GRC'nin Uygulanması ve Yeni Standartların Siber Tehdit Azaltımına Etkisi

IV MİLLİ KİBERTƏHLÜKƏSİZLİK FORUMU 2026

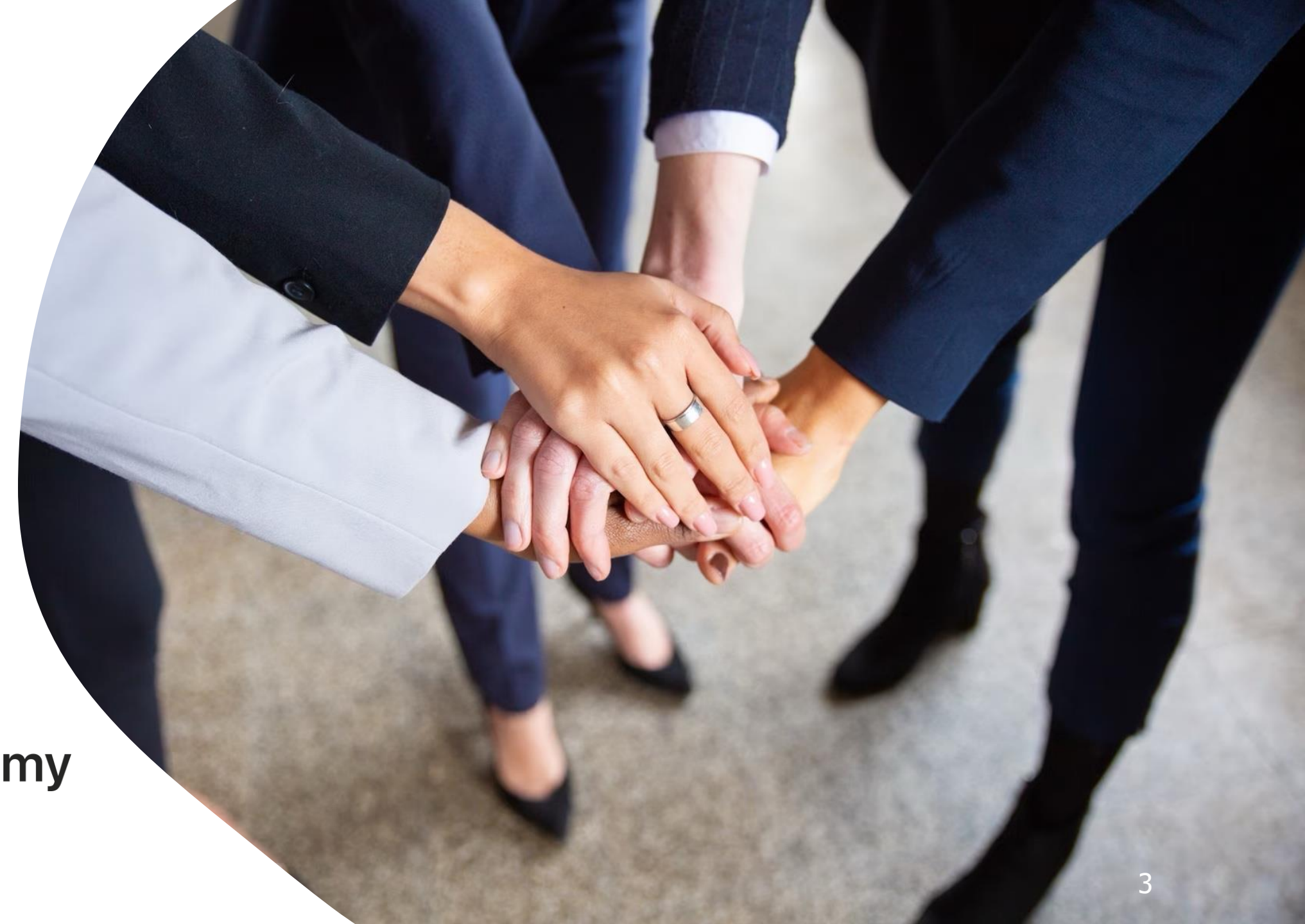
CFEACADEMY Kurucu, Eğitmen – **Ömer KILINÇ**

Hakkımızda

CFE Uyum Hizmetleri

CFECERT

- ✓ **CFECERT**, **UKAS**, **IAS** ve **TURKAK** tarafından akredite edilmiş, birçok ülkede faaliyet gösteren bağımsız bir denetim kuruluşudur.
- ✓ **CFECERT**, İngiliz eğitim akreditasyon otoritesi CPD Certification Service üyesidir.
- ✓ **CFECERT**, İngiliz Sertifikasyon Kuruluşları Birliği'nin **(ABCB)** bir üyesidir.
- ✓ **CFECERT,** UK Cyber Security Council Kurumsal bir üyesidir.
- ✓ **CFECERT,** Kurumsal Risk Yönetim Derneği **(KRYD)** bir üyesidir.
- ✓ **CFECERT**, Bilgi Güvenliği, İş Sürekliliği, IT Hizmet Yönetimi, Kalite Yönetimi, GDPR, Yapay Zeka, Kişisel Veri Yönetim Sistemi gibi birçok alanda GAP Analizi, Eğitim, Denetim ve Belgelendirme hizmetleri sunmaktadır.



