DOI: http://doi.org/10.7207/dpcram22-01

Sayısal Koruma Koalisyonu Hızlı Değerlendirme Modeli (DPC RAM)

İçindekiler

DOI: http://doi.org/10.7207/dpcram22-01

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

Kısaltma Listesi

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

Genel Bakış

Sayısal Koruma Koalisyonu Hızlı Değerlendirme Modeli, bir kurumun sayısal 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.

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

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

DOI: http://doi.org/10.7207/dpcram22-01

Model kullanım için herkesin erişimine ücretsiz olarak açıktır. Ancak, DPC üyelerine tecrübelerini paylaşma ve ilerlemelerini diğer üyelerle karşılaştırma fırsatı da sunulmaktadır. Bu süreç, aynı 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 Sayısal Koruma Olgunluk Modeli'ne dayanmaktadır[2]. Bununla birlikte, Ulusal Sayısal Savunuculuk Birliği (National Digital Stewardship Alliance - NDSA) Koruma Düzeyleri[3], Sayısal 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, sayısal 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 sayısal koruma projesinin parçası olarak gerçekleştirilmiştir.

DPC RAM'ın 2. versiyonu Mart 2021'de yayınlanmıştır. Modeldeki güncellemeler, sayısal 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.

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

---

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

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

4 https://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.

DOI: http://doi.org/10.7207/dpcram22-01

DPC üyeleri, galeri, kütüphane, arşiv ve müze (Galleries, Libraries, Archives and Museums - GLAM) sektöründen finans, bilim, üretim ve ötesine kadar uzanan bir çeşitliliktedir. Hâliyle sayısal 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.

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. 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 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

[7] Ön testler, sayısal 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.

DOI: http://doi.org/10.7207/dpcram22-01

vadeli hedefler daha uygunken, bazıları beş ya da on yıllık zaman dilimi içerisinde nerede olmak istediklerini değerlendirmeyi daha faydalı bulabilir.

Bu modelle birlikte bir analiz cetveli hazırlanmıştır. Bu cetvel, kurumların şu hususları kayıt altına almasına katkıda bulunacaktır:

- Her bir ölçüt için mevcut olgunluk düzeyleri
- Bu düzeyin neden seçildiğine dair notlar/kanıtlar
- Kurumun ulaşmak istediği olgunluk düzeyi
- Özellikle hedef seviyeye ulaşmak için ne yapılması gerektiğine dair notlar

Bu cetvel, çalışmanın sonunda yer almaktadır ve elde edilen sonuçların görselleştirilmiş hâllerini üreten bir Excel dosyası olarak da mevcuttur.[8]

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 sayısal koruma yeteneklerinde geliştirilmesi gereken yerler mevcut mudur?
- Gelecekte nerede olmak istiyoruz?
- Kurumumuz ulaşmak istediği sayısal koruma olgunluk düzeyine ne kadar yakın?
- Kurumumuzun sayısal 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 Türkçe'ye de çevrilen bu Excel dosyası, DPC RAM websitesinden indirilebilir. https://www.dpconline.org/digipres/implement-digipres/dpc-ram (ç.n.)

DOI: http://doi.org/10.7207/dpcram22-01

DPC, üyelerine yıllık olarak olgunluk seviyeleri hakkında bilgi girebilecekleri çevrimiçi bir form sağlayacaktır. Bu form, üyelerin verilerin nasıl kullanılacağı ve paylaşılacağına ilişkin hususları belirlemesine imkân tanır. DPC, kaynaklık etmesi için üyelere cevaplarının bir kopyasını gönderecek, bu bilgileri derleyip analiz edecek ve eğilimler ile modelin kullanım biçimlerini raporlayarak iletecektir. DPC, izin almak kaydıyla DPC üyeleri arasında ilişki kurmak için verileri kullanabilir. Bu model, DPC çalışanları ile Koalisyon üyeleri arasındaki iletişimi destekleyecek ve üye destek faaliyetlerini kolaylaştırmada 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 sayısal koruma olgunluğu, DPC üyeleriyle nasıl karşılaştırılabilir?
- Kurumumun sayısal koruma olgunluğu, DPC'deki benzer üyelerle nasıl karşılaştırılabilir?
- DPC desteğinden en çok hangi noktada faydalanabiliriz?
- İlerleyebilmek için hangi DPC kaynaklarına ihtiyacımız var?

