TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
STRATEJİ VE BÜTÇE BAŞKANLIĞI

KAMU BİLGİ VE İLETİŞİM TEKNOLOJİLERİ YATIRIMLARI REHBERİ

2022

İçindekiler

GİRİŞ	2
BİLGİ VE İLETİŞİM TEKNOLOJİLERİ POLİTİKALARI	3
AĞ SİSTEMLERİ	6
SİBER GÜVENLİK	8
SUNUCU SİSTEMLERİ	10
VERİ DEPOLAMA VE YEDEKLEME SİSTEMLERİ	12
VERİ MERKEZLERİ VE FELAKET KURTARMA MERKEZLERİ	14
UYGULAMA YAZILIMLARI	16
EK: TEHDİT – ETKİ DEĞERLERİ TABLOSU	22

GİRİŞ

Günümüzde kamu hizmetlerinin bütün aşamalarında bilgi ve iletişim teknolojilerinden (BİT) büyük ölçüde faydalanılmaktadır. Öyle ki, BİT yatırımlarının etkinliği kamu hizmetlerinin etkinliğinin önemli bir göstergesi haline gelmiştir. Bu gelişime uygun olarak, kamu BİT yatırımları nicelik ve nitelik itibarıyla sürekli artış eğilimindedir.

BİT projelerinin yüksek seviyede teknik beceri gerektirmesi ve projelerdeki karmaşıklık seviyesinin yüksek olması BİT projelerinin başarılı bir şekilde hayata geçirilmesini zorlaştırmaktadır. Teknolojinin hızla değişmesi ise hayata geçmiş olan BİT projelerinin idamesinde güçlüklere neden olmaktadır. Bu gibi zorluklardan ötürü, BİT projelerine daha hassas bir bakış açısı ve bütüncül bir stratejiyle yaklaşılması önem taşımaktadır.

Kamu kurumları tarafından Başkanlığımıza iletilen BİT projeleri yatırım tekliflerinin incelenmesinde, Başkanlığımızca değerlendirmeye konu edilen önemli hususlar mevcuttur. Rehber, bu hususların bütüncül bir şekilde kamu kurumlarımıza duyurulmasında fayda görülmesi sebebiyle hazırlanmıştır. Başkanlığımıza teklif edilen BİT projelerinin değerlendirilmesinde, Rehberde yer alan yönlendirmeler esas alınacaktır.

Teknolojinin hızlı gelişimi ve buna mukabil ülkemiz BİT politikalarının dönüşümü, Rehberin mütemadiyen değişen ve gelişen bir yapıda olmasını zorunlu kılmaktadır. Rehberin gelişiminde, belirli alanlarda yoğun saha tecrübesine sahip kamu kurumlarımızın katkıları da önem taşımaktadır. Rehbere yönelik katkı ve geri dönüşler btd@sbb.gov.tr adresine yapılabilir.

Çalışmanın ilk taslağının ortaya çıkması sürecinde sahadan edindikleri tecrübeyi Rehberimize yansıtan İzmir Katip Çelebi Üniversitesi Bilgi İşlem Dairesi Başkanlığına teşekkür ederiz.

1. BÖLÜM
BİLGİ VE İLETİŞİM TEKNOLOJİLERİ POLİTİKALARI

- **Açık kaynak kodlu yazılım kullanımı için yol haritaları hazırlanmalıdır.**

Yazılım lisanslarında sürdürülebilirliğin sağlanması, ithalat-ihracat dengesinin ülkemiz lehine değiştirilmesi ve bilhassa kritik sistemlerde bilgi güvenliğinin daha etkin sağlanabilmesi için, kamu kurumları tarafından açık kaynak kodlu yazılımlara geçiş süreci planlanmalı ve bir yol haritası halinde dokümante edilmelidir. Açık kaynak kodlu yazılımlara geçişte, sektörden teknik destek alınabilecek, görece daha kolay geçiş yapılabilecek ve daha fazla katma değer sağlayacak yazılım türlerine öncelik verilmelidir. Kurumların bilgi işlem kapasiteleri buna yönelik olarak geliştirilmelidir. (11. Kalkınma Planı p.813.2)

- **Yerlilik payı yüksek ve yabancı ürün bağımlılığını azaltan yazılım ve donanım ürünlerinin kullanıldığı projelere öncelik verilmektedir.**

Bilgi ve iletişim teknolojileri altyapılarında olgun yerli ürünlerin tercih edilmesi, ithalat-ihracat dengesine olumlu etki yapmakta ve ülkemizin bu alandaki insan kaynağı kapasitesine doğrudan olumlu etkide bulunmaktadır. Başta siber güvenlik olmak üzere kritik alanlarda yerli ürün ve çözümlerin temini ulusal güvenlik açısından da büyük önem taşımaktadır. Bu çerçevede temin edilecek donanım ve yazılımların yerli muadilleri araştırılmalı, yerinde testleri yapılmalı ve bilgi ve iletişim teknolojileri alımlarına yönelik şartnameler bu ürünleri dışarıda bırakmayacak şekilde hazırlanmalıdır. (11. Kalkınma Planı p.486.1)

- **Bilgi ve iletişim teknolojileri projeleri, ürün ve platform bağımlılığına neden olmayacak şekilde geliştirilmelidir.**

Bilgi teknolojileri yatırımlarında marka ve ürün bağımlılığın oluşmasına neden olmayacak ürünler tercih edilmelidir. Bu kapsamda, farklı ürünlerin entegrasyonuna izin veren uluslararası kabul görmüş standartları destekleyen ürün içeriklerine sahip projeler tercih edilmelidir. Yazılım projelerinde belirli bir işletim sistemine ve internet tarayıcısına bağımlılık oluşmadığından emin olunmalıdır.

- **Bilgi sistemlerini toplulaştırıcı projeler geliştirilmelidir.**

Kamu kurumlarında veri merkezi ve sistem odalarının sayıca fazlalığı, mükerrer yatırımlara sebebiyet vermektedir. Mümkün olan her durumda bilgi teknolojileri altyapılarının bütünleştirilmesi hizmet kalitesini artıracağı gibi sürdürülebilirliği de sağlayacaktır. Bu çerçevede farklı birimler için bilgi teknolojileri altyapısı kurulması yöntemi izlenmemeli, var olan ayrı sistemler bütünleştirilmelidir. (11. Kalkınma Planı p.808.2)

- **Ortak platform ve çözümlere öncelik tanınacaktır.**

Bilgi ve iletişim teknolojileri arasında işlev bakımından benzerlik gösteren ve ortak yönleri bulunan projelerin merkezi olarak tek seferde geliştirilmesi ve ilgili tüm paydaşların kullanımına açılması bu alanda mükerrer yatırımları önleyecektir. Ulusal ölçekte ihtiyacı karşılayabilecek ve bu suretle kurumların münferit proje ihtiyaçlarını merkezi olarak giderebilecek projelere öncelik verilmektedir. (11. Kalkınma Planı p.812)

- **Proje tasarımında birlikte çalışabilirliğin tesisi göz önünde bulundurulmalıdır.**

Kamu hizmetlerinin sunulmasında bilgi sistemleri arasındaki entegrasyon belirli standartlar çerçevesinde temin edilmeli ve ilgili kurumlar arasında eşgüdüm sağlanmalıdır. Projelerin tasarımı bir birimin veya bir kamu kurumunun ihtiyaçları ile sınırlı tutulmamalı, proje kapsamında üretilecek veriye ihtiyaç duyan paydaş kamu kurumlarının da katkısı alınarak daha bütüncül tasarımlar oluşturulmalıdır.

- **Coğrafi tabanlı BİT projelerinde Türkiye Coğrafi Bilgi Sistemi Kurulunun kararlarına uyulması esastır.**

On Birinci Kalkınma Planında 812 numaralı politika ile Ulusal Coğrafi Bilgi Sisteminin tamamlanması öngörülmüştür. Bu çerçevede 49 sayılı Coğrafi Bilgi Sistemleri Hakkında Cumhurbaşkanlığı Kararnamesi gereğince oluşturulan Türkiye Coğrafi Bilgi Sistemi Kurulu tarafından ülkemizde coğrafi verilerin üretilmesinden sorumlu olan kurumlar Ulusal Coğrafi Veri Sorumluluk Matrisinde tanımlanmış, verilerin TUCBS'den merkezi olarak paylaşımına ilişkin esaslar ise Ulusal Coğrafi Veri Paylaşım Matrisi ile uygulamaya konulmuştur. Bu kapsamda coğrafi verilerin belirlenen standartlara uygun şekilde üretilmesi, mükerrer veri üretiminin engellenmesi ve tek merkezden paylaşımının sağlanması amacıyla Türkiye Coğrafi Bilgi Sistemi Kurulunun kararları doğrultusunda coğrafi tabanlı BİT projelerinde kamu kurumlarının görev ve sorumluluklarına ve veri paylaşım esaslarına uygun şekilde veri üretilmesi ve paylaşılması gerekmektedir. (11. Kalkınma Planı p.812.7)

- **Siber güvenlik projelerinde Bilgi ve İletişim Güvenliği Rehberinde paylaşılan hususlara uyulması esastır.**

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından kamu kurumlarınca uyulması gereken bilgi ve iletişim güvenliği tedbirlerini içeren Bilgi ve İletişim Güvenliği Rehberi yayımlanmıştır. Siber güvenlik ihtiyaçları kurumlar arasında farklılık gösterebilmekle birlikte, projelerin bahse konu rehberde yer alan hususlar dikkate alınarak projelendirilmesi gerekmektedir. (11. Kalkınma Planı p.814.2)

- **Yatırım projeleri kapsamındaki donanım ve yazılım alımlarında takvimlendirmeye dikkat edilmelidir.**

Uygulama geliştirme projelerinin bir unsuru olarak temin edilen donanımlar belirli bir kullanım ömrüne sahiptir. Yazılım geliştirilme süreci başında donanımların tahmine dayalı şekilde tümüyle temin edilmesi yerine, geliştirme süreci devam ederken oluşan ihtiyaçlara paralel şekilde kademeli alımlar yapılmalı, yazılımın tamamlanmasına müteakip ortaya çıkan kesin ihtiyaca uygun şekilde alımlar tamamlanmalıdır.

