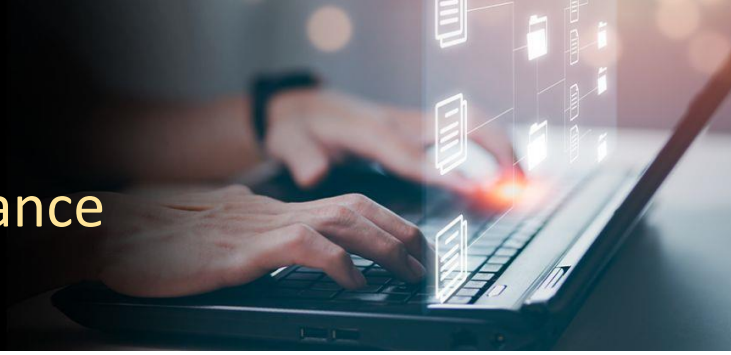
IBM Verify Identity Governance

Yeni Nesil Kimlik Yönetişimi ve BBS Stratejik Ortaklığı



Günümüzün hibrit çalışma modelleri ve çoklu bulut (multicloud) mimarileriyle şekillenen dijital dünyasında, geleneksel ağ güvenliği çeperi tamamen erimiş durumdadır. Kimlik, artık ağın kenarında duran bir kontrol noktası değil; kurumun en kritik ve yegâne güvenlik sınırıdır. **Yapay zeka destekli saldırıların %56 oranında artış gösterdiği** mevcut tehdit ortamında, saldırganlar artık "sistemi kırmıyor", geçerli kimlikleri "kullanarak içeri sızıyor". Bu paradigma değişimi, kimlik yönetimini bir BT operasyonu olmaktan çıkarıp kurumun en stratejik savunma hattına dönüştürmüştür.

- Kim, hangi kaynağa, hangi yetkiyle ve neden erişiyor?
- Bu erişim hâlâ gerekli mi?
- Verilen yetki kurum politikalarıyla ve görevler ayrılığı kurallarıyla uyumlu mu?
- Kullanıcı kurumdan ayrıldığında erişimleri zamanında kaldırılıyor mu?

Bilgi Birikim Sistemleri, **IBM Verify Identity Governance** ile dijital kimliklerin ve erişim haklarının yaşam döngüsü boyunca merkezi, otomatik ve denetlenebilir biçimde yönetilmesini sağlar. Kimlik süreçlerini kurumsal politikalara bağlayan çözüm; güvenliği güçlendirirken manuel iş yükünü azaltır, erişim risklerini görünür hâle getirir ve denetim süreçlerini kolaylaştırır.

IBM Verify Identity Governance (IVIG): Bütünleşik IGA Platformu

IBM, kimlik yönetimi dünyasındaki köklü mirasını modern bir vizyonla yeniden tanımlayarak, eski **IBM Security Identity Manager (ISIM)** ve **Identity Governance (IGI)** bileşenlerini tek bir stratejik çatı altında toplamıştır. Bu dönüşümün kalbinde, tüm kimlik türlerini (insan, makine, ayrıcalıklı hesaplar) sarmalayan bütünleşik bir **"Identity Fabric" (Kimlik Dokusu)** vizyonu yer almaktadır.

- ✓ Kimlik yaşam döngüsü yönetimi
- ✓ Otomatik provisioning ve de-provisioning
- ✓ Erişim talebi ve onay iş akışları
- ✓ Rol ve yetki yönetimi
- ✓ Görevler ayrılığı kontrolleri
- ✓ Erişim sertifikasyonu
- ✓ Kimlik analitiği ve risk görünürlüğü
- ✓ Denetim izi ve raporlama

IBM'in bu hamlesi, operasyonel hesap yönetimi ile stratejik yönetişim arasındaki duvarları yıkmıştır. Geçmişte bağımsız olarak yönetilen provisioning yetenekleri, artık IVIG içerisinde merkezi yönetişimin doğal bir parçasıdır. Bu konsolidasyon, kurumların "silolanmış yönetimden merkezi yönetişime" geçmesini sağlayarak tek bir platform üzerinden tam hakimiyet kurmasına olanak tanır.

IBM Verify Identity Governance Nedir?

