Vendor–Sistem–Veri Erişim Haritası & Due Diligence Checklist Şablonu — Yazılım / Vendor (v1.0)

Asset Amaç: Bu asset; veri işleyen üçüncü taraf tedarikçilerin (*vendor*) teknik erişimlerini tam olarak görünür kılmak için tasarlanmıştır. Hangi vendor'ın, hangi sistem ve veri alanlarına, hangi yolla (API / FTP / Panel) eriştiğini tek bir haritada toplar. API token ve panel erişimlerini "minimum yetki" (*least privilege*) prensibiyle yönetmek, entegrasyon loglarını standardize etmek ve periyodik gözden geçirme (*review*) ile sözleşme bitimi (*offboarding*) adımlarını süreçleştirmek için operasyonel bir Due Diligence kontrol listesi sunar. Otel ve B2B altyapılarında vendor riskini BT, Satın Alma ve KVKK/Uyum ekiplerinin ortak zemininde güvenle yönetmeyi hedefler.

Kim Kullanır?: BT / IT Yöneticileri, Satın Alma Ekipleri, KVKK / Uyum Sorumluları ve Sistem Sahipleri (*Owner'lar*).

Nasıl Kullanılır?

1. Tüm vendor'lar için envanter çıkarın; **Vendor–Sistem–Veri** tablosunu doldurarak erişim yollarını (API/FTP vs.) ve yetki seviyelerini (Read/Write) işaretleyin.
2. Token ve panel girişleri için güvenlik kontrollerini (minimum yetki tanımlaması, MFA zorunluluğu, IP allowlist, token rotasyonu) devreye alın.
3. Çeyreklik hesap temizliği, periyodik review ve offboarding (yetki iptali) adımlarını 365 günlük güvenlik takvimine bağlayın.

CHECKLIST & SPRINT PLAN — Vendor Yönetimi & Teknik Due Diligence

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Vendor Envanteri Çıkarıldı:** CRM, chat aracı, çağrı merkezi, bulut hizmetleri ve raporlama araçları gibi tüm üçüncü parti yazılımlar listelendi.
- [ ] **Vendor Owner'ları Atandı:** Her bir entegrasyon veya vendor için kurum içinden bir iş birimi sorumlusu belirlendi.
- [ ] **Vendor–Sistem–Veri Eşleme Tablosu Tamamlandı:** Hangi tedarikçinin hangi veri setine dokunduğu haritalandırıldı.
- [ ] **Erişim Yolu Belirlendi:** Bağlantı mimarisi (API, FTP, Web Panel, Veritabanı doğrudan erişimi) netleştirildi.
- [ ] **Yetki Seviyesi Tanımlandı:** Read (Okuma), Write (Yazma) veya Export (Dışa Aktarma) yetkileri "minimum erişim" prensibiyle sınırlandırıldı.
- [ ] **Token / Key Envanteri Çıkarıldı:** Vendor'lara tahsis edilen tüm API anahtarları kayıt altına alındı.
- [ ] **Token Minimum Yetkili (Scope Restricted):** API anahtarlarına sadece ihtiyaç duyulan modüller/endpoint'ler için yetki verildi (Global/Root yetki yok).
- [ ] **Token Rotasyon Takvimi Var:** Statik token'ların belirli periyotlarla (örn. 90 gün) otomatik yenilenmesi kurala bağlandı.
- [ ] **Secrets Manager Kullanımı Aktif:** Şifre ve key'ler açık metin (*plaintext*) olarak değil, güvenli kasa (Secrets Manager) mimarisiyle yönetiliyor.

- [ ] **Vendor Panel RBAC Aktif:** Vendor yönetim panellerinde rol bazlı erişim modeli (Rol-Yetki matrisi) devrede.
- [ ] **Vendor Panel MFA Zorunlu:** Tedarikçi ekiplerin sistemlere girişlerinde Çok Faktörlü Doğrulama kuralı mecburi tutuldu.
- [ ] **IP Allowlist / VPN Uygulanıyor:** Kritik panellere veya veritabanlarına sadece yetkili tedarikçi IP'lerinden/VPN'lerinden izin veriliyor.
- [ ] **Entegrasyon Logları Tutuluyor:** API üzerinden yapılan veri çekme/yazma işlemleri "Kim, Ne Zaman, Hangi Veri" formatında audit loguna yazılıyor.
- [ ] **Offboarding Prosedürü Hazır:** Hizmeti biten vendor'lar için Token Revoke (İptal) ve hesap kapatma iş akışı standartlaştırıldı.
- [ ] **365 Gün Refresh Planlandı:** Çeyreklik hesap temizliği ve yıllık due diligence kontrolleri takvime eklendi.

2) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm (Vendor Due Diligence)
Vendor'ın Hangi Veriye Eriştiği Bilinmiyor	Merkezi bir erişim haritasının ve sorumlunun olmaması	**Vendor–Sistem–Veri Tablosu** + **Sistem Owner Ataması**
Token'lar (API Key) Sınırsız ve Süresiz	Token rotasyonu eksikliği ve yetki daraltma (scope) yapılmaması	**Scope Daraltma (Least Privilege)** + **Rotasyon** + **Secrets Manager**
Vendor Panelinde Eski (Kullanılmayan) Hesaplar Açık	Tanımlı bir Offboarding (ilişik kesme) sürecinin yokluğu	**Çeyreklik Hesap Temizliği (Audit)** + **Offboarding Checklist**

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14)

[Gün 1–4: Envanter & Haritalama] ⟶ [Gün 5–8: Güvenlik, Token & Erişim Kurgusu] ⟶ [Gün 9–11: Offboarding & Loglama Provası] ⟶ [Gün 12–14: Dokümantasyon & Audit]

- **Gün 1:** Vendor envanterinin çıkarılması ve iç sorumluların (owner) atanması.
- **Gün 2:** Vendor–Sistem–Veri erişim tablosunun ilk taslağının oluşturulması.
- **Gün 3:** Erişim yollarının (API/FTP/Panel vb.) ve yetki seviyelerinin (Read/Write/Export) netleştirilmesi.
- **Gün 4:** Sistemlerdeki tüm aktif Token/Key envanterinin çıkarılması ve scope daraltma (yetki kısıtlama) çalışmalarına başlanması.
- **Gün 5:** Secrets Manager entegrasyonunun yapılması ve statik token'lar için rotasyon planının oluşturulması.

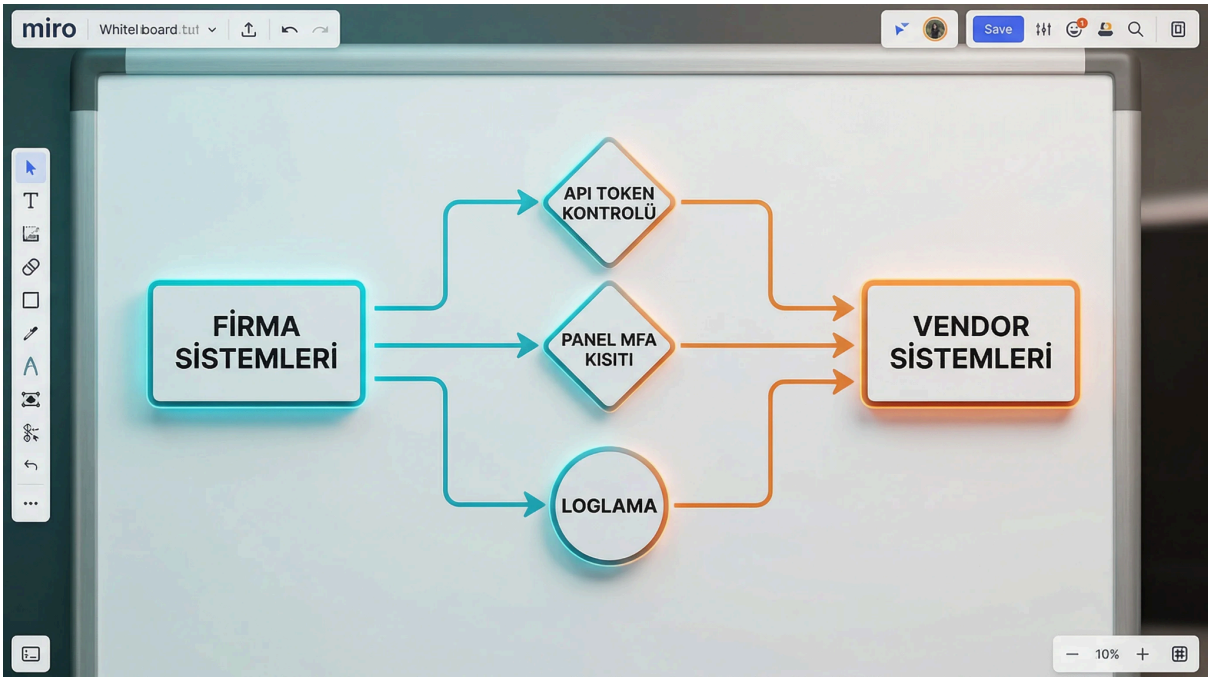
- **Gün 6:** Vendor panellerinde Role-Based Access Control (RBAC) yetkilerinin düzenlenmesi ve MFA zorunluluğunun aktif edilmesi.
- **Gün 7:** Kritik paneller ve veritabanı erişimleri için IP allowlist ve/veya VPN kurgusunun ağ katmanında yapılandırılması.
- **Gün 8:** API ve entegrasyon log şemasının SIEM/merkezi log sunucularında yapılandırılması (Audit Trail).
- **Gün 9:** Varsa FTP veya dosya transfer kurallarının güvenli kanallara (SFTP) taşınması ve standartlarının belirlenmesi.
- **Gün 10:** Vendor Offboarding prosedürünün yazılması (Token iptali + Yetkili hesap kapatma adımları).
- **Gün 11:** Prova: Seçilen 1 vendor için "erişim kanıt paketi" (log ve yetki raporu) çıkarılarak sürecin test edilmesi.
- **Gün 12:** Prova sonucunda tespit edilen erişim ve loglama boşluklarının kapatılması.
- **Gün 13:** Due diligence kontrol listesinin, prosedürlerin ve haritaların versiyonlanarak yayımlanması.
- **Gün 14:** Yönetim kapanış raporunun sunulması ve 365 günlük refresh (yenileme/temizlik) takviminin devreye alınması.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	**Önce (Mevcut Durum)**	**Sonra (Sprint Sonrası)**	**Hedef Yönü**
Haritalanmış Vendor Oranı (%)	%10 - %20 (Tahmini)	%100 (Tam Görünürlük)	**Hedef ↑ (Yükselme)**
Rotasyonu Planlı Token Oranı (%)	%0 (Sınırsız süre)	%100 (90 Gün vb. otomatik)	**Hedef ↑ (Yükselme)**
MFA Etkin Vendor Panel Oranı (%)	%15	%100	**Hedef ↑ (Yükselme)**
Log Kapsama Oranı (Entegrasyon)	Sadece Sistem Açık/Kapalı	Tüm Read/Write/Export işlemleri	**Hedef ↑ (Yükselme)**
Offboarding SLA (Hesap Kapatma)	Belirsiz (Aylar sürebilir)	< 24 Saat (Sözleşme bitiminde)	**Hedef ↓ (Düşüş - Hızlanma)**