- **İdame projelerinde bakım süreleri en uygun şartlar göz önünde bulundurularak belirlenmelidir.**

Mevcut donanım ve yazılım altyapısına ilişkin bakım hizmetlerinin temin edildiği idame nitelikli projeler, Yatırım Programında genel olarak tek yıllık proje olarak yer almaktadır. Bu projeler kapsamında yapılacak hizmet alımlarının çok yıllık alınması halinde ortaya çıkacak maliyetlerin de proje teklifi aşamasında çalışılması ve maliyet avantajı sağlayacak çözümün tercih edilmesi gerekmektedir.

- **Bilgi sistemlerinin sürdürülebilirliğinde kurumun insan kaynağı kapasitesinden aktif şekilde faydalanılmalıdır.**

Bilgi sistemlerinin idamesinde kurum personelinin aktif kullanımı esastır. Derinlemesine uzmanlık gerektiren veya personel istihdamından daha maliyet-etkin olan alanlar haricinde, kurumun insan kaynağı kapasitesinin artırılması ve bu suretle idame maliyetlerinin azaltılarak sürdürülebilirliğin sağlanması hedeflenmelidir. Bu kapsamda, kamu kurumlarınca geliştirilen yazılım projelerinde kurum personelinin sürecin başından itibaren aktif rol alması ve idame sürecinde dış kaynağa ihtiyaç duyulmayacak bir planlama yapılması esastır. (11. Kalkınma Planı p.811)

- **Temin edilecek çözümlerde toplam sahip olma maliyeti dikkate alınmalıdır.**

Proje teklifleri kapsamında temin edilecek ürün ve çözümlerin yıllık yenilemeleri, güncelleme, bakım ve teknik destek bedelleri de hesaba katılarak toplam sahip olma maliyeti açısından en uygun olan çözümün teklif edilmesi gerekmektedir.

- **Yeni bilgi ve iletişim teknolojileri projelerinin sağlayacağı katkı çok boyutlu bir şekilde değerlendirilmelidir.**

İnternet teknolojisinin gelişmesiyle birlikte birçok kamu kurumu hizmet sunumunda uzaktan 7/24 hizmet sunumunu ve işlem yapılmasını sağlayan sistemler geliştirmek için yatırım projeleri hazırlamaktadır. Özellikle pandemiyle birlikte bu süreç hızlanmıştır. Kamu idarelerinin bu tür projeleri geliştirirken, söz konusu projelerin sağlayacağı ekonomik ve sosyal katkıları, bütçe yükünü ve/veya tasarruflarını (örneğin hizmet binası, taşıt, makine teçhizat yatırımı, işletme maliyeti, personel istihdamı vb.) detaylı bir şekilde ortaya koyması gerekmektedir.

- **Kamu bilişim hizmetlerinin sunulmasında dış kaynak kullanımının tercih edilmesi durumunda yetkilendirilmiş hizmet sağlayıcılardan hizmet alınmalıdır.**

Kamu bilişim projelerinin yürütülmesi, yazılım geliştirme, entegrasyon ve bakım hizmetleri ile sızma testine yönelik hizmet alımlarında, Kamu Bilişim Hizmet Alımı Kapsamında Katılımcıların Yetkilendirilmesi Hakkında Yönetmelik kapsamında Sanayi ve Teknoloji Bakanlığı tarafından yetkilendirilen hizmet sağlayıcılarından hizmet alınması gerekmektedir.

2. BÖLÜM
AĞ SİSTEMLERİ

Ağ sistemlerinin güvenilir şekilde hizmet vermesini sağlamak ve ağ altyapısından yüksek verim elde etmek için ağ altyapısının etkin yönetimi günümüzde büyük öneme sahiptir. Bu kapsamda ağ kaynaklarının ve trafiğinin ayarlanabilmesi, gerektiği durumda ağ ölçeğinin genişletilebilmesi ve ağ kullanımının en iyi duruma getirilmesi gerekmektedir. Diğer yandan yeni cihazların sisteme entegre edilmesi öncesinde mevcut altyapının etkin kullanımına yönelik adımlar atılmalıdır.

- **Ağ altyapısı genişletilebilir bir yapıda tasarlanmalıdır.**

Kurumun kullanıcı sayısında yaşanan değişim, yeni hayata geçirilen uygulamalar ve temin edilen cihazlar, ağ altyapısı üzerinde yeni taleplere neden olabilmektedir. Tümüyle öngörülebilir olmayan bu tür gelişmeler nedeniyle ağ altyapısına yönelik uzun vadeli gerçekçi planlar yapılamamaktadır. Bu nedenle, ağ altyapısının her türlü olasılığı göz önünde bulundurarak geniş bir ölçekte kurulmasından ziyade mevcut ihtiyaçlara cevap verebilir ve potansiyel ihtiyaçlara göre genişletilebilir bir yapıda tasarlanması esastır.

- **Ağ altyapısının ölçeği belirlenmeli ve kullanılacak donanımlar bu ölçeğe uygun seçilmelidir.**

Ağ gereksinimlerinin belirlenmesinde temel ölçütlerden birisi ağın ölçeğinin belirlenmesidir. Bu amaçla hizmet verilecek son kullanıcı sayısı, iletişim kurulacak uç noktaların sayısı, son kullanıcıya sunulacak hizmetlerin gerektirdiği bant genişliği, sunucu ve uygulamaların ihtiyaçları gibi etkenler göz önünde bulundurulmalıdır. Temin edilecek altyapı bu metriklerle, dolayısıyla kurumun ağ ölçeğine uygun seçilmiş olmalıdır.

- **Ağ altyapısında kullanılan cihazlara ilişkin metrikler izlenebilmelidir.**

Kurum ağına bağlı cihazları tanımlamak ve donanım envanterindeki değişiklikleri takip etmek için ağ cihazlarının mevcut durumları, bağlantı kapasiteleri gibi teknik özellikleri anlık olarak takip edilmelidir. Böylelikle ağ altyapısında meydana gelen hataların tespiti ve hızlı bir şekilde çözüm üretilebilmesi mümkün olacaktır. Bu amaçla kullanılabilecek olgun açık kaynak kodlu yazılımlar mevcut olup ihtiyacı karşılaması halinde bu tür yazılımların kullanımı önerilmektedir. Bilgi teknolojileri altyapılarının idamesine yönelik proje tekliflerinin, mevcut cihazlara ilişkin metriklerle desteklenmesi beklenmektedir.

- **Omurga ve uç noktalardaki cihazlar, ihtiyaca uygun niteliklerde olmalıdır.**

Kurum ağının merkezini oluşturan omurga anahtarlarda seçilen mimari, donanımın ve modüllerinin temin ve idame maliyeti, enerji ihtiyacı, genişleme potansiyeli ve trafik performansı gibi konularda belirleyici olmaktadır. Bu çerçevede mimari seçiminde ihtiyaca ilişkin bu gibi faktörler göz önünde bulundurulmalıdır. Bununla birlikte ağın farklı noktalarında standart bir yaklaşım benimsenmesi yerine değişen ihtiyaca uygun farklı özelliklerde donanımların tercih edilmesi gerekmektedir. İhtiyacın üzerinde cihaz konfigürasyonlarının tercih edilmemesi, bu alanlardaki gereksiz harcamaları önleyecektir. Bu kapsamda, omurga cihazları ile son kullanıcıya yönelik cihazların temini öncesinde ihtiyaç planlaması verilerle desteklenmek suretiyle yapılmalıdır.