IBM Verify Identity Governance, kullanıcı kimliklerini ve erişim haklarını tüm yaşam döngüsü boyunca yöneten kapsamlı bir **Identity Governance and Administration – IGA** çözümüdür. Kimliklerin oluşturulması, kullanıcı hesaplarının hedef sistemlere tanımlanması, erişim taleplerinin onaylanması, riskli yetki kombinasyonlarının belirlenmesi ve erişimlerin düzenli olarak gözden geçirilmesi aynı yönetişim yaklaşımı içinde ele alınır.

Çözüm, kullanıcı erişimi ve faaliyetlerinin yaşam döngüsü, uyumluluk ve analitik yetenekleriyle sağlanmasına, denetlenmesine ve raporlanmasına yardımcı olur. Şirket içi, bulut ve hibrit ortamlardaki kimlik süreçlerinin ortak politikalar altında yönetilmesini destekler.

Kimlik Yaşam Döngüsünü Otomatikleştirin

Yeni bir çalışanın kuruma katılması, görev veya departman değiştirmesi ve kurumdan ayrılması farklı sistemlerde çok sayıda hesap ve yetki işlemi gerektirir. Manuel yürütülen süreçler gecikmelere, hatalı yetkilendirmelere ve kaldırılmayan erişimlere yol açabilir.

IBM Verify Identity Governance ile:

- İnsan kaynakları gibi güvenilir kaynaklardan kimlik verisi alınabilir.
- Yeni kullanıcı hesapları hedef sistemlerde otomatik oluşturulabilir.
- Görev veya departman değişikliklerinde erişimler güncellenebilir.
- Geçici ve süreli erişimler yönetilebilir.
- İşten ayrılan kullanıcıların hesapları ve yetkileri otomatik kapatılabilir.
- Yetim, sahipsiz veya kullanılmayan hesapların azaltılması desteklenebilir.

Sonuç olarak kullanıcılar ihtiyaç duydukları kaynaklara daha hızlı erişirken, gereksiz erişimlerin sistemlerde kalma süresi kısaltılır.

Erişim Taleplerini İş Akışına Bağlayın

Kullanıcılar veya yetkili yöneticiler, self servis erişim kataloğu üzerinden uygulama, rol ya da yetki talebinde bulunabilir. Talepler; kullanıcının yöneticisi, uygulama sahibi, veri sahibi, bilgi güvenliği, insan kaynakları veya uyumluluk birimi gibi farklı sorumluların onayına yönlendirilebilir.

Onay süreci kullanıcının görevi, talep edilen kaynağın risk düzeyi, kurumun onay matrisi ve görevler ayrılığı politikaları dikkate alınarak yapılandırılabilir. Onaylanan erişimin hedef sisteme otomatik uygulanması, manuel BT işlemlerini ve insan hatalarını azaltır.

Rol ve Yetki Yönetimi

Doğru erişim doğru kullanıcı doğru zaman

Her kullanıcı yetkisinin tek tek yönetilmesi, özellikle büyük ve karmaşık yapılarda sürdürülebilir değildir. IBM Verify Identity Governance, erişimlerin iş rolleri ve BT rolleri üzerinden yönetilmesine yardımcı olur.

- İş rolleri ve teknik roller oluşturulabilir.
- Roller uygulama ve erişim yetkileriyle ilişkilendirilebilir.
- Kullanıcılara görevlerine uygun temel erişimler atanabilir.
- Aşırı yetkilendirilmiş kullanıcılar belirlenebilir.
- Kullanılmayan veya birbiriyle çakışan roller analiz edilebilir.
- Rol değişiklikleri yönetişim ve onay süreçlerine bağlanabilir.

Rol tabanlı yapı, erişim modelini sadeleştirirken kurumsal yetkilendirme politikalarının tutarlı uygulanmasını destekler.

Faaliyet Tabanlı Erişim Yönetişimi

Teknik yetkiler çoğu zaman iş birimleri ve denetçiler için anlaşılması güç isimlerden oluşur. IBM Verify Identity Governance, teknik erişimleri “satın alma talebi oluşturma”, “siparişi onaylama”, “tedarikçi kaydı açma” veya “ödeme gerçekleştirme” gibi iş faaliyetleriyle ilişkilendirebilir.

Faaliyet tabanlı yaklaşım sayesinde:

- Teknik yetkiler iş süreçleri bağlamında değerlendirilir.
- Riskli erişim kombinasyonları daha kolay anlaşılır.
- İş birimleri erişim kararlarına daha etkin katılır.
- Kontroller denetçi ve uyumluluk ekipleri için daha anlamlı hâle gelir.

