerik için temel kaynak keşif aracı mevcuttur. ● Bazı dijital içerikler için tam metin arama imkânı vardır. ● Kullanıcıların erişim hakları görüntülenebilirdir ve uygulanır. ● İçeriğin izin verilen kullanımları hakkında kullanıcılara açık bilgiler sağlanır. ● Kullanıcıların dijital içeriğe erişimiyle ilgili istatistiksel raporlar oluşturulabilir. ● Erişim mekanizmaları, kullanıcı topluluğundan alınan geri bildirimlere göre güncellenir. ● Kaynak keşif bilgisi, engelli kullanıcılar için erişilebilir formatta sunulur. ● Yerli halklar veya diğer topluluklara ait ya da onlarla ilgili olan içeriğe erişim, ilgili toplumsal, yasal ve kültürel kurallar tarafından düzenlenir ve toplulukla istişare edilerek sunulur. ● Hassas veya gizli bilgi içeren dijital içerik, ifşa riski göz önüne alınarak erişime açılır. ● Bir çıkış stratejisi söz konusu olduğunda, her dijital içeriğin toplu olarak sistemin dışına aktarılmasından sonra erişimine yönelik uygulama örnekleri hazırlanmıştır.
4 – Optimum	Kurum, erişim haklarının izin verdiği ölçüde, proaktif olarak iyileştirilen ve geliştirilen ileri düzey keşif ve kullanım süreçlerini uygulamaya almıştır. Örneğin: ● Çok boyutlu arama, veri görselleştirme veya API'ler aracılığıyla erişimi düzenleme gibi ileri düzey kaynak keşif ve erişim araçları sağlanmıştır. ● Göç ettirilmiş, öykünmesi yapılmış ve görselleştirilmiş içerik için erişim, oluşturma veya yeniden kullanma gibi farklı seçenekler bulunur. ● İhtiyaç ve beklentileri karşılamak için proaktif olarak kullanıcı topluluğuna danışılır. ● Dijital içeriği keşfetmek ve erişmek için toplanan bilgi, kullanıcı deneyimini iyileştirme ve geliştirmede kullanılır. ● İçeriğin erişimden kaldırılması taleplerini ele almak için bir süreç mevcuttur. ● Dijital içerik, engelli kullanıcılar için erişilebilir formatlarda erişime sunulur. ● Erişim mekanizmaları, engelli kullanıcılar için genel erişilebilirlik araçlarıyla uyumludur veya birlikte çalışabilir. ● Koleksiyona özel erişim sistemleri, uzun ömürlü olacak şekilde tasarlanmıştır.

DOI: dpcram24-03-tr

Ek I – DPC RAM Analiz Cetveli

Kurum:	
Değerlendirmeyi yapan:	
Değerlendirme tarihi:	
Değerlendirmenin kapsam notları (içeriğin türü veya birim):	
Hedeflenen düzeyler için zaman aralığı (Ör. 1/3/5/10 yıl)	

KURUMSAL YETENEKLER				
	Mevcut Düzey	**Neden bu düzeyi seçtiniz?**	**Hedeflenen Düzey**	**Hedefe ulaşmak için nelerin mevcut olması gerekmektedir?**
A. Kurumsal uygulanabilirlik: Dijital koruma faaliyetlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması.				

B. Politika ve strateji: Dijital arşivin işleyişi ve yönetimini yönlendiren politikalar, stratejiler ve prosedürler.				
	Mevcut Düzey	**Neden bu düzeyi seçtiniz?**	**Hedeflenen Düzey**	**Hedefe ulaşmak için nelerin mevcut olması gerekmektedir?**
C.Yasal ve etik: Dijital içeriğin sağlanması, korunması ve erişimiyle ilgili yasal, toplumsal ve kültürel hak ve sorumlulukların ilgili mevzuat ve etik kurallara uyumlu olarak yönetilmesi.				
D. Bilgi İşlem yeteneği: Dijital koruma faaliyetlerini desteklemek için bilgi teknolojileri kabiliyeti.				

E. Sürekli İyileştirmeler: Mevcut dijital koruma kabiliyetlerinin değerlendirilmesi, hedeflerin belirlenmesi ve ilerlemenin takip edilmesine yönelik süreçler.				
F. Topluluk: Dijital koruma topluluğuyla daha geniş katılım ve katkı.				
HİZMET YETENEKLERİ				
	Mevcut Düzey	**Neden bu düzeyi seçtiniz?**	**Hedeflenen Düzey**	**Hedefe ulaşmak için nelerin mevcut olması gerekmektedir?**
G. Sağlama, Transfer ve Sisteme Dâhil Etme: İçeriğin sağlanması ya da transferi ve bunun dijital arşive dâhil edilmesine yönelik süreçler.				

H. Bit akışının Korunması: Korunacak dijital içeriğin depolanması ve bütünlüğünün sağlanmasına yönelik süreçler.				
I. İçeriğin Korunması: Dijital içeriğin zaman içerisinde anlamını, kullanılabilirliğini ve işlevselliğini korumaya yönelik süreçler.				
	Mevcut Düzey	**Neden bu düzeyi seçtiniz?**	**Hedeflenen Düzey**	**Hedefe ulaşmak için nelerin mevcut olması gerekmektedir?**
J. Üstveri Yönetimi: Arşivlenen dijital içeriğin, koruma, keşif ve kullanımına ilişkin yeterli üstverinin üretilmesi ve muhafazasına yönelik süreçler.				

K. Keşif ve Kullanım: Dijital içeriğin keşfini mümkün kılmak ve kullanıcıların erişimini sağlamaya yönelik süreçler.				