Deliverables (Teslim Edilecek Çıktılar)

- **Vendor–Sistem–Veri Erişim Haritası (v1.0):** Kurumun tüm veri işleyen tedarikçilerinin tam topolojisi ve veri matrisi.
- **Token & Key Envanteri + Rotasyon Takvimi:** API ve servis hesaplarının güvenli yönetim yaşam döngüsü dokümanı.
- **Vendor Panel Erişim Politikası (RBAC / MFA / IP):** Üçüncü taraf sistem girişleri için teknik zorunluluklar rehberi.
- **Entegrasyon Log Standardı Mimarisi:** KVKK denetimlerinde kullanılmak üzere API/Panel hareketlerinin izleme şeması.
- **Vendor Offboarding Prosedürü & Audit Planı:** Sözleşme sonlanmalarında veri ve yetki izolasyonunu garantiye alan kontrol listesi.



[Diagram / Flow]

Üçüncü taraf (vendor) bulut hizmetleri, API ağ geçitleri ve kurum içi veri tabanları arasındaki veri akışını gösteren, 16:9 formatında yüksek çözünürlüklü bir Vendor Entegrasyon Akışı Diyagramı. Koyu şık zemin üzerinde; mavi ve turuncu veri aktarım hatları, MFA korumalı erişim kapıları, Secrets Manager token kasası, IP allowlist filtreleri ve merkezi log sunucusu (Audit Trail) kurumsal ve scannable bir mimari şema olarak sergileniyor.

[Checklist / Framework Card]

IT, satın alma ve uyum liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Vendor Due Diligence Checklist Kartı. Koyu karbon gri zemin üzerine yerleştirilmiş; API entegrasyon ikonları, kilitli token/anahtar simgesi, yetki onay kalkanı ve offboarding zamanlayıcısı. Kartın üzerinde; "Comprehensive Vendor-to-Data Access Mapping", "Least Privilege Token Scope & Auto-Rotation", "MFA & IP Allowlist Enforced Vendor Panels", ve "Strict Offboarding SLA & Quarterly Audits" teslimat kalemi başlıkları, yanlarında yeşil onay rozetleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.