



NIS2

Was IT-Entscheider jetzt konkret tun müssen

10.02.2026





Was mache ich hier eigentlich?

M365-Compliance-Experte & Datenschutzbeauftragter



Wo komme ich her?

Compliance-Projekte über Unternehmensgrößen, Branchen und Reifegrade hinweg



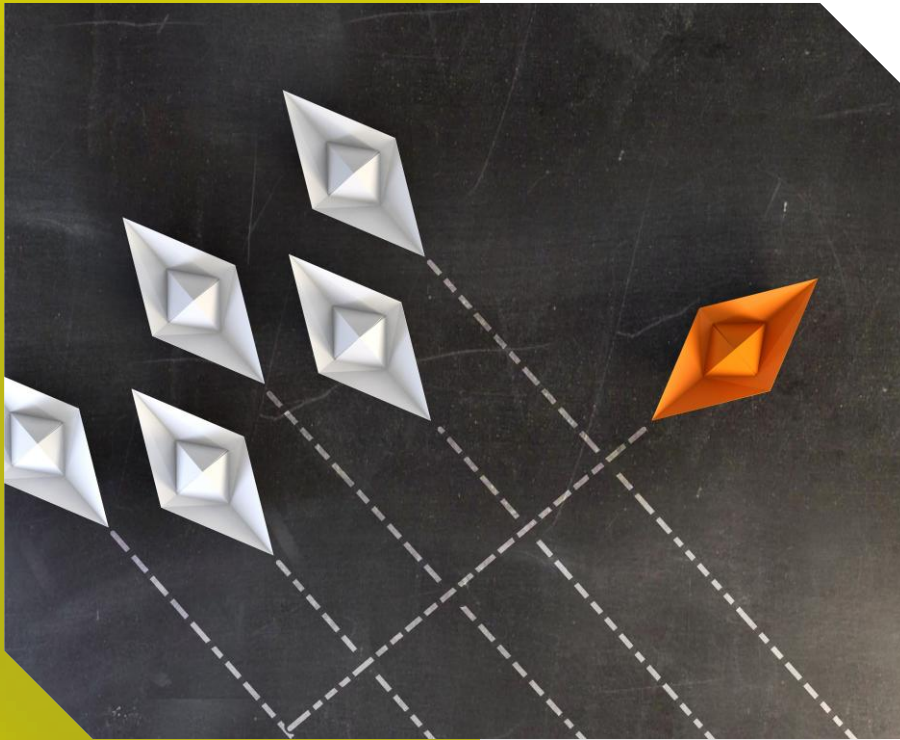
Wofür brenne ich?

Compliance von Menschen für Menschen



Was dürft ihr mitnehmen?

Orientierung & Entscheidungsgrundlagen



NIS2 ist kein Technikprojekt

Es ist ein verbindlicher
Ordnungsrahmen für den Betrieb.



Menschen

- Fehler, Gewohnheiten, Zeitdruck
- Legitimes Arbeiten ≠ sicheres Arbeiten



Identitäten

- Berechtigungen wachsen
- Rollen ändern sich schneller als Zugriffe



Zusammenarbeit & Lieferkette

- Externe Partner
- Geteilte Verantwortung
- Unklare Zuständigkeiten



Prozesse

- Informell entstanden
- Selten dokumentiert
- Kaum geübt (Incident)