Terimler

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

Kurum (organizasyon)[9] terimi ise, analiz yapılan her bir idari birim anlamında kullanılmaktadır. Bu birim, alışageldiğimiz gibi bir organizasyonda sayısal 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[10]). 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 sayısal 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

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

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

DOI: http://doi.org/10.7207/dpcram22-01

düzeylerinin her birinin temel dayanağının aynı kalacağı tahmin edilmektedir. Ancak her bölümdeki örnekler, sahadaki gelişmeler ve DPC üyeleriyle sayısal koruma topluluğundan gelen geri bildirimler neticesinde zaman içerisinde güncellenebilir ve geliştirilebilir. Güncellemeler ya da eklemeler için bir öneriniz varsa lütfen DPC RAM web sitesindeki geri bildirim formunu doldurun[11].

Model

DPC RAM'ın iki parça hâlinde gruplandırılmış farklı sayısal koruma yeteneklerini kapsayan 11 bölümü bulunmaktadır. Kurumsal yetenekler, kurumsal veya diğer daha uygun yüksek ayrıntı düzeylerinde tanımlanmaktadır. Hizmet yetenekleri ise olası belirli bir içeriğe özgü olmak gibi daha düşük bir ayrıntı düzeyinde değerlendirilebilecek işlevsel düzeyleri ifade etmektedir.

Kurumsal yetenekler		
A	Kurumsal uygulanabilirlik	Sayısal koruma faaliyetlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması.
B	Politika ve strateji	Sayısal arşivin işleyişi ve yönetimini yönlendiren politikalar, stratejiler ve prosedürler.
C	Yasal dayanak	Sayısal içeriğin sağlanması, korunması ve erişimiyle ilgili yasal hak ve sorumlulukların ilgili mevzuat ve etik kodlara uyumlu olarak yönetilmesi.
D	Bilgi İşlem yeteneği	Sayısal koruma faaliyetlerini desteklemek için bilgi teknolojileri yetenekleri.
E	Sürekli iyileştirmeler	Mevcut sayısal koruma yeteneklerinin değerlendirilmesi, hedeflerin belirlenmesi ve ilerlemenin takip edilmesine yönelik süreçler.
F	Topluluk	Sayısal koruma topluluğuyla daha geniş etkileşim ve katkı.
Hizmet yetenekleri		
G	Sağlama, transfer ve sisteme dâhil etme	İçeriğin sağlanması ya da transferi ve sayısal arşive dâhil edilmesine yönelik süreçler.
H	Bit akışının korunması	Korunacak sayısal içeriğin depolanması ve bütünlüğünün sağlanmasına yönelik süreçler.
I	İçeriğin korunması	Sayısal içeriğin muhteviyatı veya mahiyetini korumaya ve zaman içerisinde sürekli erişilebilirliği ile kullanılabilirliğinin sağlanmasına yönelik süreçler.

11 https://forms.gle/qDhxsnYoVMaYbtki6

DOI: http://doi.org/10.7207/dpcram22-01

J	Üstveri yönetimi	Arşivlenen sayısal içeriğin, koruma, keşif ve kullanımına ilişkin yeterli üstverinin üretilmesi ve muhafazasına yönelik süreçler.
K	Keşif ve erişim	Sayısal içeriğin keşfini mümkün kılmak ve kullanıcıların erişimini sağlamaya yönelik süreçler.

Kurumsal yetenekler

A - Kurumsal uygulanabilirlik Sayısal koruma faaliyetlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması.	
0 - Düşük farkındalık	Kurum, sayısal koruma faaliyetlerinin desteklenmesi ihtiyacı konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, sayısal koruma faaliyetlerinin desteklenmesi ihtiyacının farkındadır.
2 – Temel	Sayısal 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 sayısal koruma için bir bütçe ayrılmıştır. ● Personel gelişim gereksinimleri belirlenmiştir.
3 – Yönetilebilir	Kurumda sayısal koruma faaliyetleri yönetilir ve desteklenir. Örneğin: ● Üst yönetimin kararlılığı vardır. ● Sayısal koruma için sorumluluklar açıkça tevdi edilmiştir. ● Personel sayısal koruma faaliyetlerini yürütmek için ihtiyaç duydukları becerilere sahiptir ve gerektiğinde ilgili uzmanlığa erişebilir. ● Sayısal koruma için özel bir bütçe tahsis edilmiştir. ● Bütçeler, personel rolleri ve geliştirmeler düzenli olarak değerlendirilir. ● Raporlama, planlama ve yönetime yardımcı olmak için sayısal arşivle ilgili analizler ve raporlar hazırlanabilir. ● Personel gelişim gereksinimleri için kaynak ayrılır. ● Sayısal koruma, stratejik bir öncelik olarak belirlenmiştir.