Görevler Ayrılığı (SoD) ve Erişim Sertifikasyonu

Özellikle SAP gibi kritik ERP sistemlerinde SoD risklerinin tespiti hayati önem taşır. Bir kullanıcının hem kritik bir işlemi başlatması hem de aynı işlemi onaylaması hata, suistimal ve dolandırıcılık riskini artırabilir. **Segregation of Duties – SoD** kontrolleri, çelişen görevlerin aynı kullanıcı üzerinde toplanmasının önlenmesine yardımcı olur.

IBM Verify Identity Governance ile:

- Çakışan roller ve yetkiler tanımlanabilir.
- Yeni talepler onaylanmadan önce risk kontrolünden geçirilebilir.
- Mevcut kullanıcıların erişim ihlalleri belirlenebilir.
- Risk kabulü ve telafi edici kontrol süreçleri uygulanabilir.
- SAP gibi kritik kurumsal uygulamalardaki SoD riskleri yönetilebilir.

Erişim Sertifikasyonu ve Periyodik Gözden Geçirme

Bir kullanıcının geçmişte ihtiyaç duyduğu erişim, bugün artık gerekli olmayabilir. Görev değişiklikleri, geçici projeler ve manuel yetkilendirmeler zaman içinde yetki birikimine neden olabilir.

IBM Verify Identity Governance; kullanıcı, grup, rol, uygulama veya risk seviyesine göre erişim sertifikasyon kampanyaları oluşturulmasını sağlar. Yetkili yöneticiler erişimleri onaylayabilir, kaldırılmasını isteyebilir, kararlarını gerekçelendirebilir ve yüksek riskli erişimleri önceliklendirebilir. Kritik uygulamalar için tekrarlanan gözden geçirme dönemleri tanımlanabilir.

Kimlik Analitiği ve Denetim Görünürlüğü

Kimlikler, hesaplar, roller, yetkiler ve uygulamalar arasındaki ilişkiler analiz edilerek aşağıdaki risklerin görünür hâle getirilmesi desteklenir:

- Aşırı yetkilendirilmiş kullanıcılar
- Görevle uyumsuz erişimler
- Kullanılmayan yetkiler
- Riskli erişim kombinasyonları
- Sahipsiz ve yetim hesaplar
- Politika ihlalleri
- Olağan dışı kullanıcı davranışları

Kimlik ve erişim işlemlerinin kayıt altına alınması; erişimin kim tarafından talep edildiği, kim tarafından onaylandığı, hangi politikaya göre verildiği ve ne zaman gözden geçirildiği gibi soruların yanıtlanmasını kolaylaştırır.

Teknolojik Sıçrama ve TCO Avantajı

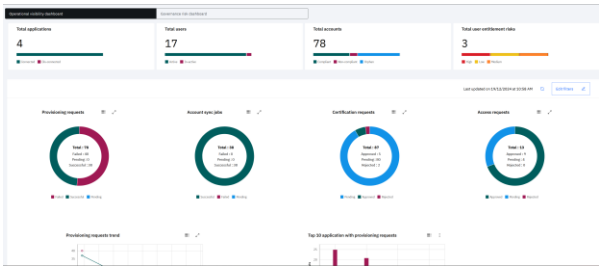
ÖZELLİK	TEKNİK VE STRATEJİK KARŞILIK
KONTEYNER DESTEĞİ	RedHat OpenShift ve Kubernetes üzerinde cloud-native dağıtım; AWS, Azure ve GCP uyumu.
ALTYAPI MODERNİZASYONU	WebSphere Liberty ve PostgreSQL desteği. **Lisans maliyetlerini artıran WAS ND ve DB2 bağımlılığının kalkmasıyla Toplam Sahip Olma Maliyetinde (TCO) ciddi düşüş.**
REST API EKOSİSTEMİ	DevOps CI/CD süreçleri için tam otomasyon ve üçüncü parti sistemlerle kusursuz entegrasyon.
MODERN UI (LOW-CODE)	Adminler ve son kullanıcılar için yenilenmiş, modern ve sezgisel "No-code" deneyimi.

Kurumunuza Sağladığı Değer

IBM Verify Identity Governance, kimlik yönetimini reaktif bir BT operasyonundan ölçülebilir bir güvenlik ve yönetişim sürecine dönüştürür.