- **Ağ tasarım ve kullanımında kurumsal veri sınıflandırması göz önünde bulundurulmalıdır.**

Ağ altyapısının tasarımında, bilgi sistemlerinin kritiklik seviyesi temel belirleyici unsurlar arasındadır. Öncelikle bilgi sistemlerinde tutulan veriler sınıflandırılmalı, ağ tasarımı verilerin kritiklik seviyeleriyle uyumlu olmalıdır. Kritik sistemlerin barındırılması ile bu sistemler arasındaki veri trafiğinin yönetimi için ayrılan kaynaklarla daha az kritikliğe sahip sistemler için ayrılan kaynaklar arasında ayrıma gidilmelidir. Örneğin, VPN altyapısı tüm bilgi ve iletişim projeleri için zorunlu görülmemeli, bu tür bir altyapının kullanımına verilerin kritiklik sınıflandırması yapıldıktan sonra karar verilmelidir.

- **Ağ cihazlarının temini öncesinde mevcut donanım ve yazılımlarla gerekli güvenlik önlemleri alınmış, alternatif çözümler araştırılmış olmalıdır.**

Temin edilecek ağ cihazlarının kullanım amacı net bir şekilde ortaya konabilmelidir. Mevcut durumun dezavantajları, yönetilebilme durumu, politika ve prosedürlerin iyi hazırlanıp hazırlanmadığı sorularına cevap verilmeli, alternatif çözümler değerlendirilmelidir. Yeni bir cihaz temini kararı öncesinde mevcut cihazlarda yapılacak konfigürasyon değişiklikleriyle ihtiyacın giderilip giderilemediği analiz edilmelidir. Ayrıca, cihazları kullanabilecek yetkin personele sahip olunduğundan emin olunmalı ve cihaz donanım bağımlılığına neden olmayacak şekilde seçilmelidir.

Kontrol Listesi
Ağ altyapısı genişletilebilir yapıda tasarlandı mı?
Kurumun ağ ölçeği belirlenerek proje teklifi bu ölçek dikkate alınarak oluşturuldu mu?
Ağ ölçeği belirlenirken hangi faktörler dikkate alındı?
Ağ yönetimine ilişkin alanlarda açık kaynak kodlu yazılımların kullanılabilirliğine yönelik bir analiz yapıldı mı?
Ağ altyapısı ihtiyaçları belirlenirken, mevcut altyapıdan elde edilen metriklerden faydalanıldı mı?
Omurga ve uç noktalardaki cihaz ihtiyaçlarının belirlenmesinde ihtiyaca göre farklılaşmaya gidildi mi?
Bilgi sistemleri ve bu sistemlerde barındırılan veriler için bir kritiklik sınıflandırması yapıldı mı? Ağ altyapısının tasarımında bu sınıflandırma dikkate alındı mı?
Temin edilecek cihazların amacı net olarak belirlendi mi? İhtiyacın mevcut cihazlarda yapılacak konfigürasyon değişiklikleriyle giderilemediğinden emin olundu mu?
Alımı yapılacak donanımın/yazılımın yerli muadili bulunuyor mu? Teknik şartname yerli ürünleri kapsayacak şekilde tasarlandı mı?
Temin edilecek cihazları yönetebilecek insan kaynağı kapasitesi mevcut mu?
Temin edilecek cihazlar donanım bağımlılığına neden oluyor mu?

3. BÖLÜM
SİBER GÜVENLİK

Siber saldırıların sayısındaki artış ve tehditlerin her geçen gün daha karmaşık bir hale gelmesi kurumların bu alana yüksek bütçeler ayırmasına ve ciddi yatırımlar yapmasına neden olmaktadır. Öte yandan, harcamaların etkin sonuç vermesi belirli şartlara bağlıdır. Siber güvenlik, farklı katmanlarda birbirini tamamlayıcı önlemler alınmasını ve kurum genelinde farkındalık oluşturulmasını gerektirmektedir. Güvenliği sağlamak amacıyla temin edilen cihaz ve yazılımların verimliliği ise, mimari tasarım ve konfigürasyonların etkinliği ile doğrudan ilişkilidir. Tehditlerin sadece kurum dışından değil kurum içinden de gelebileceği göz önünde bulundurularak bilgi güvenliğini bütünleşik bir şekilde ele alan planlamalar yapılmalıdır.

- **Siber güvenlik tehditlerine ilişkin bütüncül risk analizi ve planlama yapılmalıdır.**

Siber güvenlik alanında karşı karşıya kalınan tehditler her geçen gün artmakta, ancak bu tehditlere karşı güvenliği tümüyle etkin bir şekilde sağlamak mümkün görünmemektedir. Güvenliğin sağlanması için teknoloji ve çözüm odaklı bir yapılanma yeterli değildir. Öncelikle kurumun sahip olduğu verilerin kritiklik ve hassasiyet seviyesi belirlenmeli, karşı karşıya kalınabilecek tehditlerle bu tehditlerin yol açabileceği potansiyel zararlar analiz edilmeli, mevcut personelin yetkinlik düzeyi analiz edilmeli ve tüm bu değerlendirmelerin neticesinde kurumsal siber güvenlik politikası ve yol haritaları ortaya konmalıdır.

- **Verilerin kritiklik sınıflandırması yapılmalıdır.**

Bilgi sistemlerinde barındırılan ve sistemler arasında aktarılan verilerin kritiklik seviyelerine göre sınıflandırılması gerekmektedir. Bu sayede, farklı kritiklik seviyelerindeki veriler için farklı seviyelerde siber güvenlik önlemlerinin alınabilmesi sağlanabilecektir. Verilerin kritiklik sınıflandırması için Ek'te yer alan "Tehdit – Etki Değerleri" tablosundan faydalanılarak objektif ve veriye dayalı bir sınıflandırma yapılmalıdır.

- **Kurumsal siber güvenlik sertifikasyonları belgelendirme ile sınırlı tutulmamalı, aktif bir süreç olarak sürdürülmelidir.**

Kamu kurumları tarafından başta ISO 27001 olmak üzere bilgi güvenliğine yönelik sertifikasyonlar alınmaktadır. Sertifikasyon sürecinin ve bilgi güvenliği kültürünün, bilgi işlem birimi ile sınırlı kalmayarak kurum geneline yaygınlaştırılması gerekmektedir. Ayrıca, siber güvenliğe ilişkin çalışmalar sertifikasyonla sınırlı tutulmamalı, sertifikasyona sahip olma durumu aktif bir süreç olarak değerlendirilmeli ve belgelendirmeyle oluşturulan kural, çıktı ve kontroller süreklilik arz edecek şekilde takip edilmelidir.

- **Bilgi sistemleri altyapısına uygun şekilde belli sayıda personelin siber güvenlik alanında görevlendirilmesi gerekmektedir.**

Siber güvenliğin son derece özelleşmiş bir uzmanlık alanı olması sebebiyle, bu alanda bir grubun kurumun altyapısı ve ölçeğine uygun şekilde görevlendirilmesi gerekmektedir. Ayrıca SIEM, DLP gibi bazı çözümler belli sayıda personelin tahsisini gerektirmektedir. Bu tür çözümlerin temini amaçlanmakta ise cihazları kullanması planlanan personelin nicelik ve nitelik itibarıyla yeterli düzeyde olduğundan emin olunmalıdır. Bu tür çözümlerin diğer bir ön

koşulu da verilerin önem ve kritiklik derecelerinin tespit edilmesidir. Veriler kritiklik derecelerine göre sınıflandırılmadığında, bu çözümlerden beklenen fayda sağlanamayacaktır. Hızla değişen ve gelişen siber güvenlik tehditlerine karşı grubun bilgi birikimin güncelliği sağlanmalıdır. Siber güvenlik eğitimleri teknik ekiple sınırlı tutulmayarak kurum genelinde siber güvenlik kültürü oluşturulmalıdır. Nihai aşamada, kurumun kendi kendine yetebilen bir seviyeye erişebilmesi amaçlanmalıdır.

- **Mümkün olan hallerde, alımı yapılacak olan sistemin öncesinde kavram ispatı çalışması yapılmalıdır.**

Uygun ürünün tespit edilmesi açısından yerinde deneme imkânlarından yararlanılmalı, Kavram ispatı (Proof of Concept - PoC) aşamasında kurumsal ihtiyaçlara uygunluk değerlendirmesi yapılmalı, gerektiği durumda güncellemeye gidilmelidir. Ayrıca PoC aşaması firmanın tüm konfigürasyonları yaptığı ve belli bir süre ürünün çalıştığı bir süreç olarak görülmemeli, kurum personelinin de aktif katılımı sağlanmalıdır. PoC aşamasında kurumun ihtiyacını görecek senaryoların kavram ispatı özellikle talep edilmelidir. Mümkün ise kurum ağında, kurum trafiğinde testler gerçekleştirilmeli, çözümün kurum trafiğindeki davranışı değerlendirilmelidir. Mümkün olmadığı durumda üretici ortamında veya test merkezlerinde kurum trafiğine yakın nitelikte paketler ve kurum ortamına yakın mimari ile PoC testlerinin yapılması sağlanmalıdır.