DOI: http://doi.org/10.7207/dpcram22-01

4 – Optimum	Sayısal koruma faaliyetleri kurumda proaktif olarak yönetilir, iyileştirilir ve geliştirilir. ● Sayısal korumanın faydaları bilinir, desteklenir ve kurum geneline yayılmıştır. ● Birimler arasında bir sayısal koruma paydaş grubu kurulmuştur. ● Bir ya da daha fazla personelin alanında uzman olması beklenir. ● Bütçeler, personel rolleri ve gelişim ihtiyaçları gelecekteki değişikliklere karşı proaktif olarak değerlendirilir. ● Proaktif olarak raporlama, planlama ve yönetime yardımcı olmak için sayısal arşivle ilgili analiz ve raporlar, gelecekteki ihtiyaçlara yönelik tahminlerle ilişkilendirilir. ● Personel gelişiminin etkinliği düzenli olarak takip edilir. ● Kurumun sayısal koruma faaliyetlerini gerçekleştirememesi durumunda malzemelerin sürekli korunmasını sağlamak için süreklilik ve haleflik (devir) planlaması[12] mevcuttur.

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

DOI: http://doi.org/10.7207/dpcram22-01

B - Politika ve strateji Sayısal arşivin işleyişi ve yönetimini yönlendiren politikalar, stratejiler ve prosedürler.	
0 - Düşük farkındalık	Kurum, sayısal 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 sayısal koruma politika ya da stratejisi mevcut değildir.
2 – Temel	Kurumun temel bir çerçeve politikası mevcuttur. Örneğin: ● Üst düzeyde bir sayısal koruma politikası ya da stratejisi bulunur. ● Sayısal korumayla ilgili başka politikalar mevcut olsa da kapsamında boşluklar bulunabilir. ● Sayısal 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: ● Sayısal koruma politikası/stratejisi diğer kurumsal politikalarla ilişkilidir ve kararlaştırılan takvime göre gözden geçirilir. ● Politika ve prosedürler ilgili etik hususları dikkate alır. ● Sayısal arşivdeki içeriği yönetmek ve erişim sağlamak için dokümante edilmiş süreçler ve prosedürler bulunur. ● İlgili tüm personel, sayısal 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.
4 – Optimum	Kurum, proaktif olarak politika, strateji ve prosedürlerini yönetir ve süreç iyileştirmelerinin sürekliliğini taahhüt eder. Örneğin: ● Sayısal 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.

