We Love Ingredients.

IT-Security@AZO

Die Roadmap zur erfolgreichen Zertifizierung nach ISO27001

Jörg Märker
Teamleiter IT-Infrastruktur & Security
Tel: +49 6291 92253
E-Mail: joerg.maerker@azo.com

Wo kommen wir her…?

- Bis 2018 hatten wir eine IT-Sicherheit nach damaligem Stand der Technik.
  - Firewall
  - Antivirus
  - Backup
- Risiken beschränkten sich im Wesentlichen auf die Verfügbarkeit von Systemen und Informationen
- Vorfälle bestätigten die Wirksamkeit der Maßnahmen
  - 2000 Ausbruch des Wurms „I-Love-You“ in USA
    - Exchange Server war am Anschlag (DOS)
    - Netzwerktrennung, Bereinigung der Postfächer
  - 2005 Hardwareausfall mit Datenverlust beim ERP-System
    - Wiederherstellung aus Backup
  - 2017 Crypto-Trojaner auf einem Client (Download über Dropbox-Link)
    - 400.000 verschlüsselte Dateien auf einem Netzwerklaufwerk innerhalb von 45 Minuten.
    - Isolation des infizierten PCs + Recovery aus SnapShots (NetApp)
- Bis dahin waren komplexe mehrstufige Angriffe kein verbreitetes Problem. Keine Exfiltration. Keine laterale Ausbreitung.

Cyber-Bedrohungen & Ransomware: Wichtige Entwicklungen seit 2015

2015–2017: Aufstieg der Ransomware

- Angriffe wie WannaCry (2017) und NotPetya (2017) markierten den Beginn weit verbreiteter, zerstörerischer Ransomware.
- Staatlich unterstützte Cyberangriffe nahmen zu (z. B. Russland, Nordkorea).

2018–2020: Zielgerichtete Angriffe & Kritische Infrastruktur

- Gesundheitswesen, Energie und öffentliche Verwaltung wurden zu Hauptzielen.
- Die COVID-19-Pandemie führte zu einem Anstieg von Phishing und Social Engineering.

2021–2023: Professionalisierung & Monetarisierung

- Ransomware-as-a-Service (RaaS) wurde weit verbreitet.
- Lieferkettenangriffe (z.B. SolarWinds) und Angriffe auf Cloud-Dienste nahmen zu.

2024–2025: KI, Deepfakes & Cyberkrieg

- Anstieg von KI-gesteuertem Phishing und Deepfake-Desinformation.
- Cyberkrieg wurde Teil militärischer Konflikte (z. B. Russland–Ukraine).
- Automatisierte Angriffe erreichten Geschwindigkeiten von bis zu 36.000 Scans pro Sekunde.

Veränderungen der regulatorischen Anforderungen

- 2018 – Inkrafttreten der DSGVO
  - Ziel: Schutz personenbezogener Daten in der EU.
  - Auswirkungen: Einführung von Datenschutzbeauftragten, Dokumentationspflichten, Meldepflichten bei Datenpannen

- 2022 – Verabschiedung der NIS2-Richtlinie
  - Ziel: EU-weite Cybersicherheitsstandards für mehr Unternehmen
  - Betroffene: ca. 30.000 Unternehmen in Deutschland
  - Neue Anforderungen:
    - Risikomanagement und Nachweispflichten
    - Meldepflichten bei Sicherheitsvorfällen
    - Registrierungspflicht beim BSI
  - Umsetzung der NIS2 in nationales Recht: Ende 2025 oder Anfang 2026

- 2024 – Cyber Resilience Act (CRA) beschlossen
  - Ziel: Cybersicherheit für digitale Produkte über den gesamten Lebenszyklus
  - Anforderungen:
    - „Security by Design“
    - Schwachstellenmanagement und Patch-Pflicht
    - Dokumentations- und Meldepflichten

Erste Erkenntnis: „Die Bedrohungen verändern sich“

„Traditionelle IT-Sicherheit reicht nicht mehr aus“

- Klassische Schutzmaßnahmen wie Firewall & Antivirus sind nicht mehr ausreichend
- Bedrohungslage verändert sich dynamisch und dauerhaft
- IT-Sicherheit wird zur strategischen Notwendigkeit für den Fortbestand des Unternehmens
- Ein wirksames Informationssicherheitsmanagement wird zur gesetzlichen Pflicht

Zweite Erkenntnis: „Sicherheit braucht Systematik“

„Systematik statt Einzelmaßnahmen – aber nicht um der Norm willen“

- Risiken systematisch identifizieren und minimieren
- Angemessene, am Bedarf der Geschäftsprozesse ausgerichtete Sicherheit
- ISO 27001 ist global anerkannt und lässt genügend Spielraum
- Bürokratie vs. echte Sicherheitswirkung: Entscheidung gegen sofortige Zertifizierung
- Orientierung an der Norm als Strukturhilfe – nicht als Ziel

„Nicht das Zertifikat macht uns sicher – aber der Weg dorthin zwingt uns, Sicherheit systematisch zu denken.“

Erkenntnisse über die Norm: „Es ist mehr als ein IT-Problem“

„Die ISO-27001-Zertifizierung schützt uns vor Angriffen.“
Falsch: Schutz entsteht durch wirksame Maßnahmen, nicht durch das Zertifikat.

