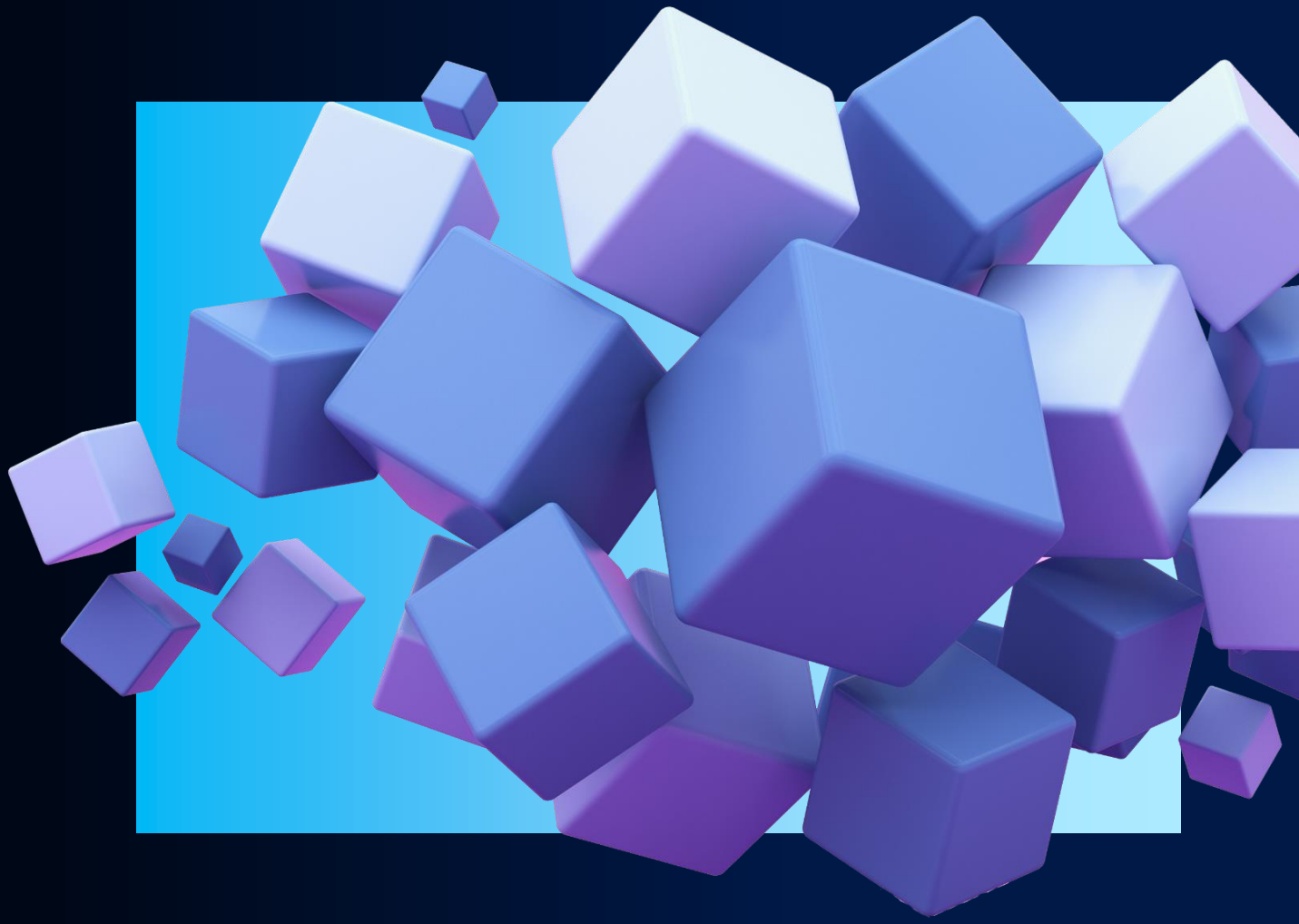
KPMG Türkiye

SAP Siber Güvenlik Hizmet Yaklaşımı



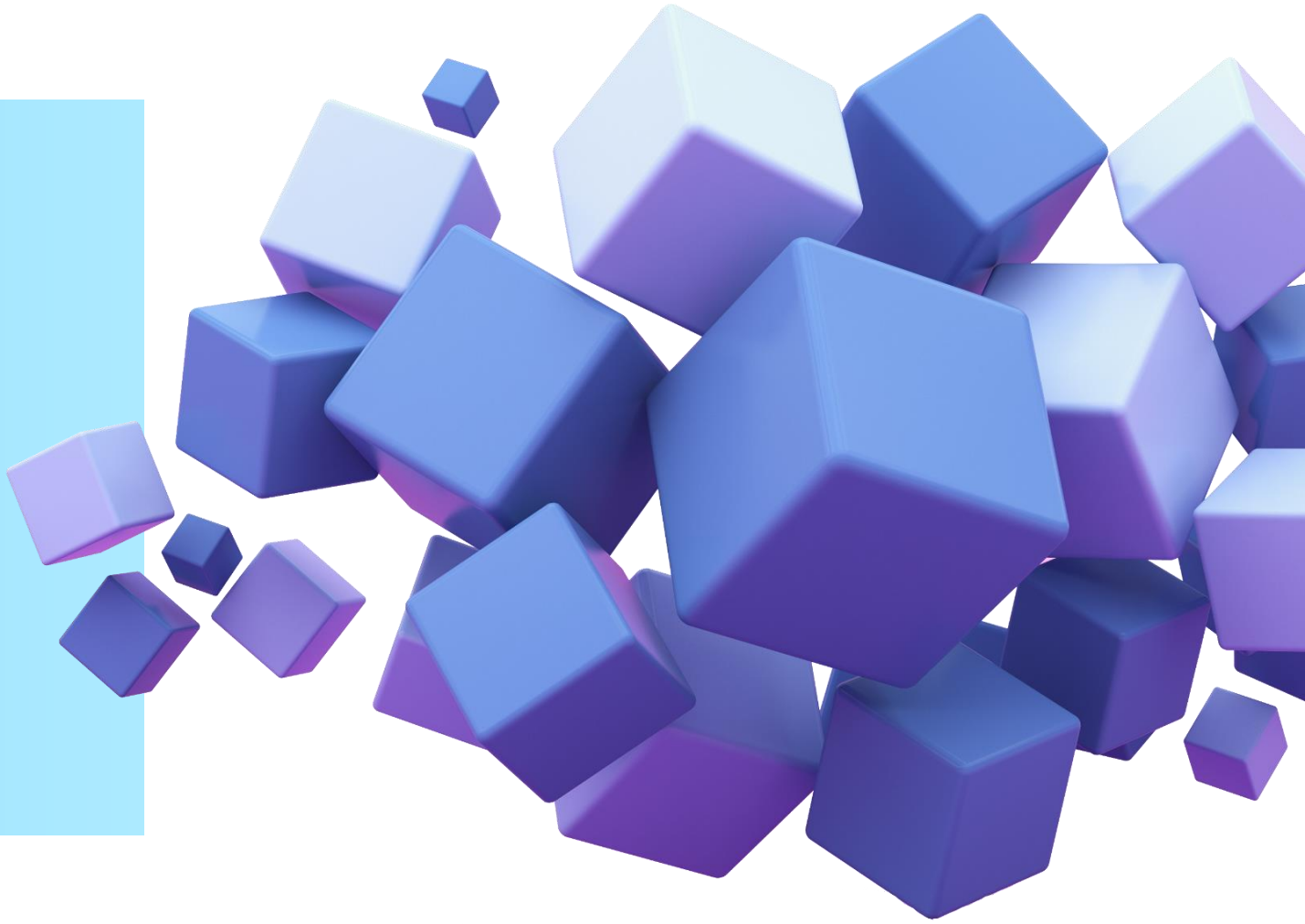
Siber Güvenlik Hizmetlerimiz

İçerik

01 SAP Ortamı Güvenliğine Genel Bakış 03

02 KPMG SAP Siber Güvenlik Yaklaşımı 05

03 SAP Siber Güvenlik Hizmetlerimiz 15



© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

SAP Ortamı Güvenliğine Genel Bakış

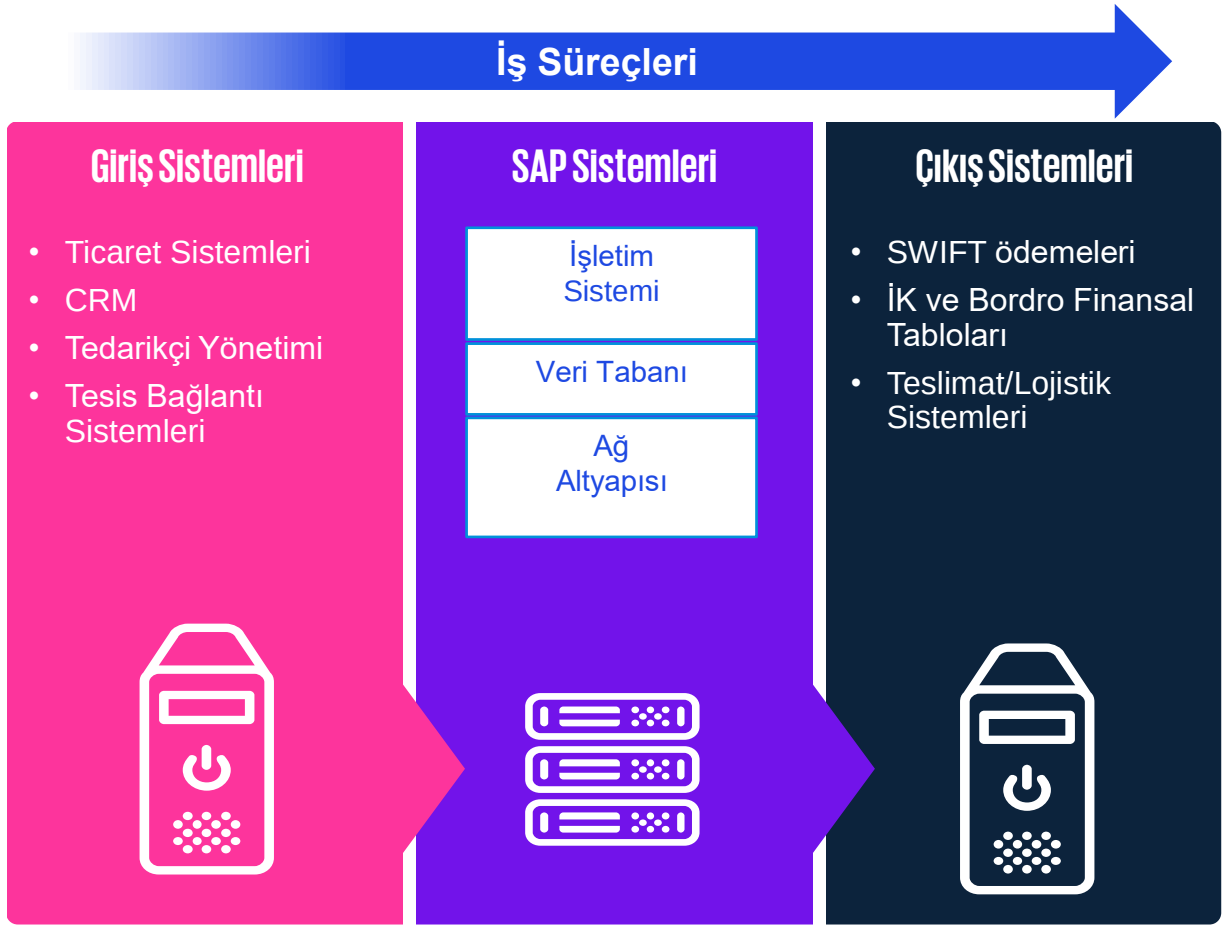
01

SAP Siber Güvenlik Hizmet Yaklaşımı

SAP Ortamına Genel Bakış