- **Donanım veya yazılım temininde mevcut durum değerlendirilmeli, eksiklikler ortaya konmalı ve uygun çözümlerin temini sağlanmalıdır.**

Güvenlik cihazları kademeli bir ürün yelpazesi sunmaktadır. Karmaşıklık arz etmeyen siber güvenlik ihtiyaçları ağ topolojisinde yapılacak değişiklerle giderilebileceği gibi basit seviye cihazların iyi konfigüre edilmesiyle de giderilebilir. Bu cihazların yeterli olmadığının tespiti halinde bir üst kademede yer alan ve görece daha karmaşık siber güvenlik ihtiyaçlarına yönelik olan çözümler tercih edilmelidir. Ayrıca, temin edilecek çözümlerin bilgi sistemlerinin kritiklik seviyesiyle orantılı olması esastır. Mümkün olan hallerde çözüm temininden önce yerinde deneme yapılması uygun olacaktır.

- **Gelişmekte olan teknolojilere sahip ürünlerin temini konusunda temkinli olunmalıdır.**

Siber güvenlik alanında yapay zeka ve davranış analizi temelli çözümler giderek artmaktadır. Bu tür çözümler makine öğrenmesi algoritmaları yardımıyla geleneksel imza tabanlı çözümlerin tespit edemediği saldırı türlerini tespit edebilmektedir. Ancak, henüz gelişim sürecinde olan bu çözümlerin temin edilmesinde temkinli davranılmalıdır.

Kontrol Listesi
Kurum ağı için öncelikli güvenlik tehditleri belirlendi mi? Kabul edilebilir riskler tanımlandı mı?
Kurumun siber güvenlik sertifikasyonu bulunuyor mu? Siber güvenlik yaklaşımı dinamik bir süreç anlayışını içeriyor mu?

Kurumsal verilerin kritiklik sınıflandırması yapıldı mı?
Kurumun münhasıran siber güvenlik alanına tahsis edilmiş ekibi mevcut mu? Bu personelin eğitim planlaması yapılıyor mu?
Kurum genelinde siber güvenlik farkındalık eğitimleri planlanıyor mu?
DLP, EDR, SIEM gibi spesifik çözümler talep edilmekte ise bu çözümlerin kullanımı için personel tahsis edilebilecek mi?
Kurumun altyapısında kullanılacak olan güvenlik çözümlerinin yerli muadilleri bulunuyor mu? Teknik şartnameler bu yerli muadilleri de kapsayacak şekilde hazırlandı mı?
Kurumun ihtiyacı olan sistemlerin görevini yapabilecek açık kaynak kodlu olgun çözümler bulunmakta mıdır?
Kurum bünyesinde alımı yapılacak olan sistemin daha öncesinde PoC çalışması yapılmış mıdır?
Mevcut ağ güvenliği sistemlerinin performans durumuna ilişkin veriler ve grafikler detaylı olarak incelenmiş midir?
Tehdit istihbaratının zenginleştirilmesi ve güçlendirilmesi için bir yaklaşım mevcut mu?

4. BÖLÜM
SUNUCU SİSTEMLERİ

Kurumsal uygulamalar, dosya paylaşımı, belge yönetim sistemleri gibi elektronik ortamda sunulan pek çok hizmet için sunucular kullanılmaktadır. Bu yönüyle sunucular bilgi sistemlerinin merkezi bir konumundadır. Bu uygulamaların etkinliği, doğru mimari tasarım, uygun sunucu sistemlerinin tercihi ve altyapının etkin kullanımı ile yakından ilgilidir.

- **Sunucu mimarisi kullanım alanına uygun şekilde seçilmelidir.**

Sunucunun kullanım amacı ve karşılanacak hizmetler kurumun bilgi sistemleri altyapısı ve ölçeği de göz önünde bulundurularak uygun mimari seçimi yapılmalıdır. Zorunlu olmadıkça raf tipi sunucular tercih edilmeli, üretici bağımlığına sebep olacak özelleştirilmiş donanımlar bulundurulmamalıdır. Proje kapsamında raf tipi sunucu haricinde özelleşmiş bir sunucu mimarisi kullanılacak ise bu durumun gerekçeleriyle birlikte belirtilmesi önem taşımaktadır.

- **Hizmet ölçeği belirlenerek bu ihtiyaca uygun sunucular tercih edilmelidir.**

Kurumun farklı lokasyonlarda bulunan birimleri ve hizmet verilen kullanıcı sayıları, kurum içi ve dışına hizmet veren uygulamalar, üretilen veri miktarı gibi mevcut duruma ilişkin faktörler tespit edilmeli, temin edilecek sunucu üzerinde hizmet verecek sanal sunucular, hizmet verecek uygulamalar ve bu uygulamaların gereksinimleri göz önünde bulundurularak ihtiyaçlara uygun sunucular temin edilmelidir. Bu amaçla sunucu bileşenlerine ilişkin gereksinim dokümanları oluşturulmalıdır. Sunucu sistemlerinin teknolojik ve ekonomik ömrü

göz önünde bulundurularak, ihtiyaç tespitinde cihazların teknik ömrünü aşacak derecede uzun vadeli projeksiyonların yapılmaması kaynak israfını önleyecektir.

- **Donanım temini öncesi mevcut durum değerlendirilmelidir.**

Her bir yeni yazılım veya uygulama planlaması öncesinde mevcut sunucu altyapısına ilişkin yeterlilik değerlendirmesi yapılmalı, yeni uygulama için yeni sunucu temin edilmeden önce mevcut sunucu altyapısının kullanılmasına öncelik verilmelidir.

- **Sanallaştırma alanında yenilikçi teknolojilerden ve açık kaynak kodlu yazılımlardan faydalanılmalıdır.**

Günümüzde klasik sanallaştırmanın yanı sıra farklı yöntemlerle özelleştirilen sanallaştırma teknolojileri de bulunmaktadır. Kurumun hizmet ölçeği de göz önünde bulundurularak kaynak tüketimleri açısından önemli bir tasarruf ve performans kazancı sağlayabilen farklı sanallaştırma teknolojilerinden faydalanılması gerekmektedir. Örneğin, donanım kaynaklarının sanallaştırılması düşünülebileceği gibi konteyner bazlı sanallaştırma sistemleri de değerlendirilmelidir. Bu alanda açık kaynak kodlu olgun yazılım çözümleri de analizlerde göz önünde bulundurulmalıdır.

- **Sunucular üzerinden kullanılan yazılımların temini öncesinde açık kaynak kodlu yazılımlar araştırılmalıdır.**

Sunucu sistemleri üzerinde veritabanı, uygulama sanallaştırma, büyük veri analitiği, aktif dizin yönetimi, kimlik yönetimi, e-posta gibi farklı alanlarda geliştirilen yazılımlar kullanılmaktadır. Bu gibi yazılımların temin kararı öncesinde açık kaynak kodlu alternatifler araştırılmalı, geliştirilecek uygulamanın gereksinimleri de göz önünde bulundurularak açık kaynak kodlu alternatiflerin kullanımına öncelik verilmelidir.

Kontrol Listesi
Mevcut sunucu altyapısının kullanım oranları ve performans durumuna ilişkin raporlama proje teklif formuna eklendi mi?
Sunucu üzerinde çalışacak olan uygulamalara ilişkin ihtiyaç analizi yapıldı mı?
Teklif edilen sunucu kapasitesi uygulamalara ilişkin ihtiyaç analiziyle örtüşüyor mu?
Temin edilecek donanım veya bu donanımın kullanımına ilişkin yazılımların yerli veya açık kaynak kodlu muadilleri bulunuyor mu? Teknik şartnamelerin yerli veya açık kaynak kodlu muadilleri de kapsayacak şekilde hazırlanması planlanıyor mu?
Temin edilecek sunucularda üretici ve platform bağımsızlığını temin edecek önlemler alındı mı?

5. BÖLÜM
VERİ DEPOLAMA VE YEDEKLEME SİSTEMLERİ

Bilgi sistemlerinde kullanılan uygulamalar ile kullanıcıların ve uygulamaların kullandığı veriler, veri depolama sistemlerinde saklanmaktadır. Ayrıca veri depolama alanları sistem sorunlarına karşın yedekleme amacıyla da kullanılmaktadır. Böylece veri depolama sistemleri sunucularla birlikte bilgi sistemlerinin merkezini oluşturmaktadır.