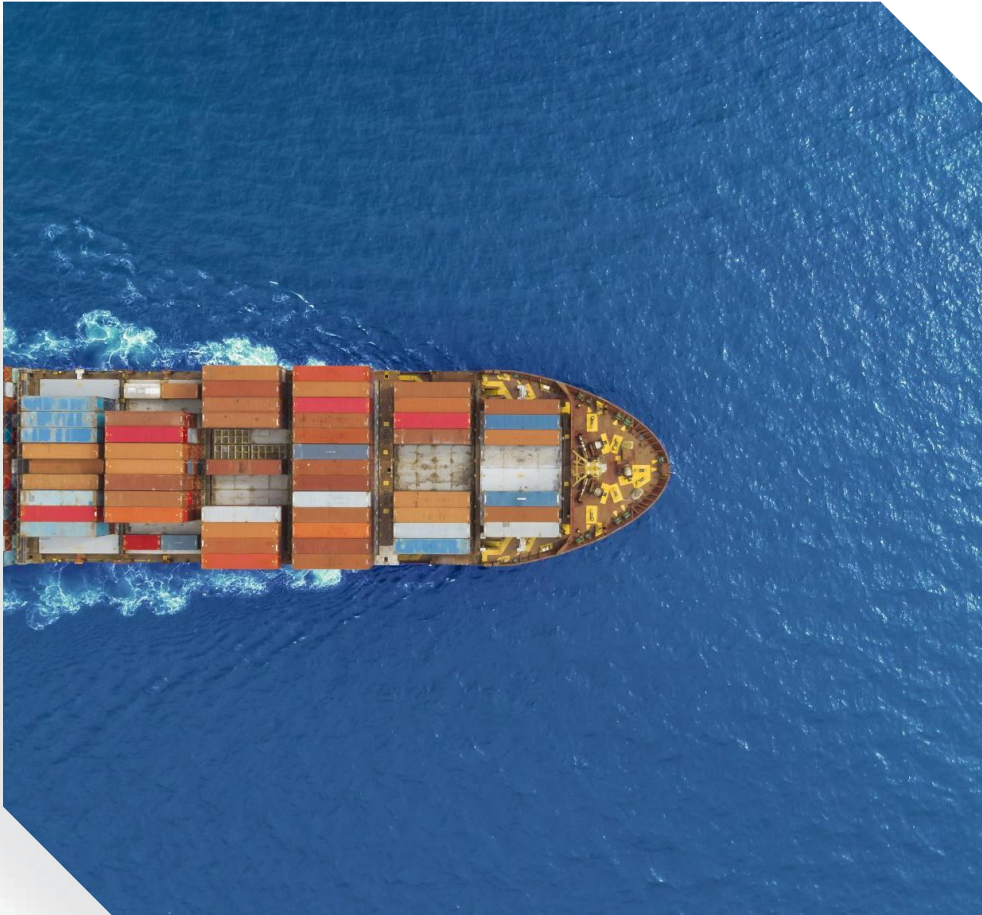
Typisch heute

- **Sicherheit wird als IT-Thema betrachtet**
- **Einzelmaßnahmen ohne Gesamtbild**
- **Verantwortung endet zu früh**

Stattdessen

- **Governance vor Technik**
- **Struktur vor Aktionismus**
- **Verantwortung klar verankern**

Wer ist betroffen?



Direkt betroffen

Wesentliche & wichtige Einrichtungen



Branchen

Energie, Gesundheit, IT, Industrie, Transport, digitale Dienste & verarbeitende Unternehmen



Größe

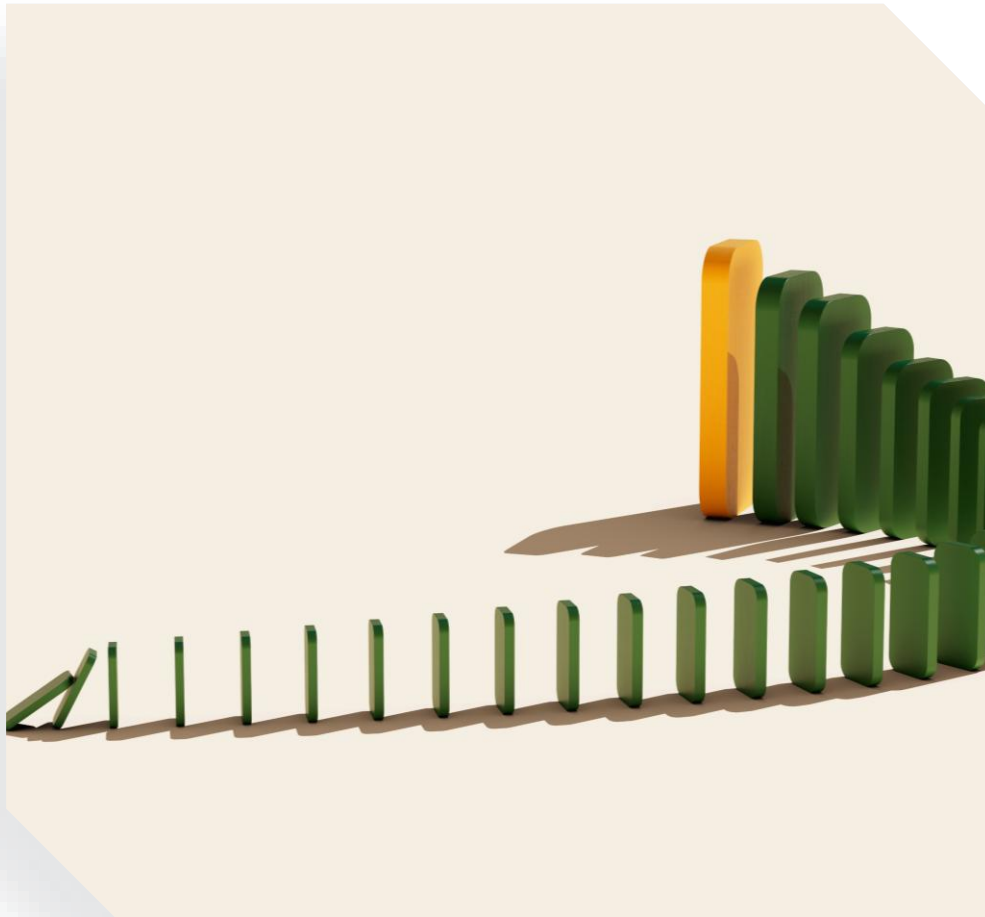
Ab 50 Mitarbeitenden oder 10 Mio. € Umsatz(je nach Branche)