SAP ortamı; giriş/çıkış sistemleri (non-SAP sistemler), iş süreçleri ve bu iş süreçlerini kolaylaştıran çekirdek altyapıdan oluşan kompleks bir sistemdir. Bu sistem işletim sistemleri, veritabanları, SAP ya da non-SAP ara yüzler ve diğer özel amaçlı araçlar ile desteklenmektedir. SAP altyapısına girdi veren, ondan çıktı alan veya işlemleri kolaylaştıran teknoloji ve iş süreçlerinin tamamına SAP ortamı denilmektedir.

Bu bileşenlerin herhangi birinde güvenlik zafiyeti olması durumunda, siber saldırganların yasa dışı ödemeler yapması, üretimi aksatması, kişisel bilgileri çalması ve/veya paralelinde SAP ortamlarında bir ihlal durumunun oluşması söz konusu olabilir. Bu sebeple tüm SAP ortamlarını güvence altına almak için kapsamlı bir siber güvenlik yaklaşımı benimsenmelidir.



© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG SAP Siber Güvenlik Yaklaşımı

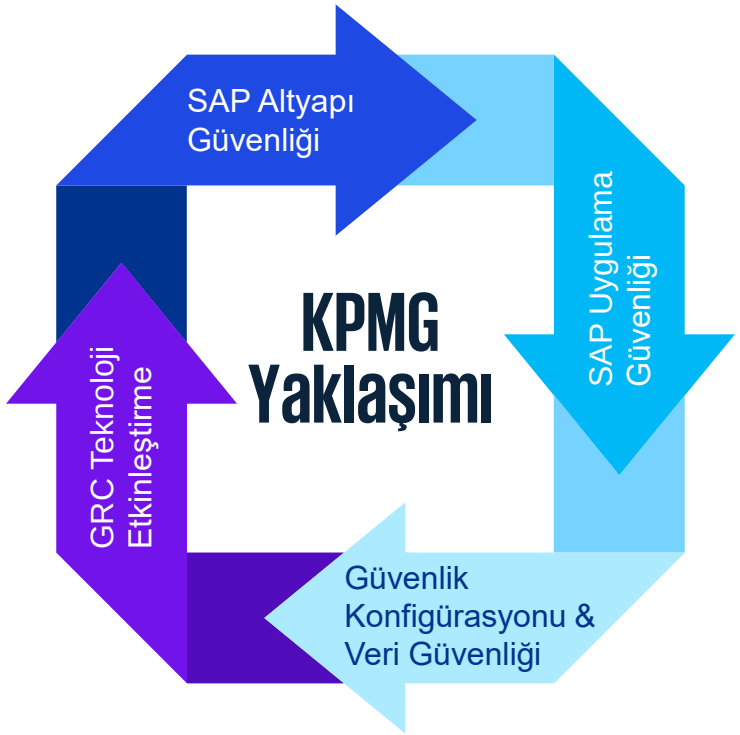
02

SAP Siber Güvenlik Hizmet Yaklaşımı

KPMG SAP Siber Güvenlik Yaklaşımı

1. Altyapı Güvenliği

- SAP uygulama ve veritabanı sunucu güvenliği (sıkılaştırma, CIS benchmarkları)
- SAP router, diğer web uygulamaları vb. entegrasyon güvenliği (ör: OWASP Top 10)
- Network segmentasyonu ve trafik güvenliği (ör: kriptolama vs.)