- **Kullanım alanı, hizmet ölçeği ve performans ihtiyacı ile uygun veri depolama çözümü tercih edilmelidir.**

Veri depolama çözümlerinin kullanılacağı dosya paylaşımı veya görsel içerik saklanması gibi kullanılacak verinin kullanım alanı mimari tercihinde belirleyici olabilmektedir. Bununla birlikte bilgi sisteminin ölçeği de veri depolama mimarisi seçiminde önemlidir. Tercih edilecek çözümde bu gibi değişkenlerin göz önünde bulundurulması beklenmektedir. Veri depolama sisteminde kullanılacak olan disklerin türü sistemin maliyetini etkilemektedir. Disk teknolojisi, ihtiyaç duyulan depolama kapasitesi ve uygulama performansını yakından etkilemektedir. Kurumun veri depolama sistemi tercihinde farklı veri depolama mimarisi alternatifleri ve bu mimariler üzerinde konumlandırılacak disk türleri fayda-maliyet açısından karşılaştırılmalı ve sistemin ekonomik ve teknolojik ömrü dâhilinde en uygun maliyetle en fazla katma değer sağlayacak mimari ve disk türleri seçilmelidir. Veri depolama sisteminin sahip olduğu disk teknolojisinin seçiminde en yüksek performanslı disk türlerinin tercihi yaklaşımı yerine ihtiyaç duyulan spesifikasyona uygun disk türünün seçilmesi beklenmektedir. Disk türlerinin seçiminde, verilerin farklı disk türlerinde performans odaklı, hibrit şekilde saklanabileceği hatırda tutulmalıdır.

- **Kullanılacak veri depolama sisteminin kapasite ve performans ihtiyacı en ideal seviyede belirlenmelidir.**

Veri depolama sistemlerinin temini için var olan veri depolama sistemlerinin kapasiteleri ve veri değişim miktarının belirlenmesi gerekmektedir. Değişen veri miktarına ve yeni doğabilecek ihtiyaç öngörülerine göre kapasite planlaması yapılmalıdır. Yapılacak kapasite planlamasında, kullanılacak donanımın ekonomik ve teknolojik ömrü göz önünde bulundurulmalıdır.

- **Kritiklik arz eden projelerde kullanılacak veri depolama sistemlerinde iş sürekliliği ve yedekleme fonksiyonları da dikkate alınmalıdır.**

Kritiklik arz eden projelerin kesintisiz hizmet verebilmesi için özel veri depolama sistemlerine ihtiyaç duyulabilmektedir. Kurumun proje kapsamındaki tüm uygulamaları için topyekün bir çözüm yerine uygulama bazlı ihtiyaçlara göre özelleşmiş bir mimari çözüm daha maliyet etkin olacaktır. Uygulamaların kabul edilebilir veri kayıp süresi ve kurtarılan verinin devreye alınma süresi, tercih edilecek veri depolama sistemi türünü doğrudan etkilemektedir. Bu sürelerin çok kısa olması gerekli ise, veri depolama sistemlerinin veri sanallaştırma özelliğiyle anlık kopyalarının alınabileceği ve bu sayede iş sürekliliğinin temin edilebileceği bir mimari oluşturulmalıdır.

- **Veri yedekleme sistemleri, ayrı birer donanım olabileceği gibi var olan depolama sistemi içerisinde de planlanabilir.**

Uygulamalar kapsamındaki verilerin yedeklerinin aynı veri depolama sistemi üzerinde saklanmaması gerekmektedir. Veri yedeklerinin ayrı bir yedekleme sistemiyle, ayrı bir depolama alanında saklanması uygun olacaktır. Kurumun hali hazırda mevcut olan yedekleme sisteminin kullanılmasına öncelik verilmelidir. Varsa farklı veri depolama birimleri arasında veri yedeklerini dağıtarak veri yedekleme planlaması yapılabilir.

- **Veri yedekleme sistemlerinin kapasite ihtiyacının belirlenmesi için bir analiz yapılmalıdır.**

Veri yedekleme sistemlerinin kapasitelerinin belirlenmesinde, uygulama kapsamında tutulan veri miktarı, veri değişim miktarı, yedekleme sayıları ve kritiklik seviyelerinin belirlenerek planlamaların yapılması gerekmektedir. Proje kapsamında teklif edilen uygulamaların kritiklik seviyesi ve veri değişim miktarına göre, kabul edilebilir veri kayıp süresi ve kurtarılan verinin devreye alınma süresi de göz önünde bulundurularak yedekleme alan kapasitesi belirlenmelidir.

- **Kurumun felaket kurtarma merkezi mevcut olması halinde, veri yedekleme sistemlerinin planlamasına dahil edilmelidir.**

Kurumun felaket kurtarma merkezi mevcut olması halinde, veri yedekleme planlarının felaket kurtarma merkezine de aktarılacak şekilde yapılması gerekmektedir. Her verinin ya da yedekleme planının felaket kurtarma merkezine aktarılması maliyet açısından uygun olmayabilir. Uygulamaların kritiklik seviyesine ve kurumun ihtiyaçlarına göre yedekleme planları felaket kurtarma merkezine aktarılacak şekilde yapılmalıdır.

Kontrol Listesi
Veri depolama çözümü tercih edilirken kullanım alanı, hizmet ölçeği, kapasite ve performans gibi unsurlara ilişkin ihtiyaç analizi yapıldı mı?
Kritiklik arz eden projelerde kullanılacak veri depolama sistemlerinde iş sürekliliği ve yedekleme fonksiyonları dikkate alındı mı?
Kurumda hali hazırda kullanılan bir veri yedekleme sistemi var mı? Veri yedekleme sistemleri için yapılan tekliflerde var olan sistemler planlamaya dahil edildi mi?
Veri yedekleme sistemlerinin kapasite ihtiyacının belirlenmesi için bir analiz çalışması yapıldı mı?
Kurumun felaket kurtarma merkezi mevcut ise, veri yedekleme sistemlerinin planlamasına dahil edildi mi?

6. BÖLÜM
VERİ MERKEZLERİ VE FELAKET KURTARMA MERKEZLERİ

Veri merkezi tasarım süreçleri; veri merkezi alan seçimi ve çevresel koşulların sağlanması, kritik güç sistemleri ve elektrik altyapı tasarımı, hassas iklimlendirme, yangın algılama ve söndürme, yükseltilmiş zemin planlama, fiber ve bakır yapısal kablolama, ortam izleme sistemi, fiziksel güvenlik ekipmanları, altyapı yönetim sistemi, bina yönetim sistemi gibi bileşenlerden oluşmaktadır.

Veri merkezi bileşenleri Tablo 1'de yer alan aktif ve pasif bileşenlerden oluşmaktadır.

Tablo 1: Veri Merkezi Aktif ve Pasif Bileşenleri

Aktif Bileşenler	Pasif Bileşenler
● Sunucu sistemleri ● Veri Depolama ve Yedekleme Sistemleri ● Ağ sistemleri ● Ağ güvenlik sistemleri ● Uygulama Yazılımları ● Veri Merkezi Yönetim Sistemleri ● Veri merkezi ortam izleme sistemleri	● İklimlendirme Sistemleri ● Enerji Sistemleri ● Yangın Algılama ve Güvenlik Sistemleri ● Yükseltilmiş Zemin (Beyaz Alan) ● Yapısal Kablolama ● Sertifika ve Standartlar

Veri merkezleri mimari açıdan üç ayrı şekilde kurulabilmektedir. Fiziksel veri merkezleri, genellikle büyük ölçekli kurumların kendi fiziki ortamlarında kurdukları bir veri merkezi türüdür. Mobil veri merkezleri, ölçeğinden bağımsız olarak kritiklik ve risk unsurları göz önünde bulundurularak tercih edilebilecek yapılardır. Bu tür veri merkezleri yangın, sel ve deprem gibi afetlere karşı doğal bir koruma sağlamasının yanı sıra taşınabilme özelliğine de sahiptir. Ayrıca yer sıkıntısı yaşanması halinde bina harici konumlandırmaya da imkân vermektedir. Mikro veri merkezi, birkaç kabinetlik ihtiyaca sahip sistem odaları için değerlendirilebilecek küçük ölçekli veri merkezi türüdür. Özellikle pasif bileşen maliyetlerinin (yükseltilmiş zemin, hassas kontrollü iklimlendirme, kablolama, vb.) oldukça düşük olduğu bir veri merkezi türüdür.

Felaket kurtarma merkezi (FKM), ana veri merkeziyle bire-bir aynı bileşenlere, ancak çoğunlukla daha düşük kapasiteye sahip olan ikinci bir veri merkezidir. FKM, maliyetli bir çözüm olması nedeniyle genellikle büyük ölçekli kurumlar tarafından tercih edilmektedir. Ancak, FKM kurumlar arası karşılıklı işbirliği ile oluşturulabileceği gibi bulut hizmeti olarak da temin edilebilmektedir. Daha önceden belirlenmiş olan kritik sistemlerin bulunduğu FKM, aktif-pasif veya aktif-aktif kurulabilmektedir. Aktif-pasif kurulumda FKM, sadece bir felaket durumunda devreye alınır. Aktif-aktif kurulumda ise hem ana veri merkezi hem de FKM anlık olarak çalışmaya devam etmekte ve birbirleri arasında senkronize olmaktadır.

