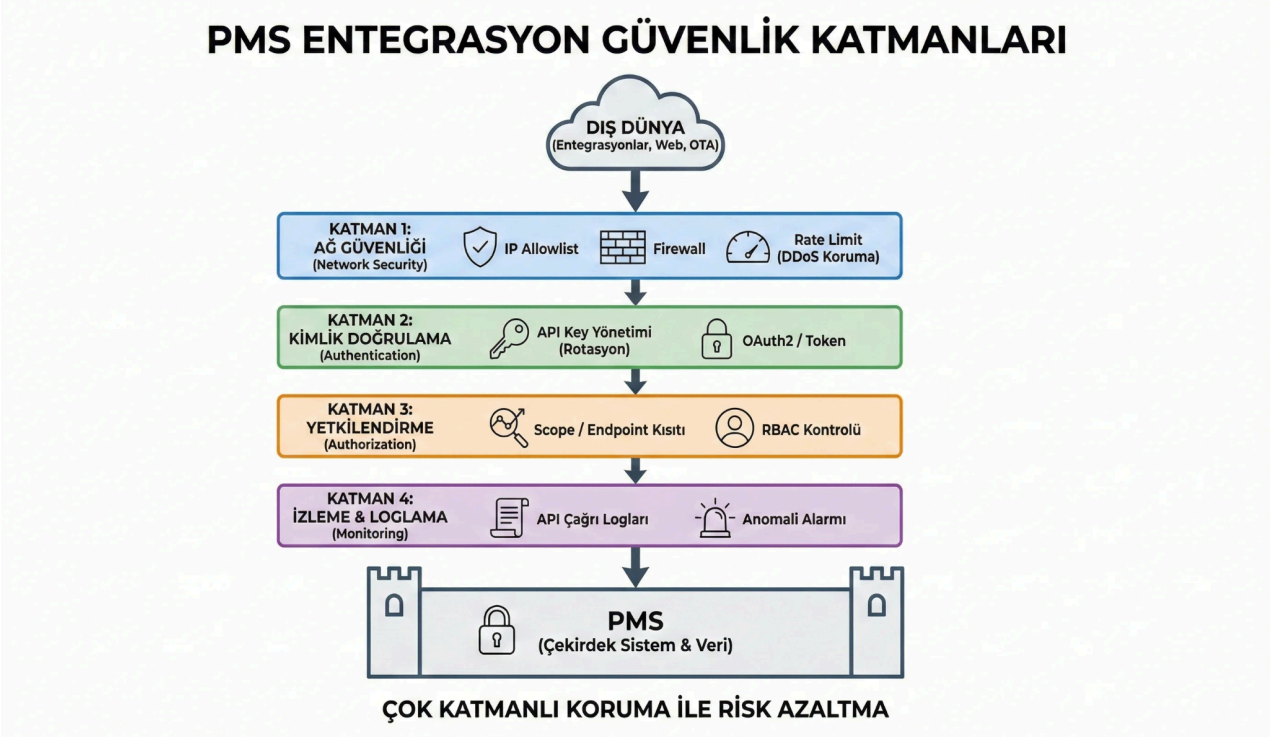
PMS Rol & Güvenlik Kontrol Listesi (v1.0)

Asset Amacı: Bu kontrol listesi; PMS entegrasyonlarında rol bazlı erişimi (RBAC), API güvenliğini, loglama ve KVKK veri yaşam döngüsünü standardize eder. Amaç; geniş yetki erişimi, API anahtarı sızıntısı ve log eksikliği gibi riskleri azaltarak teknik denetimlere hazırlıklı olmaktır.

Kim Kullanır?: IT/BI, Ön Büro, Muhasebe, Call Center ve Yönetim ekipleri birlikte kullanır.



"API güvenlik katmanları: Key, IP, Scope ve Rate Limit hiyerarşisi."

Nasıl Kullanılır? (3 Adım)

1. **Yetki Matrisi:** Rol matrisini çıkararak "minimum yetki prensibiyle" (least privilege) onay sürecini tamamlayın.
2. **Güvenlik Katmanları:** API seviyesinde anahtar (key), IP kısıtlaması (allowlist), kapsam (scope) ve hız limitlerini (rate limit) uygulayın.
3. **Denetim Rutini:** Veri saklama (retention), silme ve anonimleştirme süreçlerini dokümante ederek periyodik denetim rutinlerini kurun.

Ölçüm & Önceliklendirme Checklist'i (PMS Security)

- [ ] Hassas veri envanteri (misafir, rezervasyon, ödeme) çıkarıldı.
- [ ] Entegrasyonlarda veri minimizasyonu yapıldı; gereksiz alanlar kaldırıldı.
- [ ] Admin kullanıcı sayısı minimuma indirildi ve RBAC rol matrisi onaylandı.
- [ ] Call center ve rapor dışa aktarımları (export) için maskeleme standartları tanımlandı.
- [ ] API key'ler "Test" ve "Prod" ortamları için birbirinden ayrıldı.

- [ ] IP allowlist ve anomali tespiti için rate limit alarmları aktif edildi.
- [ ] Veri saklama (retention) ve anonimleştirme süreçleri loglanmaya başlandı.

Problem ➔ Kök Neden ➔ Çözüm Tablosu

Problem	Kök Neden	Çözüm
Yetki suistimali	Geniş admin erişimi	RBAC + Onay + Denetim
Veri sızıntısı	API key yönetimi zayıf	Rotasyon + IP allowlist + Scope
"Kim yaptı?" bilinmiyor	Log eksikliği	Merkezi log + Audit
Denetimde sorun	Retention belirsiz	Veri yaşam döngüsü dokümanı
Raporlarda hassas veri	Maskeleme yok	Maskeli / Aggregate dashboard

14 Günlük Güvenlik & KVKK Sprint Planı

- **Gün 1-5:** Hassas veri envanteri ve minimizasyonu, rol matrisi (v1.0) ve kritik işlem onay akışlarının kurgulanması.
- **Gün 6-9:** API key yönetimi SOP'u, IP allowlist/scope kısıtlamaları ve merkezi loglama sisteminin kurulumu.
- **Gün 10-14:** Retention dokümantasyonu, silme/anonim testleri, olay yönetimi (incident management) playbook'u ve güvenlik tatbikatı.

Öncesi / Sonrası KPI Tablosu

KPI	Öncesi	Sonrası (Hedef)	Takip
Yetki İhlali Sinyali	Takipsiz	İzlenir	Günlük
Admin İşlem Log'u	Eksik	Tam	Gerçek Zamanlı
API Key Rotasyon Uyumu	Düşük	Yüksek	Aylık

Export Kontrolü	Zayıf	Onaylı	Haftalık
Retention Uyumu	Belirsiz	Yazılı + İzlenir	Aylık

Deliverables

RBAC Rol Matrisi, API Güvenlik Katmanları SOP'u, Retention & Veri Yaşam Döngüsü Dokümanı, Loglama & Alarm Kurgusu, Olay Yönetimi Playbook'u.

"PMS güvenlik ve erişim rolleri kontrol listesi."