DOI: http://doi.org/10.7207/dpcram22-01

C - Yasal dayanak Sayısal içeriğin sağlanması, korunması ve erişimiyle ilgili yasal hak ve sorumlulukların ilgili mevzuat ve etik kodlara uyumlu olarak yönetilmesi.	
0 - Düşük farkındalık	Kurum, yasal hak ve sorumlulukların yönetilmesi veya bunların uygulanmasına yönelik temel ilkelerle ilgili ihtiyaçlar konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, yasal hak ve sorumlulukların yönetilmesi ve temel ilkelerin anlaşılmasıyla ilgili ihtiyaçlar konusunda farkındalığa sahiptir.
2 – Temel	Sayısal içerikle ilgili yasal haklar ve sorumlulukların yönetiminde temel hususlar gerçekleştirilir. Örneğin: ● Önemli yasal hak ve sorumlulukların kim tarafından gerçekleştirileceği belirlenir ve kayıt altına alınır. ● Gerekli yasal anlaşma ve sözleşme taslakları mevcuttur. ● Mesleki etik kurallarına bağlı kalınır.
3 – Yönetilebilir	Sayısal içerikle ilgili yasal hak ve sorumluluklar yönetilebilir. Örneğin: ● Lisanslama, yasal haklar ve sözleşmelerle ilgili bilgiler gerektiğinde kolayca bulunabilir ve erişilebilir. ● Yasal sorunlar ve riskler yönetilirek düzenli aralıklarla gözden geçirilir. ● Yasal sorunlar ve risklerin yönetimiyle ilgili yetkiler ve sorumluluklar açıkça belirlenmiştir. ● Gerek duyulduğunda hukuk, satın alma, sözleşme yönetimi veya bilgi edinme uyumluluğu[13] gibi uzman görüşüne başvurulabilir. ● Yasal haklar ve sorumluluklarla ilgili gerçekleştirilen faaliyetlerin dokümantasyonu yapılır. ● Farklı yasal ya da mevzuatsal gereksinimlerin söz konusu olduğu içerikler için ayrı koruma ve erişim iş akışları mevcuttur. ● Erişilebilirlikle ilgili sorumluluklar, yerel veya ulusal mevzuatın gereklilikleri doğrultusunda yerine getirilir.
4 – Optimum	Sayısal içerikle ilgili yasal haklar ve sorumluluklar proaktif olarak yönetilir. Örneğin: ● Yasal sorunlar ve riskler proaktif olarak izlenir ve hafifletilir. ● Kurum, mevzuat oluşturulmasına kaynaklık eden yasal ve adli süreçlerle ilişki kurarak bunlara girdi sağlar.

[13] 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.)

DOI: http://doi.org/10.7207/dpcram22-01

D - Bilgi İşlem yeteneği Sayısal koruma faaliyetlerini desteklemek için bilgi teknolojileri yetenekleri.	
0 - Düşük farkındalık	Kurum, sayısal arşivi destekleyecek bilgi işlem yeteneğine duyulan ihtiyaç veya bu yeteneğin uygulanmasına yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, sayısal 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: ● Sayısal arşiv için temel seviyede bilgi işlem desteği mevcuttur. ● Bilgi işlem faaliyetlerinden sorumlu olan çalışan, sayısal 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: ● Sayısal arşiv için yeterli bilgi işlem desteği mevcuttur. ● Sayısal 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: ● Sayısal arşiv için iyi seviyede bir bilgi işlem desteği mevcuttur. ● Bilgi işlem, sayısal korumayla ilgili konulara hâkimdir ve bunlarla etkileşim içerisindedir. ● Yeni bir bilgi işlem sistemi alındığında sayısal koruma gereksinimleri dikkate alınır. ● Bilgi işlem sistemlerinin geleceğe yönelik iyileştirmeleri için ayrıntılı bir yol haritası mevcuttur. ● Muhtemel yeni araçlar ve sistemler proaktif olarak belirlenir ve test edilir.

DOI: http://doi.org/10.7207/dpcram22-01

E - Sürekli iyileştirmeler Mevcut sayısal koruma yeteneklerinin değerlendirilmesi, hedeflerin belirlenmesi ve ilerlemenin takip edilmesine yönelik süreçler.	
0 - Düşük farkındalık	Kurum, mevcut durumu veya hedefleri hakkında düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, mevcut durumu anlama ve hedefleri belirleme ihtiyacı konusunda farkındalığa sahiptir.
2 – Temel	Kurum, mevcut sayısal koruma yetenekleri ve geliştirilecek alanlar konusunda temel bir anlayışa sahiptir. Örneğin: ● İlk karşılaştırmalı değerlendirme yapılmıştır. ● Sayısal koruma yetenekleri konusunda geliştirilmesi gereken hususlar belirlenmiştir. ● Kurum, muadilleri arasındaki yeri hakkında bilgi sahibidir.
3 – Yönetilebilir	Kurum, karşılaştırma ve hedefleri belirleme konusunda yönetilebilir süreçlere sahiptir. Örneğin: ● Hedefler kararlaştırılmış ve üst yöneticiler tarafından onaylanmıştır. ● Hedeflere ulaşmak için yol haritası hazırlanmıştır. ● Karşılaştırmalı değerlendirmeler belirli aralıklara tekrarlanır.
4 – Optimum	Kurum, proaktif yönetim biçimiyle süreç iyileştirmeyi sürekli kılar. Örneğin: ● Sertifikasyon/dış değerlendirme gerçekleştirilmiştir ve uygun bir biçimde sürdürülmektedir. ● İyileştirme önerileri dikkate alınarak uygulanmıştır. ● Hedefler ve yol haritası belirli aralıklara gözden geçirilir.