- **Veri merkezi türü, kuruluş ölçeğine ve çalıştırılan uygulamaların kritikliğine uygun olarak seçilmelidir.**

Tercih edilecek veri merkezi türünün belirlenmesinde ihtiyaç duyulan kabinet sayısı ile kabinetlerde yer alması planlanan cihazların sayısı ve türü önemli parametrelerdir. Az sayıda kabinet ihtiyacı için fiziksel veri merkezi kurulumunun uygun maliyetli bir çözüm olmayacağı hesaba katılmalı, alternatif veri merkezi türleri ve bulut hizmeti fayda-maliyet açısından incelenmelidir.

- **Veri merkezi ihtiyacının karşılanması amacıyla bulut sistemleri alternatif olarak değerlendirilmelidir.**

Günümüzde bulut sistemleri veri merkezi yatırımlarında önemli oranda maliyet avantajı sunabilmektedir. Kamu kurumları tarafından veri ve uygulamaları analiz edilerek bulutta hizmet verebilir nitelikteki veri ve uygulamalar ortaya konulmalıdır. Bu uygulamalar için yer kiralama yönteminden başlayarak servis olarak altyapı, yazılım veya platform seviyelerinde bulut hizmeti alımına varan veri merkezi yatırımları alternatif olarak incelenmelidir.

- **Felaket kurtarma merkezi kapsamında, kurumun uygulama bazında iş sürekliliği ve veri yedekleme politikaları belirlenmelidir.**

Felaket kurtarma merkezinin aktif-aktif veya aktif-pasif kurulum tercihinin belirlenmesinde iş sürekliliği ve yedekleme sistematiğinin kurgulanması gerekmektedir. Tüm verilerin transferinden ziyade kritiklik seviyesine göre uygulama bazında veri kaybı tahammül süreleri ve veri kaybı tahammül miktarına bağlı olarak veri transferi yapılacak uygulamalar belirlenmelidir. Belirlenen uygulamaların veri değişim miktarı, toplam kapasitesine bağlı olarak iş sürekliliği ve yedekleme politikaları belirlenmelidir. Kurumun kullandığı internet altyapısı ve bağlantı kapasitesi de iş sürekliliği ve yedekleme politikalarının oluşturulmasında ve felaket kurtarma merkezinin aktif-aktif veya aktif-pasif kurulum tercihinin belirlenmesinde önem arz etmektedir.

- **Kurumun uygulama bazında veri kaybı tahammül süreleri ve veri kaybı tahammül miktarı tespit edilmelidir.**

Felaket kurtarma merkezine aktarılacak uygulamalar ile uygulama verilerinin aktarım sıklığının öncelikli olarak belirlenmesi gerekmektedir. Tüm uygulamaların bütün verileriyle birlikte aynı sıklıkla aktarılması sürdürülebilirliği etkileyeceğinden tercih edilmemelidir. Uygulama ve veri aktarım sıklığı belirlenirken veri kaybı tahammül süreleri ve veri kaybı tahammül miktarı göz önünde bulundurulmalıdır. Belirlenen uygulamaların veri kapasiteleri ve veri aktarım sıklığına dikkat edilmek kaydıyla, belirlenen veri kaybı tahammül süreleri ve veri kaybı tahammül miktarı felaket kurtarma merkezinin aktif-aktif ya da aktif-pasif kurulum kararını belirleyecektir.

- **Kurumun uygulama bazında kritiklik seviyeleri ve sunduğu hizmetler kategorize edilmelidir.**

Felaket kurtarma merkezine tüm veriler tek bir politikayla aktarılmamalıdır. Veri merkezinden felaket kurtarma merkezine veri transferi uygulama bazında kritiklik seviyelerine göre planlanmalıdır. Bu transfer süreçleri, öncelik ve sıklık oranına göre kritik olan verilerin transferi önceliklendirilmek suretiyle planlanmalıdır. Görece daha az veri değişimi olan ve kritiklik seviyesi az olan uygulamaların aktarım sürecinin, kritik uygulamaların aktarım sürecini sekteye uğratmayacağından emin olunmalıdır.

Kontrol Listesi
Kurumun uygulama bazında veri kaybı tahammül süreleri ve veri kaybı tahammül miktarı tespit edildi mi?
Kurumun uygulama bazında kritiklik seviyeleri ve sunduğu hizmetler kategorize edildi mi?
Veri merkezi türünün seçiminde kuruluş ölçeği ve çalıştırılan uygulamaların kritikliği dikkate alındı mı?
Veri merkezi ihtiyacının karşılanması amacıyla bulut sistemleri fayda-maliyet açısından değerlendirildi mi?
Felaket kurtarma merkezinin kapasite planlaması kapsamında kurumun uygulama bazında iş sürekliliği ve veri yedekleme politikaları oluşturuldu mu?

7. BÖLÜM
UYGULAMA YAZILIMLARI

Kamu kurumlarında yazılım geliştirme veya temin süreçleri farklı yöntem ve yaklaşımlarla ele alınmaktadır. Bazı kurumlar yazılımcıları doğrudan istihdam ederken bazı kurumlarda yazılım ihtiyaçları anahtar teslimi hizmet alımı süreçleriyle giderilmektedir.

Kamu kurumlarında yazılım geliştirme süreçleri en genel anlamda beş farklı yöntemle yürütülmektedir.

Kadrolu personel kullanımı yoluyla yazılım geliştirme

Bu yönteme, kurumun kadrolu personel sayısı ve niteliği yeterli olduğu durumlarda başvurulmaktadır. Özellikle büyük ölçekli bilgi işlem birimlerinde, Hazine ve Maliye Bakanlığının onay vermesi halinde sözleşmeli bilişim personeli çalıştırılabilmektedir.

Hizmet alımı yoluyla yazılım geliştirme

Bu yöntemde yazılım ihtiyaçları genel hatlarıyla tanımlanarak ihaleye çıkılır ve ihaleyi alan yüklenici firmanın yazılımı geliştirerek teslim etmesi sağlanır.

Paket yazılım kullanımı

Çok sayıda kuruluşun benzer ihtiyaçlara sahip olduğu alanlarda paket yazılımlar mevcut olabilmektedir. Bu gibi genel konularda paket yazılım belirli bir süreyle lisanslanır ve lisans gideri temin edilir.

Uyarlama gereksinimli paket yazılım kullanımı

Bazı alanlarda kullanılan paket yazılımlar genel ihtiyaçlara cevap verebilecek nitelikte olmakla birlikte, kuruluşun özel ihtiyaçlarına uyarlanması için ilave yazılım geliştirilmesi gerekmektedir. Bu yazılım grubuna ilişkin en iyi örnek kurumsal kaynak yönetimi yazılımlarıdır.

Açık kaynak kodlu yazılım kullanımı

Paket yazılıma benzer şekilde, açık kaynak kodlu yazılım da çok sayıda kuruluşun benzer ihtiyaçları dolayısıyla ortaya çıkmıştır. Paket yazılımlara göre daha yüksek teknik birikim gerektirebilir. Ayrıca tercih edilecek açık kaynak kodlu yazılımın yaygın ve aktif kullanılıyor olması, geliştirici topluluğun büyüklüğü, dokümantasyon ve benzeri kaynakların yeterliliği, gerektiğinde ücretli destek alınabilecek kuruluşların varlığı gibi kriterleri taşıması gerekmektedir.

Yukarıda açıklanan alternatif yöntemler birbirinin her durumda ikamesi değildir. Alternatif yöntemlerin güçlü ve zayıf yanlarının bilinmesi, bir yandan doğru yöntemin seçimine yardımcı olurken diğer yandan seçilen yöntemin olumsuz etkilerinin azaltılmasında yol gösterici olacaktır.

- **Temin edilen veya geliştirilen yazılımın toplam sahip olma maliyeti dikkate alınmalıdır.**

Yazılımlarda toplam sahip olma maliyeti, ilk yatırım maliyetleri ve idame maliyetleri ile bunlardan kaynaklı diğer doğrudan maliyetlerin toplamı anlamına gelmektedir. Örneğin, kurumun kadrolu yazılım personeli ile geliştirilen bir yazılımda personel maaşları da toplam sahip olma maliyetine dâhildir. Diğer bir örnek olarak, yazılımın müteakip yıllardaki bakım maliyetleri ve paket yazılımlarda ilk lisans anlaşması süresinin ardından gelen lisans maliyetleri de toplam sahip olma maliyetine dâhildir. Fayda-maliyet oranı en yüksek yazılım yatırımının tespitinde karşılaştırmaların sağlıklı yapılabilmesi için bu ve benzeri maliyetler hesaba katılmalıdır. Gelişen teknolojinin yeni yazılım altyapı ve araçları gerektirmesi söz konusu olabilmektedir. Yazılımın hayata geçmesinin üzerinden belirli bir süre geçtikten sonra yazılımın güncel altyapılara göre yeniden yapılandırılması gerekebilecektir. Bu da toplam sahip olma maliyetinde dikkate alınması gereken bir husustur. Yazılım yeni teknolojilere göre güncellenmediğinde, eskimekte olan teknolojilerin idame maliyetleri ve personel temin süreçleri ciddi sorun haline gelmekte olup bu durum yazılımın sürdürülebilirliği açısından risk oluşturmaktadır.