Auch indirekt

Dienstleister, Zulieferer & IT-Partner nicht formal betroffen, aber durch Kunden, Lieferketten, Gesamtlandschaft





Funktionale Abhängigkeit

Wer ist real von uns abhängig?
bwE/wE Kunden, Kernprozesse betroffen, nicht optional



Substituierbarkeit

Wie leicht sind wir realistisch ersetzbar?
kurzfristige Alternativen, Komplexität des Wechsels



Ketten- & Bündelwirkung

Treffen wir viele gleichzeitig?
Kunden im selben kritischen Sektor, single point of failure



Wirkungsdimension

Was wäre die reale Auswirkung eines Incidents?
Versorgungssicherheit, öffentliche Sicherheit, Gesundheit



Aufsichtliche Plausibilität

Wie würde eine Behörde argumentieren?
plausibel begründbare Relevanz, Erklärungsbedarf,
öffentliche Wahrnehmung

Was NIS2 (nicht) verlangt

Gefordert

- Klare Struktur
- Definierte Prozesse
- Benannte Verantwortlichkeiten
- Nachvollziehbare Nachweise

Nicht gefordert

- Kein bestimmte Hersteller
- Keine maximale Tooltiefe
- Keine ISO-Zertifizierung o.ä.

Von Anforderungen zu messbaren Ergebnissen.



Automatisierte Checks

Tenant-Analyse:
Risiken sichtbar machen



Klarer Status

- Wo stehen wir?
- Was fehlt?