DOI: http://doi.org/10.7207/dpcram22-01

F - Topluluk Sayısal koruma topluluğuyla daha geniş katılım ve katkı.	
0 - Düşük farkındalık	Kurum, sayısal koruma topluluğuyla daha geniş bir katılım konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurum, sayısal koruma topluluğuyla daha geniş bir işbirliği yapmanın faydaları konusunda farkındalığa sahiptir.
2 – Temel	Kurum, daha geniş bir biçimde sayısal koruma topluluğuyla temel düzeyde ilişki kurar. Örneğin: ● İlgililerle bir ağ kurulmuştur. ● İlgili toplulukların etkinliklerine iştirak edilir. ● Başkalarının tecrübelerinden faydalanmak için çaba gösterilir.
3 – Yönetilebilir	Sayısal koruma topluluğuyla daha geniş bir ilişki kurulması desteklenerek bu ilişki yönetilir. Örneğin: ● İlgili ağlar ve topluluklar davet edilir. ● Sayısal koruma topluluğunda daha etkin bir rol üstlenilir. ● Gerektiğinde sayısal koruma konusunda uzman görüşüne başvurulur. ● Kendi iş süreçlerinden elde ettiği başarı ve çıkarılan dersler toplulukla paylaşılır.
4 – Optimum	Kurum, sayısal 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: http://doi.org/10.7207/dpcram22-01

Hizmet yetenekleri

G - Sağlama, transfer ve sisteme dâhil etme İçeriğin sağlanması ya da transferi ve sayısal arşive dâhil edilmesine yönelik süreçler.	
0 - Düşük farkındalık	Kurum, sayısal arşive içerik sağlamak ya da transfer etmek ihtiyacı ile bunu gerçekleştirmeye yönelik temel ilkeler konusunda düşük farkındalığa sahiptir.
1 – Farkındalık	Kurumun sayısal arşive sayısal 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 sayısal içeriğin seçimi ve kaydedilmesine ilişkin süreç belgelenebilir (örneğin web ve e-posta arşivleri, sayısallaştırılmış içerikler, EBYS'deki belgeler). ● Bazı içerik, sayısal 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, belge sahipleri ve 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.

DOI: http://doi.org/10.7207/dpcram22-01

4 – Optimum	Kurum, sağlama, transfer ve sisteme dâhil etme sürecini proaktif olarak yönetir ve geliştirir. Örneğin: ● Kurum, muhtemel bağışçılar, belge sahipleri ve üreticileriyle belgelerin yaşam döngüsünün en iyi biçimde yönetimini desteklemek için işbirliği yapar. ● Arşive transfer edilecek sayısal 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. ● Kullanılan araçlar ve sistemler, süreçlerle bütünleştirilmiştir. ● 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 değerlendirme yapılır.

DOI: http://doi.org/10.7207/dpcram22-01

H - Bit akışının korunması Korunacak sayısal 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 sayısal bir depo mevcuttur. ● Çalışanlar, içeriğin nerede saklandığını bilir. ● Replikasyonlar, basit yedekleme usullerine dayanır. ● 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. ● Bütünlük kontrolü sıklığı ve tutulacak kopya sayısıyla ilgili kararlar, riskler, içeriğin arşiv değeri ve hem mali hem de çevresel maliyetler göz önünde bulundurularak 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.
4 – Optimum	Kurum, proaktif risk yönetimiyle birlikte iyi derecede yönetilebilir depolama usullerini uygulamaya almıştır. Örneğin: ● Felaketlerin getireceği kayıp riskini en düşüğe indirmek için coğrafi olarak farklı konumlarda içeriğin kopyaları tutulur. ● Farklı depolama teknolojileri ya da hizmetleri kullanılır. ● 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.