- **Kritik nitelikteki yazılımlarda dışa bağımlılık azaltılmalıdır.**

Hizmet verememesi halinde ulusal ölçekte etkilere neden olacak olan yazılımlar ve veri gizliliği seviyesinin yüksek olduğu yazılımlar, kritik yazılım olarak düşünülebilir. Bununla birlikte kurumun ana faaliyetlerini yerine getirmesinde kullanılan yazılımlar da kurum ölçeğinde kritiklik arz edebilmektedir. Bu gibi yazılımlarda, tek bir yüklenici kuruluşa bağımlılık oluşmamasına yönelik tedbirler alınmalıdır. Projelerin hayata geçirilmesi amacıyla hizmet alınan yüklenici kuruluş ile kurum personeli arasında teknik birikim açısından bilgi asimetrisi oluşmaması sağlanmalı, kurumsal kapasite yetersiz ise, kapasitenin kademeli şekilde artırılabileceği bir yol haritası oluşturulmalıdır. Kapasite artırımının önemli bir unsuru, kurum personelinin hizmet alınan projelerde teknik görevler de dâhil olmak üzere daha aktif roller üstlenmesinin sağlanmasıdır.

- **İlgili tüm paydaşların yazılımın ihtiyaç analizi sürecine katılımı temin edilmelidir.**

Bazı durumlarda yazılım projeleri bir birimin motivasyonu ve iç dinamikleri sonucu ortaya çıkabilmektedir. Ancak yazılımlar sadece ilgili iç birimin iş süreçleri ile değil, aynı kurumun diğer birimleri veya diğer kamu kurumlarının iş süreçleri ile de ilişkili olabilmektedir. Bu nedenle, yazılımın ihtiyaç analizi sürecinde gerek diğer birimlerin, gerekse de ilgili diğer kuruluşların ihtiyaçlarının bütüncül olarak ele alınması gerekmektedir.

Kritik paydaşlar yazılımı kullanacak olan hedef kitle olabileceği gibi yazılımın kaynak kodunda küçük ölçekli revizyonlar yapılması halinde faydalanabilecek paydaşlar da olabilir. Kritik paydaşların sürecin başından itibaren katılımı, projeye yönelik sahiplenmeyi artıracaktır. Dolayısıyla, projeden beklenen potansiyel fayda da artmış olacaktır. Projenin potansiyel faydalanıcıları birden fazla ise, kurumlar arasında mükerrer uygulamalara sebebiyet verilmemesi, hali hazırda kurumların kendi içlerinde kullandıkları uygulamalar varsa öncelikli olarak bunların diğer paydaşlar tarafından da kullanılıp kullanılamayacağının incelenmesi uygun olacaktır. Eğer çok sayıda kamu kurumu tarafından kullanılma potansiyeline sahip bir yazılım ihtiyacı söz konusu ise, bu ihtiyacın ilgili alandaki ana sorumlu kuruluş tarafından giderilmesi, yatırımlarda etkinliği artıracak ve mükerrerliği önleyecektir.

- **Geliştirilen yazılımın son kullanıcı geri bildirimlerine göre periyodik olarak iyileştirilmesi sağlanmalıdır.**

Yazılımlar, yaşayan varlıklar olduklarından mütemadiyen iyileştirmeye ve ilave geliştirmelere ihtiyaç duyarlar. Yazılımın ihtiyaç analizi ve tasarım süreçlerinde son kullanıcıların periyodik geri bildirimleri alınmalıdır. Yazılımın kullanıcı ihtiyaçlarına tam olarak cevap verebiliyor olması ve kolay kullanılabilen arayüzlere sahip olması, ilerleyen süreçteki kullanıcı eğitimleri ihtiyacını azaltacaktır. Yazılım yaşam döngüsünün ileri aşamalarında, kullanıcılara yönelik periyodik memnuniyet anketleri yapılması halinde yazılımın aksayan yönleri ve yeni fonksiyonel özellik ihtiyaçları daha kolay tespit edilebilecektir. Bu tür geri bildirimler yazılımın müteakip fazlarında yol gösterici olacaktır.

- **Performans analizleri yapılarak yazılımın ihtiyaç duyacağı sistem kaynakları optimize edilmelidir.**

Yazılım projelerinde gerekli sunucu altyapısına ilişkin tahminler yürütülerek gerekli altyapı bu tahminler doğrultusunda temin edilir. Geniş ölçekli projelerde, projenin yaygınlaşma safhası öncesinde pilot uygulama yapılacaksa, sunucu altyapısı pilot uygulamaya göre belirlenmeli ve yaygınlaşma aşamasında pilot uygulamada ortaya çıkan gereksinimler dikkate alınmalıdır.

Yazılımın yaygınlaşması ve zaman içinde ilave modüller eklenmesi sebebiyle sunucu kaynakları yetersiz hale gelebilir. Bu durumda genellikle ilk tercih olarak sistem kaynaklarının artırılması gündeme gelmektedir. Ancak kaynakların artırılması yoluna gidilmeden önce performansı artırıcı tedbirlere başvurularak mevcut sistem kaynaklarının daha verimli kullanılmasının yolları araştırılmalıdır.

- **Kurumsal yazılımlar birbiriyle entegre çalışacak şekilde tasarlanmalıdır.**

Kurumsal uygulamalar temelde üç katmanlı olarak düşünülmelidir:

1. Altyapı katmanı: Bu katmanda, tüm kurumsal uygulamalarda ortak olan unsurlar barındırılır. Bu katmana sunucu altyapısı dâhil olduğu gibi, uygulamalar arasında ortak kullanılan yazılım bileşenleri de dâhildir.

2. Ara katman: Altyapı katmanı ile uygulama katmanı arasındaki kimlik doğrulama ve yetki kontrollerini yapan, yapılan tüm işlemlerin kayıt altına alınmasını sağlayan katmandır. Altyapı katmanı ile uygulama katmanı arasındaki tüm veri akışları ara katman üzerinden geçmektedir

3. Uygulama katmanı: Altyapı katmanının üzerinde çalışan uygulamalar bu katmanda yer almaktadır.

Yazılımlar, kurumsal süreçlerin yürütülmesi amacıyla uygulamaya konan araçlardır. Çoğu durumda bir kurumsal sürecin işletilmesi, birden fazla yazılımın entegre çalışmasını veya yazılımlar arasında bilgi alışverişini zorunlu kılar. Dolayısıyla, geliştirilen yazılımların bir bütünü tamamlayacak unsurlar olarak tasarlanması önem taşımaktadır. İdeal durumda, kurum personelinin kullanıcı dostu arayüzler üzerinden mantıksal benzeşen ekranlar üzerinden işlemler yaparak kurumsal süreçlerin birçoğunu yürütebilmesi önem taşımaktadır. Bunun sağlanabilmesi için kullanıcının tek bir ana ekrandan yapacağı işlemlerle ilgili öne çıkan bütün bilgilere ulaşabilmesi, alması gereken aksiyonları bu ekrandan başlatabilmesi ve sürecin devamı için ilgili uygulamaya yönlendirilebilmesi uygun bir sistem tasarımı olacaktır.

Değişkenlik göstermekle birlikte, genellikle yazılım kaynak kodlarının çoğunluğu uygulama içerisinde, hatta farklı uygulamalar arasında ortak şekilde kullanılabilecek niteliktedir. Kullanıcı yönetimi, yetkilendirme, raporlama, günlük kayıtlarının tutulması ve güvenli erişim gibi çok sayıda yazılım modülü bu kapsamda sayılabilir. Uygulamaların yeniden paylaşılabilir kısmının kuruluş genelinde ortak bir anlayışla geliştirilmesi ve mümkünse tek bir merkezi noktadan diğer uygulamalara hizmet olarak sunulması, hem yönetilmesi gerekli kod miktarını azaltacak, hem de yeni uygulamalarda esneklik ve hız sağlayacaktır. Ayrıca yazılımın yeniden yazılması gerektiğinde bir yazılım katmanında yapılacak yazılımsal değişiklikler diğer katmanları etkilemeyeceğinden, güncelleme ve altyapı değişiklikleri kolaylaşacaktır.

- **Bilgi işlem biriminin, diğer birimlerin proje planlama süreçlerine aktif katılımı sağlanmalıdır.**

Kamu kurumları arasında tüm bilişim altyapısını merkezi bir bilgi işlem birimi aracılığıyla yöneten kurumlar olduğu gibi, kurum genelinde birden fazla bağımsız sunucu altyapısının mevcut olduğu örneklere de rastlanmaktadır. Kamu kaynaklarında verimliliğin sağlanabilmesi için, sunucu altyapısının merkezi bilgi işlem birimi tarafından bütüncül bir şekilde yönetilmesi önem arz etmektedir. Ancak bilgi işlem biriminin sorumluluk alanı bununla sınırlı kalmamalıdır.