Güvenliği güçlendirin

- En az ayrıcalık ilkesini destekleyin.
- Gereksiz ve aşırı erişimleri azaltın.
- Riskli yetki kombinasyonlarını erken aşamada belirleyin.
- Kullanıcı ayrıldığında erişimlerin zamanında kaldırılmasını sağlayın.
- İç tehdit ve yetki suistimali risklerini azaltın.



Operasyonel verimliliği artırın

- İşe giriş, görev değişikliği ve işten ayrılma süreçlerini otomatikleştirin.
- Erişim taleplerini standart iş akışlarıyla yönetin.
- Tekrarlayan hesap ve yetki işlemlerinde BT ekiplerinin yükünü azaltın.
- Kullanıcıların ihtiyaç duydukları erişimlere daha hızlı ulaşmasını sağlayın.
- Manuel işlem ve veri hatalarını sınırlandırın.

Denetim ve uyumluluk süreçlerini kolaylaştırın

- Erişim kararları için izlenebilir bir denetim kaydı oluşturun.
- Periyodik erişim gözden geçirmelerini standartlaştırın.
- Politika ihlallerini ve riskli erişimleri merkezi olarak raporlayın.
- Denetim kanıtlarının hazırlanmasını kolaylaştırın.
- KVKK, ISO 27001, PCI DSS, SOX ve sektörel düzenlemelerin erişim kontrolü gereksinimlerini destekleyin.

IBM Verify Identity Governance kullanılması tek başına mevzuata uyum garantisi oluşturmaz. Süreçlerin kurum politikaları, risk yaklaşımı ve tabi olunan düzenlemeler doğrultusunda tasarlanması gerekir.

Hangi Kurumlar İçin Uygundur?

- Çok sayıda kullanıcı, uygulama ve yetkiyi yöneten kuruluşlar
- Şirket içi, bulut ve hibrit sistemleri birlikte kullanan kurumlar
- Finans, sigorta, telekom, sağlık, enerji ve kamu gibi düzenlemeye tabi sektörler
- Manuel erişim taleplerini ve onay süreçlerini otomatikleştirmek isteyen kurumlar
- Erişim sertifikasyonu ve görevler ayrılığı kontrollerini güçlendirmek isteyen kuruluşlar
- Mevcut ISIM veya ISVG altyapısını modernize etmeyi planlayan kurumlar

BBS ile uçtan uca IBM Verify Identity Governance Hizmetleri

Başarılı bir IGA projesi yalnızca ürün kurulumundan ibaret değildir. Kimlik verisinin doğruluğu, rol ve yetki modelinin tasarımı, uygulama entegrasyonları, onay süreçleri ve iş birimlerinin katılımı projenin başarısını doğrudan etkiler.

Bilgi Birikim Sistemleri, IBM Verify Identity Governance projelerini analizden canlı kullanıma, eğitimden sürekli iyileştirmeye kadar uçtan uca ele alır.

Analiz ve Yol Haritası

- Mevcut kimlik ve erişim altyapısının değerlendirilmesi
- Kullanıcı yaşam döngüsü süreçlerinin analiz edilmesi
- Kimlik kaynakları ve hedef sistemlerin belirlenmesi
- Risk, uyumluluk ve denetim ihtiyaçlarının değerlendirilmesi
- Rol, yetki ve onay modellerinin tasarlanması
- Kademeli uygulama ve dönüşüm yol haritasının hazırlanması

Mimari Tasarım ve Kurulum

- Çözüm mimarisinin oluşturulması
- Sistem kurulumu ve yapılandırması
- Yüksek erişilebilirlik ve küme mimarilerinin tasarlanması
- Geliştirme, test ve canlı ortamların hazırlanması
- Güvenlik, performans ve kapasite ayarlarının gerçekleştirilmesi

Entegrasyon ve Uygulama Geliştirme

- İnsan kaynakları sistemleriyle kimlik besleme entegrasyonu
- Active Directory, LDAP ve kurumsal dizin entegrasyonları
- Kurumsal uygulama, veri tabanı ve bulut servisleriyle bağlantı
- Bağlayıcı, adaptör, API ve özel entegrasyon geliştirme
- Servis yönetimi ve iş akışı sistemleriyle entegrasyon
- Kuruma özel süreç, ekran ve rapor geliştirme