Handlungsempfehlungen

- Für IT
- Für Management



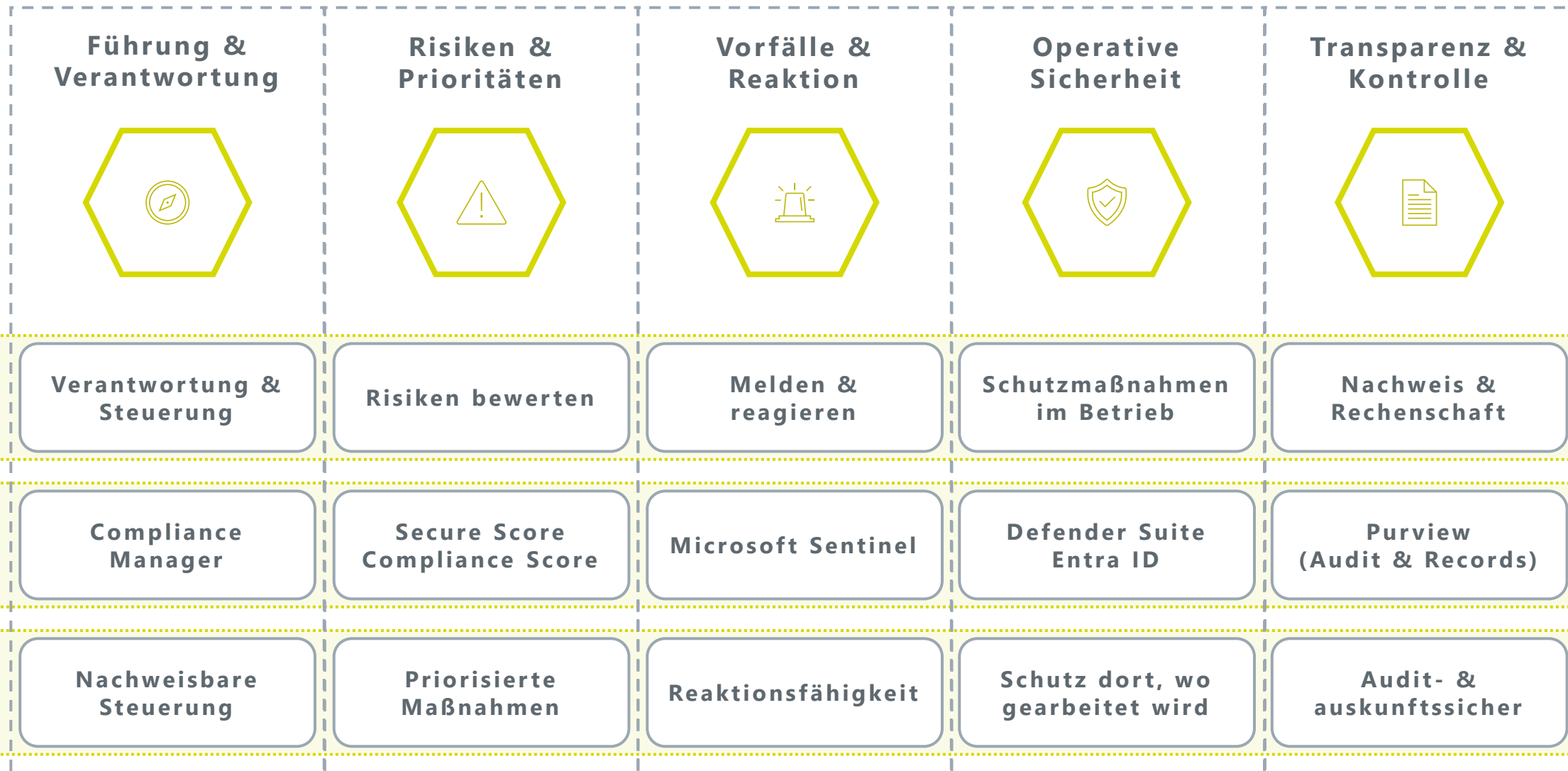
Umsetzung

z.B. mit clarios
(M365 Tenant Security Governance)