Yazılımların kurum genelinde bütüncül bir yapıda sürdürülebilmesi, merkezi bilgi işlem biriminin diğer birimlerin sahipliğindeki yazılımlara belirli ölçüde nüfuzunu gerektirmektedir. Kurumsal bilgi teknolojileri altyapısı ne kadar ortak ve standart olursa idamesi de o denli kolay

ve düşük maliyetli olmaktadır. Bu husus yüklenici kuruluşa bağımlılık oluşmasının da belirli ölçüde önüne geçebilir.

Kurumsal yazılımlar idame sürecinde bilgi işlem birimine devredilecek unsurlar olarak düşünülmemeli, bilgi işlem biriminin sürece başından itibaren dâhil olması sağlanmalıdır. Böylece, bilgi teknolojileri politikaları, kurumsal uygulamaların bütünü dikkate alınarak daha geniş bir perspektifle ve bütüncül olarak işletilebilecektir.

- **Yazılım güvenliği, yazılım geliştirme sürecinin başından itibaren ele alınmalıdır.**

Yazılım projelerinde yazılımın işlevselliği daha görünür olduğu ve eksikliği anında hissedilebildiği için proje planlamasında öncelikli görülebilmektedir. Ancak yazılım güvenliği, yazılım geliştirildikten sonra gündeme alınabilecek bir konu değildir; yazılımın ihtiyaç analizi ve tasarım sürecinden itibaren güvenlikle ilgili hususlar planlamaya dâhil edilmelidir. Bu kapsamda, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanmış olan Bilgi ve İletişim Güvenliği Rehberi'nde yer alan hususlar dikkatle takip edilmeli ve uygulanmalıdır. TÜBİTAK BİLGEM tarafından yayınlanan Güvenli Yazılım Geliştirme Kılavuzunun güncel sürümüne uyum sağlanması gerekmektedir. Ayrıca web tabanlı uygulamaların güvenliği için OWASP gibi uluslararası standartların dikkate alınması da önem taşımaktadır. Kurumsal bilgi güvenliği, tüm katmanlarda bütüncül bir bakış açısı gerektirmektedir. Bu nedenle yazılım güvenliği kurumsal bilgi güvenliğinin diğer katmanlarıyla bütün olarak düşünülmeli, diğer güvenlik önlemlerini tamamlamasına dikkat edilmelidir. Yazılım testlerine özellikle önem verilmeli, testlerin yazılımların yaşam döngüsünün ayrılmaz bir parçası olacağı bir sistematik oluşturulmalıdır.

- **Mümkün olan hallerde yeni teknoloji ve yaklaşımlar benimsenmelidir.**

Yeni teknolojiler pek çok avantajının yanı sıra mevcut teknik altyapının daha etkin kullanımına da imkân vermektedir. Yazılım teknolojisinin gelişimiyle birlikte uygulamalar daha dinamik hale gelmekte, uygulama içi sayfa güncellemeleri için sayfanın tümünün yenilenmesi yerine sadece ilgili veri alanlarının güncellenmesine imkân veren yazılım kütüphaneleri yaygınlaşmaktadır. Öte yandan, düşük kodlu ya da kodsuz platformlar da yaygınlaşmaya başlamıştır. Bu platformlar yazılımların süreç temelinde hayata geçirilebilmesine imkân vererek süreç içerisindeki değişikliklerin kaynak kodunda değişiklik yapılmadan hayata geçirilmesini mümkün kılmaktadır. Özellikle sık mevzuat değişikliklerinden etkilenen uygulamalarda bu tür yeni yaklaşımlar esneklik sağlamaktadır.

Yazılım teknolojileri alanında diğer bir gelişen alan DevOps yaklaşımı ve mikro servis mimarilerdir. Bu kapsama giren yöntem ve araçlar, yazılımların test süreçleriyle birlikte büyük oranda otomatize ve çevik bir şekilde güncellenebilmesine imkân sağlamaktadır. Bilgi işlem birimlerinin bu tür yaklaşım ve araçlara aşinalık kazanması ve zaman içinde birim kültürünün bir parçası haline getirmeleri önem taşımaktadır. İlk etapta küçük ölçekli projelerde hayata geçirilebilecek yenilikçi yaklaşımlar zaman içinde kuruluş geneline yaygınlaştırılmalıdır.

- **Yazılımlar işletim sistemi ve tarayıcı bağımsız yapıda geliştirilmelidir.**

Kuruluşa özel geliştirilecek yeni yazılımlarda ve mevcut olan yazılımların güncel teknolojilerle yenilenmesi süreçlerinde yazılımın işletim sistemi ve internet tarayıcıdan

bağımsız olarak geliştirilmesine özellikle dikkat edilmelidir. Diğer bir deyişle, yazılım yaygın olan tüm işletim sistemlerinde ve internet tarayıcılarında aynı performans ve özelliklerde çalışabilmelidir.

Kontrol Listesi
Geliştirilecek yazılım projelerinin seçiminde toplam sahip olma maliyetini dikkate alan bir sistematik takip ediliyor mu?
Kritik nitelikteki yazılımların idamesi için kurumsal kapasitenin geliştirilmesine yönelik bir yol haritası mevcut mu?
Yazılım projelerinin planlama sürecinde kritik paydaşların tespiti bütüncül şekilde yapıldı mı? Bu paydaşların ihtiyaçları proje kapsamına dâhil edildi mi?
Çok sayıda kamu kurumunun doğrudan faydalanıcısı olabileceği nitelikte projelere ilişkin olarak merkezi koordinasyon kurumlarıyla irtibat sağlandı mı?
Hayata geçirilen ve idame edilen yazılım projelerinde son kullanıcıların geri bildirimlerinin periyodik olarak alınabileceği sistematik bir mekanizma mevcut mu?
Kurumsal yazılımların performans analizleri yapılarak mevcut sunucu altyapısından daha etkin faydalanılması sağlanıyor mu?
Kurumsal yazılımların bütüncüllüğü ve entegrasyonuna yönelik bir planlama yapılıyor mu?
Yazılımlarda ortak kullanılan bileşenlerin paylaşımı ve yeniden kullanımı imkânı varsa bu imkândan faydalanılıyor mu?
Merkezi bilgi işlem birimi kurum genelinde yürütülen bütün yazılım projelerine aktif katılım sağlıyor mu?
Yazılım projelerinin planlama sürecinin başlangıcından itibaren bilgi güvenliğine ilişkin hususlar adresleniyor mu?
Yazılım projelerinde yeni teknoloji, araç ve yaklaşımların kullanımı fayda-maliyet açısından inceleniyor mu? Bu teknolojilerin bilgi işlem kültürünün parçası haline gelmesi için bir yol haritası mevcut mu?

EK: TEHDİT – ETKİ DEĞERLERİ TABLOSU

Etki Değeri Tanımı	Gizlilik	Bütünlük	Erişilebilirlik
Çok Yüksek	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %20'den fazlası şikâyetçi olur.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. Kurum operasyonları ilgili varlığa ulaşılamadığı için gerçekleştirilemez veya 1 günden uzun bir süre sekteye uğrar.
Yüksek	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %20'si şikâyetçi olur.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Kurumun operasyonlarında yaşanan kesinti 12 saat ile 1 gün arasında olur. Kurumun operasyonlarının durmasından dolayı, itibarı negatif etkilenir ve uzun vadede kapatılması zor problem oluşur.
Orta	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritiklik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %10'u şikâyetçi olur.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Kurumun operasyonlarında yaşanan kesinti 8 saat ile 12 saat arasında olur. Kısa vadede itibar kaybı olsa da kurumun operasyonları devam eder.
Düşük	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritiklik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu çok az etkiler. Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %5'i şikâyetçi olur.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi kurumu çok az etkiler. Kurumun operasyonlarında yaşanan kesinti yarım saatin üzerindedir ancak 8 saati geçmez ve etkileri çok yüksek değildir.
Çok Düşük	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritiklik seviyesi altındaki bilgi kurumu hiç etkilemez veya etkisi göz ardı edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritiklik seviyesi altındaki bilgi kurumu hiç etkilemez veya etkisi göz ardı edilebilir. Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %1'i şikâyetçi olur veya hiç şikâyet yaşanmaz.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi kurumu hiç etkilemez veya etkisi göz ardı edilebilir. Kurumun operasyonlarında kesinti yaşanmaz veya yaşanan kesinti en fazla yarım saatliktir.

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
STRATEJİ VE BÜTÇE BAŞKANLIĞI

YÖNETİM HİZMETLERİ GENEL MÜDÜRLÜĞÜ
BİLGİ VE BELGE YÖNETİMİ DAİRESİ BAŞKANLIĞI
Temmuz 2022

Necatibey Cad. No: 110/A 06570 Yücetepe - ANKARA
Tel: +90 (312) 294 50 00 • Faks: +90 (312) 294 52 98

STRATEJİ VE BÜTÇE BAŞKANLIĞI YAYINLARI BEDELSİZDİR, SATILAMAZ.