DOI: http://doi.org/10.7207/dpcram22-01

I - İçeriğin korunması Sayısal içeriğin anlamını veya işlevselliğini korumaya ve zaman içerisinde sürekli erişilebilirliği ile kullanılabilirliğinin sağlanmasına 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 erişilebilirliğini takip etmek ve planlamak için yönetilebilir süreçleri uygulamaya almıştır. Örneğin: ● Teknoloji 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 sayısal malzemelerin özellikleri göz önünde bulundurularak yapılır. ● Ne zaman, ne, nasıl, neden ve kim gibi ayrıntılarla sayısal içerikteki her türlü değişim kayıt altına alınır.

DOI: http://doi.org/10.7207/dpcram22-01

4 – Optimum	Kurum, içeriğin zaman içerisinde erişilebilir olması 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 sayısal 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 sayısal içerik ve üstverilerin versiyon kontrolü sağlanır.

DOI: http://doi.org/10.7207/dpcram22-01

J - Üstveri yönetimi Arşivlenen sayısal 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 sayısal 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. ● Sayısal içerik için kalıcı tek biçim tanımlayıcılar atanmış ve bunlar muhafaza edilmiştir. ● Sayısal 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 sayısal 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. ● Mevcut koruma stratejisinin yönetimi, standartlaştırılmış içerik paketleri ve üstveriler aracılığıyla kolaylaştırılır.

DOI: http://doi.org/10.7207/dpcram22-01

K - Keşif ve erişim Sayısal 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 sayısal içerikler için temel kaynak keşif aracı mevcuttur. ● Kullanıcılar, kurum içinden ya da dışından sayısal içerik ve üstverileri görebilir veya erişebilir. ● Kullanıcıların sayısal içeriğe erişimi kayıt altına alınır. ● Sayısal 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 sayısal içerik için temel kaynak keşif aracı mevcuttur. ● Bazı sayısal içerikler için tam metin arama imkânı vardır. ● Uygun olduğunda sayısal hak bilgisi, sistem aracılığıyla görüntülenebilir ve erişilebilir. ● Kullanıcıların sayısal içeriğe erişimiyle ilgili raporlar oluşturulabilir. ● Erişim sistemleri, kullanıcı topluluğundan alınan geri bildirimlere göre güncellenir. ● Kaynak keşif bilgisi, erişilebilir formatta kullanıcılara sunulur. ● Bir çıkış stratejisi söz konusu olduğunda, her sayısal içeriğin toplu olarak sistemin dışına aktarılmasından sonra erişimine yönelik uygulama örnekleri hazırlanmıştır.

DOI: http://doi.org/10.7207/dpcram22-01

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. ● Sayısal haklar, yeniden kullanım için anlaşmaların yapılması da dâhil olmak üzere tamamen erişim sistemleri tarafından yönetilir. ● Kurum, kullanıcılara erişim desteği sunar. ● İhtiyaç ve beklentileri karşılamak için proaktif olarak kullanıcı topluluğuna danışılır. ● Sayısal içeriği keşfetmek ve erişmek için toplanan bilgi, kullanıcı deneyimini iyileştirme ve geliştirmede kullanılır. ● Sayısal içerik, erişilebilir formatlarda kullanıcıların erişimine sunulur. ● Erişim mekanizmaları, genel erişilebilirlik araçlarıyla uyumludur veya birlikte çalışabilir.

DOI: http://doi.org/10.7207/dpcram22-01

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: Sayısal koruma faaliyetlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması.				

DOI: http://doi.org/10.7207/dpcram22-01

B. Politika ve strateji: Sayısal 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 dayanak: Sayısal içeriğin sağlanması, korunması ve erişimiyle ilgili yasal hak ve sorumlulukların ilgili mevzuat ve etik kodlara uyumlu olarak yönetilmesi.				
D. Bilgi İşlem yeteneği: Sayısal koruma faaliyetlerini desteklemek için bilgi teknolojileri kabiliyeti.				

DOI: http://doi.org/10.7207/dpcram22-01

E. Sürekli İyileştirmeler: Mevcut sayısal koruma kabiliyetlerinin değerlendirilmesi, hedeflerin belirlenmesi ve ilerlemenin takip edilmesine yönelik süreçler.				
F. Topluluk: Sayısal 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 sayısal arşive dâhil edilmesine yönelik süreçler.				

DOI: http://doi.org/10.7207/dpcram22-01

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

DOI: http://doi.org/10.7207/dpcram22-01

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