NIS2 → Microsoft 365

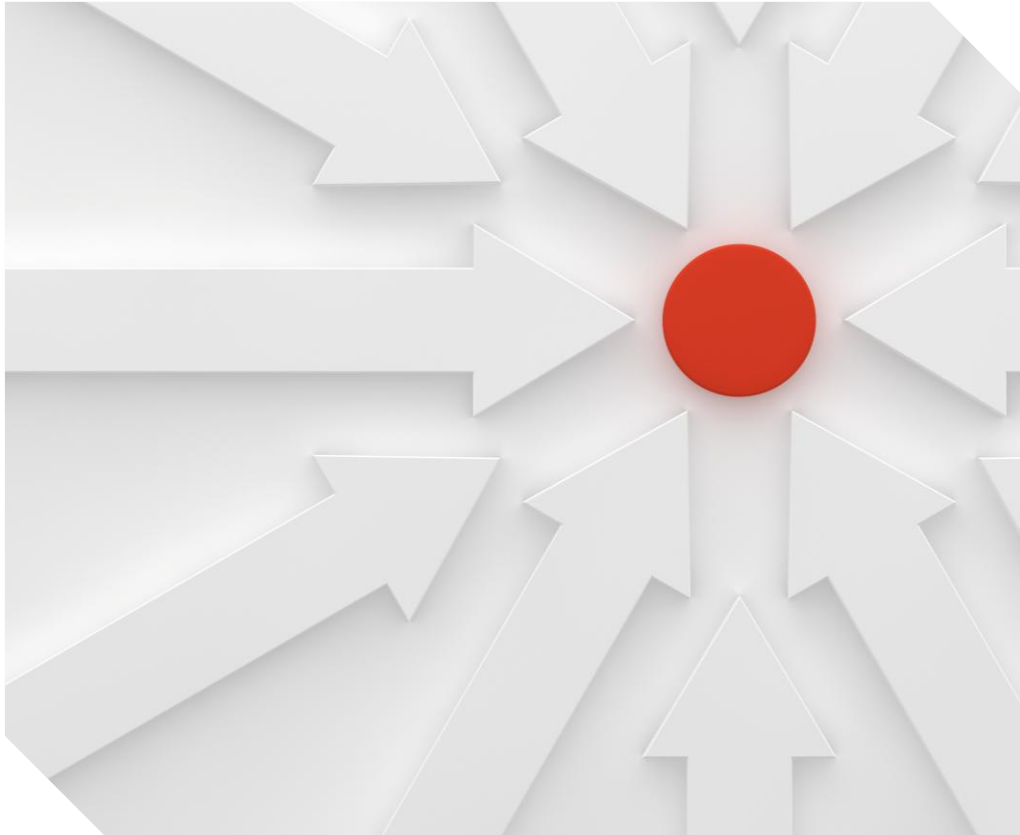
Von Pflichten zu messbarer Umsetzung



Wichtig: Diese Fristen sind nur einhaltbar, wenn ein Incident-Response-Prozess **vor dem Vorfall** definiert ist.



Verantwortung ist nicht delegierbar.



Verantwortung

Geschäftsführung trägt die Gesamtverantwortung
Delegation ≠ Haftungsabgabe



Haftung

Bußgelder bis 10 Mio. € / 2 % Umsatz (besonders wichtig)
bzw. 7 Mio. € / 1,4 % Umsatz (wichtig)
Persönliche Konsequenzen möglich



Incident-Pflichten

Melden · Reagieren · Dokumentieren
Fristen sind verbindlich!



Lieferkette

Verantwortung endet nicht am eigenen Tenant
Dienstleister & Partner einbeziehen



1) Betroffenheit prüfen

Betroffenenprüfung online durchführen
(BSI oder Transferstelle Cybersicherheit)



2) Registrierung durchführen

Falls betroffen: Registrierung im BSI Portal

Deadline: 06.03.2026



3) Gap-Analyse

Status Quo erfassen
Was existiert und ist dokumentiert?
Organisation? Prozesse? Technik?



4) Verantwortlichkeiten klären

NIS2-Owner festlegen
Aufgaben definieren
Budgets und Befugnisse offiziell zusichern



5) Risiken & Schwachstellen erfassen

Inventarisierung kritischer Systeme und Prozesse
Prozess für regelmäßige Risikoanalyse aufbauen



6) Incident-Response definieren

Playbooks und Meldekettten erstellen/dokumentieren
Incident-Response-Prozess testen



7) Dokumentation aufsetzen

Prozess- & Richtlinien-Dokumentation
Wirksamkeitsnachweise (Risiken, Entscheidungen, Maßnahmen)



8) Roadmap erstellen

Risiken priorisieren
Klar umrissene Maßnahmen definieren
Roadmap mit Ressourcen und Budget abgleichen



Fragen & Diskussion

Statt Bauchgefühl: Ein klarer, tagesaktueller Blick auf Sicherheits- und Compliance-Status im Microsoft-365-Tenant.



LinkedIn

Gerne Vernetzen
Einfach Nachricht schreiben
Im Austausch bleiben

[Link](#)



Kostenloses Sparring

25 Minuten für deine aktuelle
Herausforderung
Kostenlos & unverbindlich
Optional mit clarios Tenant Snapshot

[Link](#)

Weiterführende Links

[!\[\]\(7377a3302f3d0fb3a834bf90f4594228_img.jpg\) FitNIS2-Navigator \(Online-Betroffenheitsprüfung\)](#)

[!\[\]\(1ac7c971e7df5bf204fbb84fd617a50a_img.jpg\) Transferstelle Cybersicherheit – NIS2 Workshop am 03.03.2026](#)

[!\[\]\(397cc4c04b5e7ea225dbaa029a5dee1f_img.jpg\) BSI - nis2know-Infopakete](#)

[!\[\]\(115eff7009a76771e6b7adb966005e4c_img.jpg\) BSI - Entscheidungsbaum Betroffenheit](#)

[!\[\]\(a6eac08c103efb51b40f958fe35f07bb_img.jpg\) Transferstelle Cybersicherheit – Schlaglichtthema NIS2](#)

[!\[\]\(b73fbe1f68c0c0158be408bb873fa9d8_img.jpg\) Microsoft - NIS2-Compliance mit Microsoft Lösungen](#)

[!\[\]\(11b47853efe756d31c268612c0cc4217_img.jpg\) cubic solutions – clarios \(M365 Tenant Security Governance\)](#)