2. Uygulama Güvenliği

- Kullanıcı yönetimi (kritik profil, rol, yetki) tasarımı
- Versiyon ve yama yönetimi
- Sistem logları yönetimi
- Uyarlama ve geliştirme süreçleri güvenliği (standart ve standart dışı uyarlama, geliştirme ve müdahale yöntemleri)

4. GRC Teknoloji Etkinleştirme

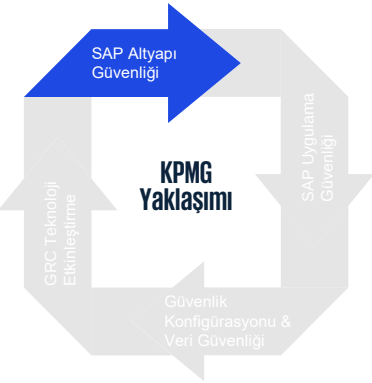
- Kimlik doğrulama, yetkilendirme ve erişim yönetimi süreçleri ve otomasyonu güvenliği

3. Güvenlik Konfigürasyonu & Veri Güvenliği

- Standart güvenlik parametreleri (SAP, ISACA vb. kılavuzları eşliğinde) ve yapılandırması
- SAP veri güvenliği yönetimi

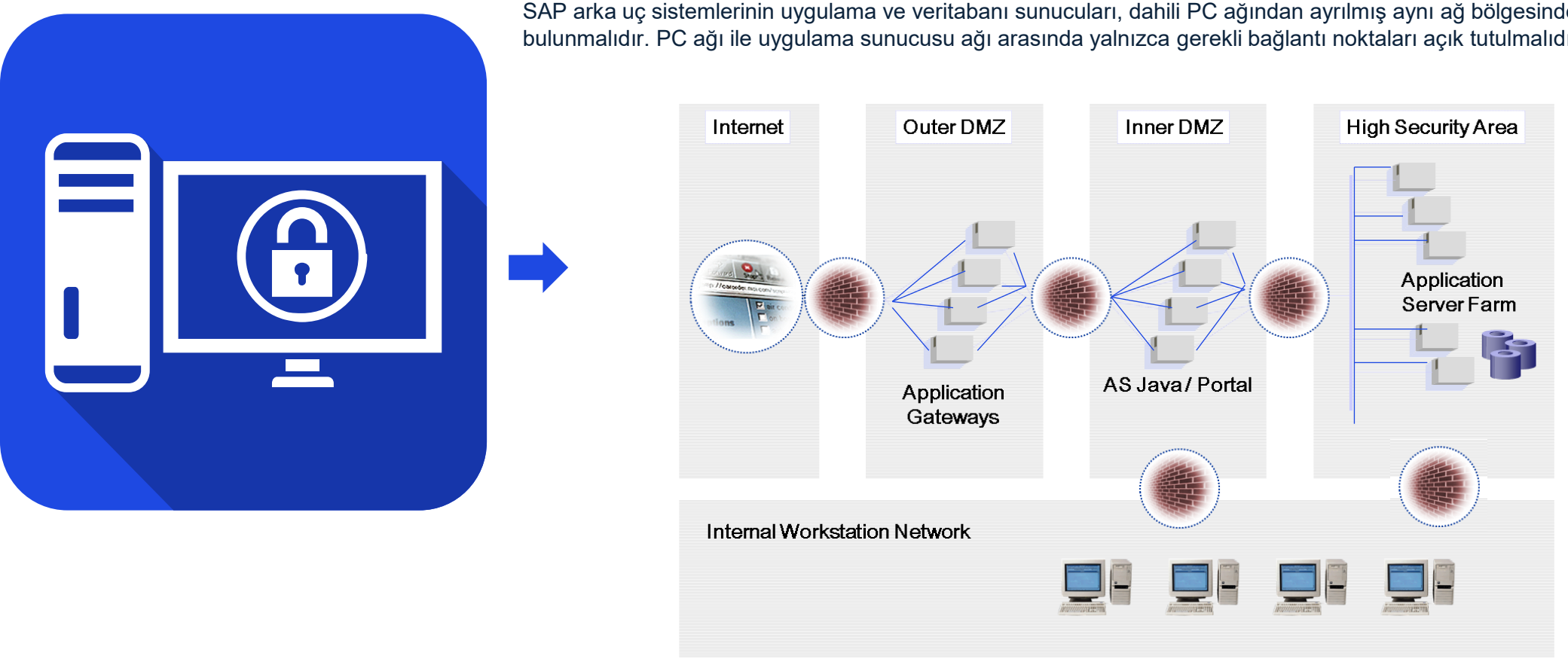
© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

1. SAP Altyapı Güvenliği



SAP sistemlerinin güvenliğini sağlamak için aşağıdaki gibi bir ağ altyapısı önerilir:

SAP arka uç sistemlerinin uygulama ve veritabanı sunucuları, dahili PC ağından ayrılmış aynı ağ bölgesinde bulunmalıdır. PC ağı ile uygulama sunucusu ağı arasında yalnızca gerekli bağlantı noktaları açık tutulmalıdır.



© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2. SAP Uygulama Güvenliği

S/4 HANA, iş süreçlerini desteklemek için dağıtılmış, esnek bir şekilde entegre edilmiş uygulamaların çoğalmasıyla ortaya çıkmıştır. Bu durum, risk profilini yükseltmiş ve son kullanıcıların güvenlik risklerini artırmıştır. Birçok kuruluş, bu sebepten ötürü tekli oturum açma (single-sign-on) hedeflerini desteklemekte zorlanmakta ve uygulama rollerini iş süreçleriyle uyumlu hale getirmede başarısız olabilmektedir.

Uygulama Güvenliği modeli, iş süreçleriyle doğrudan uyumlu ve önceden belirlenmiş rol tanımlarından yararlanır. Önceden tanımlanmış roller, veri güvenliği ile kullanıcı erişim yönetimi riskleri ve görevler ayrılığı (SOD) gibi uyumluluk gereksinimlerini ele alacak şekilde tasarlanmıştır.

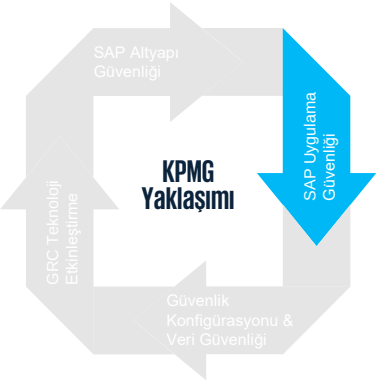
01 Uygulama Rolleri / Rol Tabanlı Erişim Kontrolü (RBAC)

02 Kullanıcı Yaşam Döngüsü Yönetimi

03 Görevler Ayrılığı (SoD)

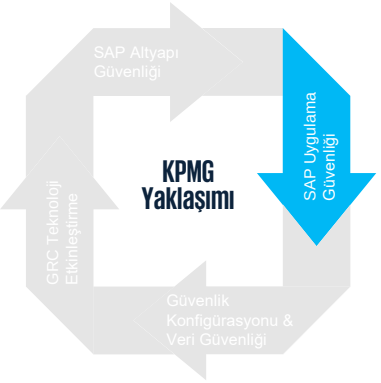
04 SAP Fiori

05 Nitelik/Özellik Tabanlı Erişim Kontrolü (ABAC)



© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2. SAP Uygulama Güvenliği (Tasarım)



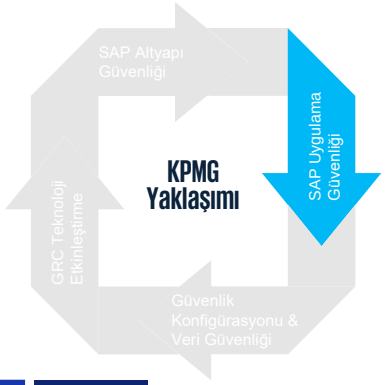
Bir SAP uygulama güvenliği tasarımının hedefi, ölçülebilir, sürdürülebilir ve görevler ayrılığı ihlali içermeyen bir mimari altyapıyı devreye almaktır.

Bu tasarımın temel özellikleri aşağıdakileri içermektedir:

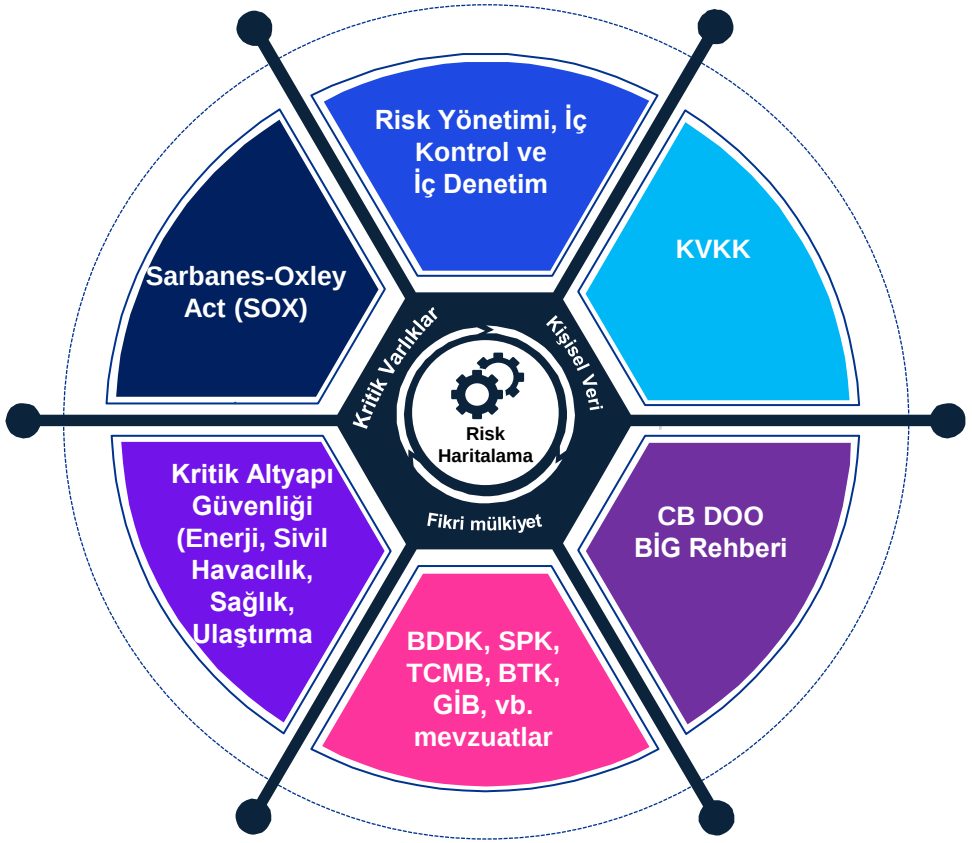
- Tek bir güvenlik mimarisinden yararlanma
- Rollerin doğası gereği risk içermemesi (rol düzeyinde sıfır SoD)
- Kritik veya hassas işlem erişimine sahip rollerin, günlük/rutin son kullanıcı rollerinden ayrılması
- Roller arasında minimum sayıda işlem tekrarı
- Son kullanıcılara, gereğinden fazla erişim sağlanması riskini sınırlayan minimum sayıda rolün verilmesi
- Rollerin, sahip oldukları görev işlevleriyle hizalanması / uyumlu olması

