sync work

Beraten | Gestalten | Digitalisieren

Leistungsangebot Beratung

IT-Governance, Risk und Compliance

(IT-GRC)

Inhalt

1 ISACA®, Global Edition, State of Digital Trust 2024 Infographic, 20. Mai 2024
https://www.isaca.org

Impressum

Herausgeber:
Syncwork AG
Franklinstraße 26A
10587 Berlin

Bildquellen:
Alle Abbildungen
© Syncwork AG
Stand: Februar 2025

*Die 2024 von der ISACA durchgeführte **State of Digital Trust**-Untersuchung kommt zu einem eindeutigen Ergebnis: **81 Prozent** der Befragten sind der Meinung, dass sich die verpflichtende **Einhaltung der Digital Trust-Kriterien positiv auf den Erfolg auswirkt**.*[1]

Insbesondere für Organisationen, die im regulatorischem Umfeld tätig sind, wirkt sich eine robuste Governance-Struktur stabilisierend aus. Um eine Institution im dynamischen Gewässer lenken zu können, bedarf es drei zentraler Elemente:

Positionierung im Marktvergleich	**Definierte Richtung** für weitere Entwicklung, inkl. Leitplanken	**Kontrolle**, inwieweit wir die Vorgaben erfüllen

Die obigen Perspektiven sind besonders relevant für die IT sowie für die Gesamtorganisation. **Hierbei muss die IT-Governance auf die Governance der Gesamtorganisation abgestimmt sein.** Es gilt die inhärenten Risiken, die mit dem Einsatz der Informationstechnologie verbunden sind, zu berücksichtigen und die Aktivitäten gemäß der Risiken zu priorisieren. Schließlich spielt die Sicherheit der prozessierten und verwahrten Informationen eine entscheidende Rolle für die Stakeholder der Organisation, u. a. für regulatorische Organe und vor allem die Kunden.

Ob sich Kunden für eine Zusammenarbeit entscheiden, hängt in der Ära der digitalen Transformation oft vom digitalen Angebot der Anbieter ab. **Das wahrgenommene Vertrauen in die digitalen Dienste des Providers fließt in die Auswahlkriterien für eine potenzielle Kooperation ein.**

2024 führte die ISACA bereits ihre dritte Untersuchung mit dem Titel „State of Digital Trust" durch. **Dabei waren 82 Prozent der Befragten der Ansicht, dass dem Thema „Digital Trust" in fünf Jahren eine höhere Bedeutung zukommen wird.** Anderseits erhöhen lediglich 20 Prozent der befragten Unternehmen geplante Investitionen in diesem Bereich1. Unserer Meinung nach ist es an der Zeit, diese Lücke zu schließen und intensiver denn je in digitales Vertrauen zu investieren.

TREIBER UND FAKTOREN FÜR IT-GOVERNANCE PROZESSE

Aus Sicht der Regulatorik stellen zum aktuellen Zeitpunkt u. a. folgende Anforderungen die Organisationen vor die Aufgabe, erweiterten Kontrollmechanismen einzuführen:

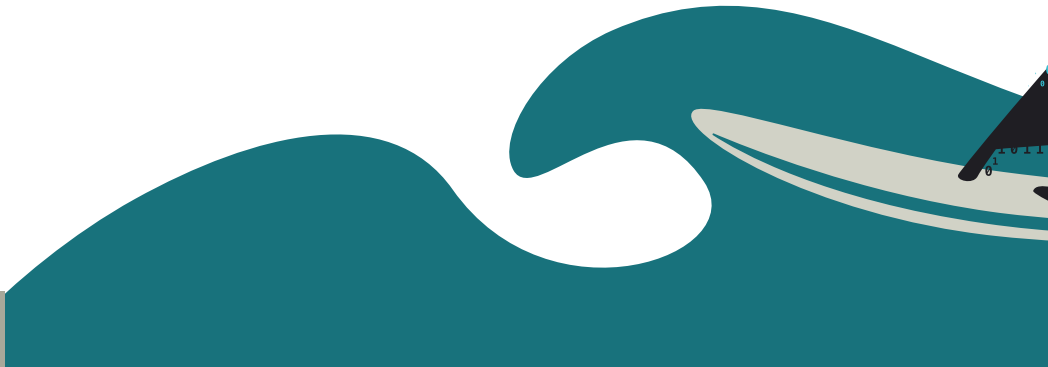
— **BaFin-Rundschreiben**, die sich an Finanzdienstleister richten

→ Bankaufsichtliche Anforderungen an die IT , die seitens BaFin schrittweise aufgehoben werden. (BAIT)

— **Digital Operational Resilience Act** (DORA) als eine finanzsektorweite Regulierung der Europäischen Union (EU) zur Reglementierung von

→ Cybersicherheit,
→ der Risiken, die mit Informations- und Kommunikationstechnologien verbunden sind
→ und der digitalen operationalen Resilienz

— **NIS-2** als EU-Richtlinie zur Erhöhung der Cyber-Resilienz von Unternehmen, die in unterschiedlichen Branchen tätig sind
— **Data Act** als EU-Verordnung mit der Zielstellung, den Austausch und die Nutzung von Daten innerhalb der Union zu harmonisieren
— **IT-Grundschutz, KRITIS** etc.