CFE | Academy

Tehdit ortamı değişti — uyum artık "kâğıt üzerinde" yetmiyor

BAĞLAM

Saldırganlar otomatikleşti, tedarik zinciri saldırıları ve AI destekli tehditler arttı. Düzenleyiciler de yanıt verdi: yeni nesil standartlar artık bir "yıllık denetim" değil, sürekli işleyen bir tehdit azaltma disiplini talep ediyor.

~22.000

finans kuruluşu DORA kapsamında — Ocak 2025'ten beri doğrudan yürürlükte

21 / 27

AB ülkesi NIS2'yi ulusal hukuka aktardı (Mart 2026); denetim başladı

11 yeni

ISO 27001:2022 kontrolü — threat intelligence, bulut, güvenli geliştirme

1'inci

yapay zekâ yönetim standardı ISO 42001 ile AI artık GRC kapsamında

GRC neden tehdit azaltmanın merkezinde?

TEMEL

GRC üç disiplini tek bir yönetim döngüsünde birleştirir. Doğru kurulduğunda, güvenlik kontrollerini tek tek olaylara değil, ölçülen riske ve hesap verebilirliğe bağlar — yani tehdidi kaynağında azaltır.

Tehdit azaltma = Yönetişimin yönlendirdiği, risk temelli, uyumla kanıtlanan sürekli bir döngü

Governance / Yönetişim

Üst yönetimin sahipliği, rol ve sorumluluklar, politika. "Kim karar veriyor, kim hesap veriyor?"

Risk

Tehditlerin sistematik tespiti, değerlendirilmesi ve önceliklendirilmesi. Kaynaklar en kritik riske gider.

Compliance / Uyum

Standart ve mevzuata uygunluğun kanıtlanması — ama amaç "kutu işaretlemek" değil, dayanıklılık.

"Yıllık denetim"den "sürekli tehdit azaltma"ya

PARADIGMA DEĞİŞİMİ

ESKİ YAKLAŞIM

- Compliance = yılda bir denetim, kutu işaretleme
- Güvenlik IT'nin sorunu; yönetim uzakta
- Statik kontrol listesi, nadiren güncellenir
- Tedarikçi riski sözleşmeye gömülü, izlenmez
- Olay olduktan sonra tepki

YENİ STANDARTLARIN GETİRDİĞİ

- ✓ Sürekli izleme ve risk-temelli kontrol
- ✓ Üst yönetimin yasal, kişisel hesap verebilirliği
- ✓ Tehdit istihbaratının kontrollere beslenmesi
- ✓ Tedarik zinciri riskinin aktif yönetimi
- ✓ Dayanıklılık testi: önceden kır, önce öğren

Bilgi güvenliğinin yeni temeli — geçiş tamamlandı

STANDART 1 · ISO/IEC 27001:2022

31 Ekim 2025 itibarıyla 2013 sürümü geçersiz. Yapı sadeleşti: **93 kontrol, 4 tema** ve tehdit ortamını yansıtan **11 yeni kontrol.**

A.5.7 Threat Intelligence

Tehdit istihbaratının toplanması, analizi ve risk değerlendirmesine beslenmesi. Saldırıyı görmeden savunma kurulamaz.

Güvenli geliştirme & izleme

Secure coding, güvenlik testleri, sürekli izleme (8.16) ve veri maskeleme — zafiyeti üretim öncesi yakalar.

ICT hazırlık & bulut

İş sürekliliği için ICT readiness ve bulut hizmetleri güvenliği — kesinti ve yanlış yapılandırma riskini düşürür.

Tehdit azaltma etkisi: standart artık "belge" değil, istihbarat → kontrol → izleme döngüsü kuruyor.

CFE | Academy

Sorumluluğu yönetim kuruluna taşıyan zorunluluk

STANDART 2 · NIS2 DIREKTIFI (AB)

Mart 2026: 21/27 ülke NIS2'yi aktardı; hazırlık dönemi bitti, ulusal denetim başladı. Kapsam temel ve önemli sektörlere genişledi.

Yönetim kurulu sorumluluğu

Üst yönetim siber risk gözetiminden kişisel olarak sorumlu — eğitim ve onay zorunlu.

Hızlı olay raporlama

Erken uyarı 24 saat, bildirim 72 saat. Olay yönetimi artık ölçülen bir yükümlülük.