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2. SAP Uygulama Güvenliği
Risklerin Analiz Edilmesi



Etkiler (Düzenleyici ve Kurumsal) | Zafiyetler | Varlıklar | Aksiyonlar



Hizmetler, İşlevler, Süreçler	Record to Report Purchase to Pay Order to Cash Hire to Retire vb.
Teknoloji	SAP ECC, BCP, CRM, SRM, S/4HANA Central Finance, Salesforce, Hybris, Workday vb.
Sistemler	HANA, Mobil, Bulut

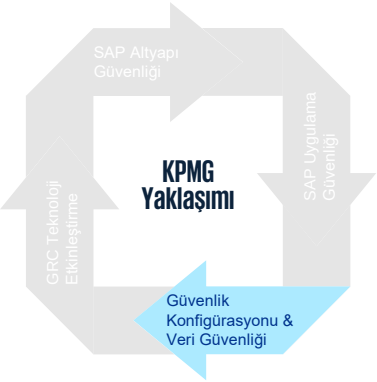
Yönetişim ve Kontroller

Organizasyon, İnsan Faktörü, Beceriler Kritik Varlıklar

Bilgi ve Performans
Verilerin yönetilmesi ve performansın ölçülmesi

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

3. Güvenlik Konfigürasyonu ve Veri Güvenliği



SAP Güvenlik Konfigürasyonu ve Veri Güvenliği çözümleri, kuruluşların uygulama portföyleriyle ilişkili yönetişim, risk ve uyumluluk gereksinimlerini yönetmeleri için operasyonel bir temel sağlar. Bu yaklaşımın temel odak noktası, bir kuruluşun Siber Güvenlik ve Veri Güvenliği programlarının sürdürülebilirliğini, otomasyonunu, etkinliğini, verimliliğini ve şeffaflığını geliştirmeye yardımcı olmak ve operasyonları SAP ortamında genişletmektir.

01 SAP Yönetişimi

02 SAP Konfigürasyon Yönetimi

03 SAP Kritik Fonksiyonlar

04 SAP Teknoloji Ortamı

05 Veri Gizliliği ve Bütünlüğü

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

3. Güvenlik Konfigürasyonu ve Veri Güvenliği (Tasarım)

SAP ortamları, giderek daha fazla verinin bulutta depolanması ve 3. taraflarca doğrudan erişilebilir hale gelmesiyle her geçen gün gelişmektedir.

Kuruluşların, SAP siber güvenlik yaklaşımlarının olgunluk seviyesini dört temel boyutta inceleyebilmesi mümkündür.

SAP ortamını korumaya yönelik bu entegre yaklaşım, Derinlemesine Savunma (Defense in Depth) ilkesine dayanmaktadır.

SAP Yönetişimi

- Yönetişim Stratejisi
- Kritik Veri Koruması
- 3. Taraf Riskleri
- Risk ve Uyumluluk
- SAP GRC

SAP Konfigürasyon Yönetimi

- Taşıma (Transport) Yönetimi
- SAP Yama Yönetimi
- Konfigürasyon Yönetimi
- Kod Güvenliği ve Testi

SAP Teknoloji Ortamı

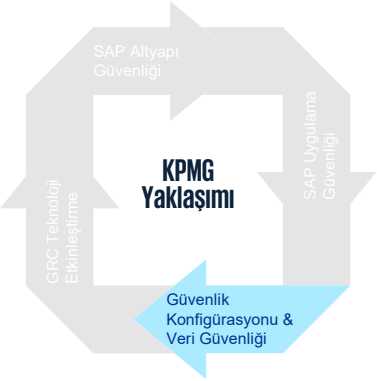
- SAP Ağ Güvenliği
- Veritabanı ve İşletim Sistemi Güvenliği
- SAP İletişim Protokolleri
- Log Kaydetme ve İzleme