Eine **moderne IT-Governance-Struktur** soll technologische Trends und Veränderungen berücksichtigen und proaktiv zur Steuerung der damit verbundenen Initiativen beitragen.

Darunter fallen insbesondere:

— **Cloud**-Adoption
— **Steigende Komplexität** der Systemvernetzung
— **Erhöhte Menge an Daten**, die produziert, ausgetauscht und gespeichert werden
— Einsatz der **Künstlichen Intelligenz**

UNSERE LEISTUNGEN

Control Compliance

Anforderungs- und Testmanagement

- ☑ Anforderungsdefinition sowie Test- und Umsetzungskoordination

Projektmanagement und Project Management Office (PMO)

- ☑ Begleitung der Anbindung der IT-Assets an ein zentrales Monitoringsystem, inkl. kontinuierliche Verbesserung und dabei Steuerung eines Portfolios des IT-Asset-Bestands
- ☑ PMO im Kontext des Gesamtportfolios der IT-Assets im Projektscope
- ☑ Ergebnisdokumentation und -aufbereitung für Wirtschaftsprüfungszwecke und Abstimmung mit den Projektbeteiligten

Unsere Technologien:

- → **Security Information and Event Management** (SIEM) und andere System- und Datenintegration (z. B. **Identity and Access Management**)

Unsere Branchen:

- → Banking & Finance
- → Public Management

Unsere Qualität:

- → Langjährige Erfahrung aus der Projekttätigkeit im Rahmen der SIEM-Integration
- → **Methoden:** u. a. MITRE ATT&CK®, STRIDE

IT-Sicherheit

Analytische und konzeptionelle Tätigkeiten

- ☑ Erstellung Informationssicherheitskonzept in Anlehnung an IT-Grundschutz
- ☑ Erstellung Risikoanalyse – u. a. ISO 27005, OWASP Top Ten, IT-Grundschutz
- ☑ Abstimmung mit Stakeholdern (Entwickler, Datenschutzbeauftragter, Sicherheitsbeauftragter, Personalrat)

Kenntnisse:

- → fachliche und technische Erfahrungen aus bestehenden Projekten im Anwendungsumfeld

Unsere Branchen:

- → Public Management
- → Andere Branchen können nach Einzelbewertung betrachtet werden

Unsere Referenzen:

- → Senatsverwaltung für Mobilität, Verkehr, Klimaschutz und Umwelt (SenMVKU)
- → Gesellschaft für innovative Beschäftigungsförderung mbH (G.I.B.)


Lassen Sie uns gemeinsam dynamische IT-GRC-Strategien entwickeln, die Sicherheit stärken und auf zukünftige Risiken vorbereiten.
Wir freuen uns über Ihre Nachricht!
syncwork.de/kontakt

NUTZEN FÜR DEN KUNDEN

Der Kunde mitsamt seiner Bedürfnisse steht bei uns im Mittelpunkt:

- In der Anfangsphase der Zusammenarbeit bauen wir auf dem vorhandenen Risikosteuerungskonzept der Kundenorganisation auf. Dabei legen wir **konstruktive Vorschläge zur kontinuierlichen Verbesserung** des Risikomanagements vor.
- Sektor- und Kundenspezifische Vorschriften und Governance-Anforderungen werden bei gemeinsamen Aktivitäten stets von uns beachtet.
- Die IT-GRC Prozesse werden aufgebaut **unter Berücksichtigung der verfügbaren technologischen Grundlage** (On-Premises, Cloud, Hybrid Cloud). Dabei reflektieren wir die Projektzielsetzung in Anlehnung an die Geschäftsstrategie bei jedem Schritt.
- Wir betreiben **kontinuierlichen Know-how-Transfer** im Projekt.
- Wir bieten einen ganzheitlichen Beratungsansatz. Dabei unterstützen wir den gesamten Prozess beim Kunden, von der Vorbereitung über die Umsetzung bis zum kontinuierlichen Verbesserungsprozess.
- Wir bringen **branchenspezifisches Know-how** ein und berücksichtigen das Zusammenspiel von generellen und branchenspezifischen Regelungen (z. B. DORA im Finanzsektor)

Sie möchten mehr über unser Leistungsangebot auf dem Gebiet IT-GRC erfahren? Wir nehmen uns die Zeit, um Ihre individuellen Anforderungen und Wünsche zu besprechen.

Kontaktieren Sie uns einfach!

Ihre Ansprechpartner:

Ondřej Kotik
Management Consultant / Teamleiter
Banking & Finance

M +49 151 544 183 29
kotik@syncwork.de

Sam Jonas Niro
Consultant
Banking & Finance

M +49 151 544 183 19
samjonas.niro@syncwork.de

Syncwork AG
Franklinstraße 26a
10587 Berlin

syncwork.de