Tedarik zinciri güvenliği

Tedarikçi ve hizmet sağlayıcı riskinin değerlendirilmesi ve sözleşmeye yansıtılması.

Caydırıcı yaptırım

Ciddi ihlallerde yüksek idari para cezaları; yönetim için kişisel sorumluluk riski.

Tehdit azaltma etkisi: hesap verebilirlik + raporlama disiplini, riski görünür ve yönetilebilir kılar.

CFE | Academy

Finans için operasyonel dayanıklılık — 5 sütun

STANDART 3 · DORA (AB TÜZÜĞÜ)

17 Ocak 2025'ten beri doğrudan yürürlükte (geçiş süresi yok). 2026'da kuruluşların yalnızca ~%50'si tam uyumlu — denetim yoğunlaşıyor.

1

ICT risk yönetimi

Uçtan uca risk çerçevesi

2

Olay raporlama

Standart, zamanında bildirim

3

Dayanıklılık testi

Tehdit-temelli (TLPT) testler

4

3. taraf riski

Kritik ICT sağlayıcı gözetimi

5

Tehdit paylaşımı

Sektörel istihbarat değişimi

Kasım 2025: 19 kritik ICT sağlayıcı (AWS, Azure, Google Cloud…) doğrudan AB denetimine alındı. Ciddi ihlal cezası: cironun %10'una veya 10M €'ya kadar; üst yöneticide 1M €'ya kadar.

Yapay zekâ yönetimi — GRC'nin yeni cephesi

STANDART 4 · ISO/IEC 42001:2023

Dünyanın ilk AI yönetim sistemi (AIMS) standardı. **AB AI Act ile birlikte (yüksek riskli sistemlerde uygulama Şubat 2026'da başladı)** yapay zekâ artık formel GRC kapsamına giriyor.

AI bir tehdit yüzeyi

Model zehirleme, prompt injection, veri sızıntısı, halüsinasyon. ISO 42001 bu riskleri yönetim döngüsüne sokar.

AI bir savunma aracı

Anomali tespiti, otomatik müdahale, davranış analizi. Yönetilen AI, tehdit azaltmayı hızlandırır.

Güven & hesap verebilirlik

Şeffaflık, insan gözetimi, sürekli izleme. Tedarikçi seçiminde yeni güven ölçütü.

Tehdit azaltma etkisi: AI'ı yasaklamadan, denetlenebilir ve güvenli biçimde ölçeklemenin çerçevesi.

Dört standart → tek bir tehdit azaltma motoru

SENTEZ

Standart	Kapsam / Kim	Tehdit Azaltmaya Somut Katkı	Durum (2026)
ISO 27001:2022	Tüm sektörler	Threat intel + sürekli izleme + güvenli geliştirme	**Zorunlu geçiş tamam**
NIS2	Kritik & önemli sektörler (AB)	Yönetim sorumluluğu + 24/72s raporlama + tedarik zinciri	**Denetim başladı**
DORA	Finans + ICT sağlayıcılar (AB)	Dayanıklılık testi + 3. taraf gözetimi + olay raporlama	**Yürürlükte (2025)**
ISO 42001	AI kullanan/ üreten kurumlar	AI risk yönetimi + insan gözetimi + şeffaflık	**Hızla yaygınlaşıyor**

Ortak payda: hepsi GRC'yi statik uyumdan, ölçülen ve sürekli işleyen bir tehdit azaltma sistemine dönüştürür.

GRC'yi tehdit azaltmaya çeviren 5 adım

UYGULAMA

1 · Sahiplen

Yönetim kurulu seviyesinde sahiplik ve risk iştahını tanımla.

2 · Eşleştir

Standart kontrollerini tek bir çerçevede birleştir (bir kez yap, çok kez kullan).

3 · İzle

Tehdit istihbaratını kontrollere besle; sürekli izleme kur.

4 · Test et

Tehdit-temelli testlerle savunmayı önceden kır ve öğren.

5 · Ölç & raporla

KPI/KRI ile etkiyi kanıtla; yönetime düzenli raporla.

Tek çerçeve, çok standart: aynı kontrolü dört rejime birden eşleyince hem maliyet düşer hem koruma güçlenir.

Yeni standartlar bir yük değil, tehdit azaltmanın işletim sistemidir.

- ✓ Uyumu "denetim" değil, sürekli işleyen bir tehdit azaltma disiplini olarak kurun.
- ✓ Dört standardı tek GRC çerçevesinde birleştirin — bir kez yapın, her yerde kullanın.
- ✓ Sorumluluğu yönetim kuruluna taşıyın; tehdit istihbaratını kontrollere besleyin.
- ✓ AI'ı yasaklamak yerine ISO 42001 ile denetlenebilir biçimde güvenceye alın.

TEŞEKKÜRLER

CFECERT

CFE | Audit CFE | Academy