SAP Kritik Fonksiyonlar

- Kullanıcı Yönetimi
- Şifre Yapılandırması
- Acil Erişim
- Hassas İşlem Kodlara Erişim
- Tabloların Oluşturulması

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

3. Güvenlik Konfigürasyonu ve Veri Güvenliği (Tasarım)
Veri Güvenliği



Veri Güvenliği	Erişim Rolleri	Kontroller	Şifreleme	Redaksiyon	Maskeleme	Veri Yönetişimi

Veri Şeffaflığı

Ortak bulutta veri erişimini, depolamayı, taşımayı, işlemeyi ve konumu izleyin ve raporlayın

Veri Kontrolü

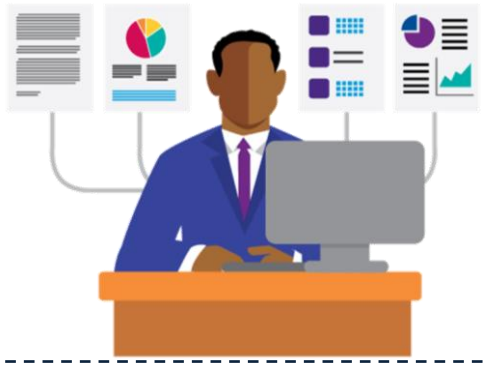
Ortak bulut veri erişimi, konum, hareket ve işleme ilkeleri oluşturun ve uygulayın

Anahtar Yönetim Hizmeti

Küresel olarak dağıtılmış, buluttan bağımsız anahtar yönetimi SaaS

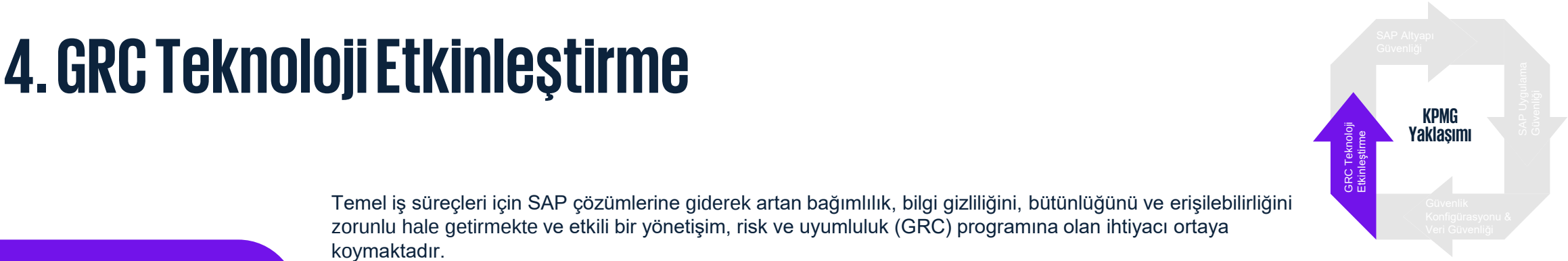
Veri Yönetişimi

- Veri Hijyeni
- Veri Sınıflandırması
- Veri Arşivleme ve Silme
- Gözetim Zinciri
- Erişim Takibi
- İndirme Takibi



© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

4. GRC Teknoloji Etkinleştirme



Temel iş süreçleri için SAP çözümlerine giderek artan bağımlılık, bilgi gizliliğini, bütünlüğünü ve erişilebilirliğini zorunlu hale getirmekte ve etkili bir yönetişim, risk ve uyumluluk (GRC) programına olan ihtiyacı ortaya koymaktadır.

Kuruluşlar, bir yandan işlem riskini yöneten ve düzenleyici gerekliliklere uyan bir iç kontrol ortamında çalışırken, diğer yandan SAP teknolojisine yaptıkları büyük yatırımlardan daha fazla fayda sağlamaya çalışıyor. Kuruluşların, GRC teknolojisinin entegrasyonu yoluyla otomasyondan yararlanarak bu dengeyi sağlaması ve operasyonel verimliliklerini artırabilmesi mümkündür.

01 Erişim Yönetişimi

02 Kurumsal Risk ve Uyum

03 Siber Güvenlik ve Veri Koruma

04 Risk Analitiği

05 Sürekli Kontrol İzleme

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

SAP Siber Güvenlik Hizmetlerimiz

03

SAP Siber Güvenlik Hizmet Yaklaşımı

Nasıl Yardımcı Olabiliriz?
Örnek bir çalışma kapsamı

SAP BASIS sistemi güvenlik yapılandırmasının değerlendirilmesi

- Standart güvenlik parametreleri (SAP, ISACA vb. kılavuzları eşliğinde) ve yapılandırması
- Kimlik doğrulama, yetkilendirme ve erişim yönetimi süreçleri ve otomasyonu güvenliği (varsa GRC dahil)
- Yüksek yetkili kullanıcılar, kritik işlem kodlarına yetkili kullanıcılar
- Kullanıcı yönetimi (kritik profil, rol, yetki objeleri yapısı) tasarımı
- Versiyon ve yama yönetimi
- Sistem logları yönetimi