Yönetişim Modelinin Kurulması

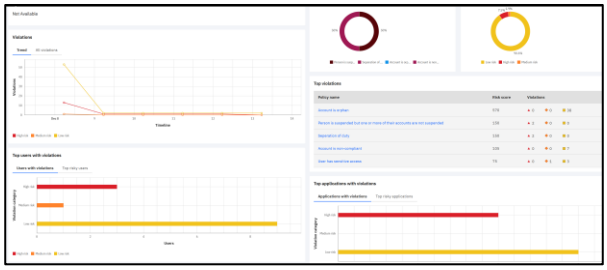
- Erişim talep ve onay iş akışlarının tasarlanması
- Rol ve yetki modelinin oluşturulması
- SoD kurallarının tanımlanması
- Erişim sertifikasyon kampanyalarının yapılandırılması
- Risk politikaları ve telafi edici kontrollerin uygulanması
- Denetim ve uyumluluk raporlarının hazırlanması

Geçiş ve Modernizasyon

- Mevcut ISIM ve ISVG ortamlarının değerlendirilmesi
- IBM Verify Identity Governance geçiş planının hazırlanması
- Entegrasyon ve özelleştirmelerin analiz edilmesi
- Kimlik, rol, yetki ve politika verilerinin taşınması
- Versiyon yükseltme ve modernizasyon çalışmaları
- Geçiş sonrası doğrulama ve optimizasyon

Eğitim Bakım ve Destek

- Sistem yöneticisi ve son kullanıcı eğitimleri
- Health-check hizmetleri
- Performans ve kapasite değerlendirmesi
- Versiyon ve güvenlik güncellemeleri
- Sorun giderme ve teknik destek
- Bakım ve danışmanlık hizmetleri



Neden Bilgi Birikim Sistemleri?

Karmaşık bir IGA projesinin başarısı, yazılımın gücü kadar onu uygulayan ekibin metodolojisine ve yerel tecrübesine bağlıdır. BBS; IBM kimlik ve güvenlik çözümlerindeki deneyimini, eski ISIM ve ISVG yapılarına ilişkin teknik bilgi birikimini ve kurumsal entegrasyon yetkinliğini bir araya getirir. Kurumun mevcut yatırımlarını, güvenlik gereksinimlerini ve iş süreçlerini dikkate alarak uygulanabilir bir IGA mimarisi oluşturur. BBS, projeleri sadece bir kurulum süreci olarak değil, kurumun dijital dönüşüm yol haritasının kritik bir parçası olarak ele alır.

BBS Uzmanlığı ve Katma Değerli Hizmetler

BBS, IBM çözümlerindeki derin mimari bilgisini şu alanlarda fark yaratan bir hizmete dönüştürür:

- ✓ **Modernizasyon ve Güvenli Geçiş:** Eski ISIM veya ISVG yapılarından v11 sürümüne veri kaybı yaşanmadan, karmaşık özelleştirmelerin korunarak taşınması (migration) konusundaki teknik uzmanlık.
- ✓ **IGA Yol Haritası ve Analiz:** Kurumun mevcut olgunluk seviyesini ölçen "Health-check" ve "Kapasite Değerlendirmesi" hizmetleriyle doğru stratejinin belirlenmesi.
- ✓ **Özel Entegrasyon Geliştirme:** SCIM ve REST API tabanlı, standart dışı kurumsal uygulamaların kimlik ekosistemine bağlanması.
- ✓ **Yerel Mevzuat ve Destek:** KVKK uyumluluğu gözetilerek tasarlanan süreçler ve proje sonrası sürekli optimizasyon desteği.
- ✓ **Canlı Kullanım Sonrasında Bakım ve Teknik Destek**

BBS'nin IBM ekosistemindeki teknik hakimiyeti, kurumların teknoloji yatırımından maksimum ROI elde etmesini ve karmaşık geçiş süreçlerini risk almadan tamamlamasını sağlar.

Gelecek vizyonunda, bu bütünleşik yapı **ISPM (Identity Security Posture Management)** ve **ITDR (Identity Threat Detection and Response)** entegrasyonlarıyla daha da güçlenecektir. Mevcut altyapınızı modernize etmek, karmaşık yetki yapılarını sadeleştirmek ve v11'in sunduğu TCO avantajlarından yararlanmak için BBS uzmanlarıyla iletişime geçin. Kurumunuza özel modernizasyon yol haritasını birlikte tasarlayalım.

Adres: Yeni Sahra Mah. Fatih Cad. No: 8 Ataşehir / İstanbul P.K 34746
T: +90 (216) 373 98 00
F: +90 (216) 373 99 93