Uygulama ve geliştirme güvenliği

- Canlı sisteme erişim ve değişiklik yetkileri
- Geliştirme-test-canlı sistem yetkileri
- Uyarlama ve geliştirme süreçleri güvenliği (standart ve standart dışı uyarlama, geliştirme ve müdahale yöntemleri)
- SAP mesaj, RFC ve gateway entegrasyon güvenliği
- Kritik tablolar loglama ve erişim güvenliği (sistem tabloları, default ve custom programlar)
- Uyarlama ve geliştirme log yönetimi ve güvenliği
- Görevler ayrılığı analizi

SAP ortamı (landscape) güvenliği

- SAP uygulama ve veritabanı sunucu güvenliği (sıkılaştırma, CIS benchmarkları)
- SAP router, diğer web uygulamaları vs. entegrasyonu güvenliği (ör: OWASP Top 10)
- Network segmentasyonu ve trafik güvenliği (ör: kriptolama vs.)

SAP veri güvenliği

- SAP üzerinde işlenen veri envanteri değerlendirme, veri sınıflandırma ve güvenlik önlemleri eşleştirmesi (varsa)
- KVKK/GDPR için alınan önlemlerin değerlendirilmesi

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Nasıl Yardımcı Olabiliriz?
Örnek bir çalışma yaklaşımı

Değerlendirme Yöntemimiz

- Gözlem, kanıt inceleme, yeniden gerçekleştirme, konfigürasyon inceleme, sızma testi teknikleri
- Her bir SAP instance için ayrı inceleme
- Network, entegrasyon, sunucu ve veritabanı gibi ortam incelemeleri
- SAP ortamlarının DEV/TEST/PROD ortamlarının her biri için uygulanabilir olan kontrollerin değerlendirilmesi

Kılavuz ve Standartlar

- SAP güvenlik kılavuzları
- ISACA SAP güvenlik & denetim kılavuzları
- OWASP Top 10 (web uygulama/servis ortamları için)
- KVKK/GDPR (kişisel veri güvenliği için)
- CB DDO BİG Rehberi (uygulama ve sistem güvenlik sıkılaştırma maddeleri için)
- CIS benchmark'ları (sunucu, veritabanı vb. güvenliği için)

Çalışma çıktıları

01 **Bulgu ve zafiyetlerin tespit edilmesi**

02 **İyileştirilmesi gereken noktaların belirlenmesi**

03 **Önerilerin ve iyileştirme yol haritasının oluşturulması**

04 **İyileştirme ve GRC desteği sağlanması**

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

İletişim

Ümit Şen

Şirket Ortağı

Siber Güvenlik Hizmetleri Lideri

M +90 532 387 40 38
E umitsen@kpmg.com

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2023 KPMG Yönetim Danışmanlığı A.Ş., a Turkish Corporation and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Detaylı bilgi için:

KPMG Türkiye Clients & Markets: **tr-fmmarkets@kpmg.com**

İstanbul: İş Kuleleri Kule 3 Kat 1-9 34330 Levent İstanbul T : +90 212 316 6000

Ankara: The Paragon İş Merkezi Kızılırmak Mah. Ufuk Üniversitesi Cad. 1445 Sok. No:2 Kat:13 Çukurambar 06550 Ankara T: +90 312 491 7231

İzmir: Folkart Towers Adalet Mah. Manas Bulvarı No:39 B Kule Kat: 35 Bayraklı 35530 İzmir T : +90 232 464 2045

Bursa: Odunluk Mahallesi, Liman Caddesi, Efe Towers, No:11/B, 9-10 Nilüfer / Bursa T : +90 232 464 2045

kpmg.com/socialmedia

© 2023 KPMG Yönetim Danışmanlığı A.Ş., şirket üyelerinin sorumluluğu sundukları garantiyle sınırlı özel bir İngiliz şirketi olan KPMG International Limited ile ilişkili bağımsız şirketlerden oluşan KPMG küresel organizasyonuna üye bir Türk şirketidir. Tüm hakları saklıdır.

Bu dokümanda yer alan bilgiler genel içeriklidir ve herhangi bir gerçek veya tüzel kişinin özel durumuna hitap etmemektedir. Doğru ve zamanında bilgi sağlamak için çalışmamıza rağmen, bilginin alındığı tarihte doğru olduğu veya gelecekte olmaya devam edeceği garantisi yoktur. Hiç kimse özel durumuna uygun bir uzman görüşü almaksızın, bu dokümanda yer alan bilgilere dayanarak hareket etmemelidir. KPMG adı ve KPMG logosu, bağımsız üye şirketlerden oluşan KPMG küresel organizasyonun lisansı altında tescilli ticari markalardır. KPMG International Limited ve ilişkili kuruluşları müşterilere herhangi bir hizmet sunmamaktadır.

© 2023 KPMG Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş., şirket üyelerinin sorumluluğu sundukları garantiyle sınırlı özel bir İngiliz şirketi olan KPMG International Limited ile ilişkili bağımsız şirketlerden oluşan KPMG küresel organizasyonuna üye bir Türk şirketidir. Tüm hakları saklıdır.

Document Classification: KPMG Confidential

kpmg.com.tr