„Mit dem Zertifikat sind alle Risiken beseitigt.“
Falsch: Die Zertifizierung bestätigt nur, dass ein ISMS existiert und funktioniert – Risiken bleiben bestehen.

„Die Zertifizierung ist ein einmaliges Projekt.“
Falsch: ISO 27001 erfordert kontinuierliche Überwachung, *Verbesserung und regelmäßige Audits.*

„Das Zertifikat ist der Nachweis für technische Sicherheit.“
Falsch: Es belegt die Einführung eines Managementsystems, nicht die Wirksamkeit einzelner Tools.

„Technische Maßnahmen allein reichen aus.“
Falsch: Die Norm umfasst auch organisatorische und prozessuale Aspekte.

„ISO 27001 ist ein reines IT-Thema.“
Falsch: Die Norm betrifft die gesamte Organisation, inklusive Prozesse, Menschen und physische Sicherheit. IT-Sicherheit ist nur ein Teilbereich. Informationssicherheit ist eine Managementaufgabe und erfordert unternehmensweite Beteiligung.

Bewusstsein wächst Unternehmen: „Informationssicherheit ist kein IT-Problem“

„Vom IT-Thema zum Unternehmensziel“

- IT erkannte früh die Notwendigkeit – aber das Unternehmen brauchte Zeit
- Informationssicherheit betrifft alle Geschäftsprozesse – nicht nur Technik
- Schrittweise Bewusstseinsbildung im Unternehmen

„Weder IT noch Informationssicherheit existieren zum Selbstzweck. Wie die IT die digitale Basis für unsere Geschäftsprozesse schafft, sorgt die Informationssicherheit dafür, dass diese Prozesse geschützt, rechtskonform und störungsfrei ablaufen können.“


ISO
27001

Ernüchterung beim ersten Anlauf: „ISO 27001 ist kein Selbstläufer“

„Die Einführung der ISO 27001 bindet Ressourcen und man benötigt einen passenden Partner.“

- Erster Anlauf um 2019 (…nicht mit dem richtigen Partner)
- Stures Vorgehen nach Normkapiteln
- „Viel Bürokratie“ – Ressourcen wurden gebunden
- Kaum kurzfristig erzielbarer Sicherheitsgewinn

➔ Projekt wurde abgebrochen

Pragmatisches Vorgehen: „Fokus auf IT-Security-Maßnahmen“

„Überwiegend technisch orientiertes Vorgehen von der IT getrieben.“

- 2018–2020: Sicherheit vor Papier
  - Bewertung von technischen Maßnahmen im Kontext der geänderten Bedrohungslage
  - Implementierung von Einzelmaßnahmen mit direktem Sicherheitsgewinn
  - Orientierung an den Controls der ISO 27001 → Konformität
  - Hilfestellung durch NIST CSF 2.0: Identify, Protect, Detect, Respond, Recover (kein Widerspruch zur ISO 27001)

Systematisches Schließen von Lücken: „Überprüfung der Ist-Situation“

„Der kritische Blick auf die Ist-Situation mit Unterstützung externer Experten.“

- 2021: Security-Workshop
  - Identifizierung von Schwächen
  - Priorisierung der Maßnahmen
  - Systematische Bearbeitung der Maßnahmen
    (Tiering, Segmentierung, Backupstrategie, Einschränkung administrativer Berechtigungen…)

Entscheidung pro ISO 27001: „Jetzt sind wir bereit“

„Die Zeit ist reif für die Zertifizierung“

- Gründe für die Zertifizierung
  - Weitere Verbesserung der Informationssicherheit erfordert ein Managementsystem zur effektiven und effizienten Steuerung der Maßnahmen
  - Nachweis gegenüber Kunden zur Einhaltung deren Richtlinien
  - Erbringung von Nachweisen zur Informationssicherheit im Rahmen gesetzlicher Compliance-Anforderungen
- Durchführung einer Gap-Analyse zur ISO 27001
- Entscheidung für den Projektstart 1/2025

Aufbau des ISMS nach ISO 27001: „Das Projekt startet“

„Die systematische Bearbeitung der Normkapitel beginnt“

- Projektplan mit Zertifizierungsziel Q4/2024
- Dokumentensatz zur Orientierung
- Abgleich mit dem laufenden IEC 62443 Projekt
- Aufbau der Organisation
- Stage 1 Audit Q4/2025
- Planung Stage 2 Audit und Erstzertifizierung auf Q1/2025

Erfolgreiche Erstzertifizierung 2025

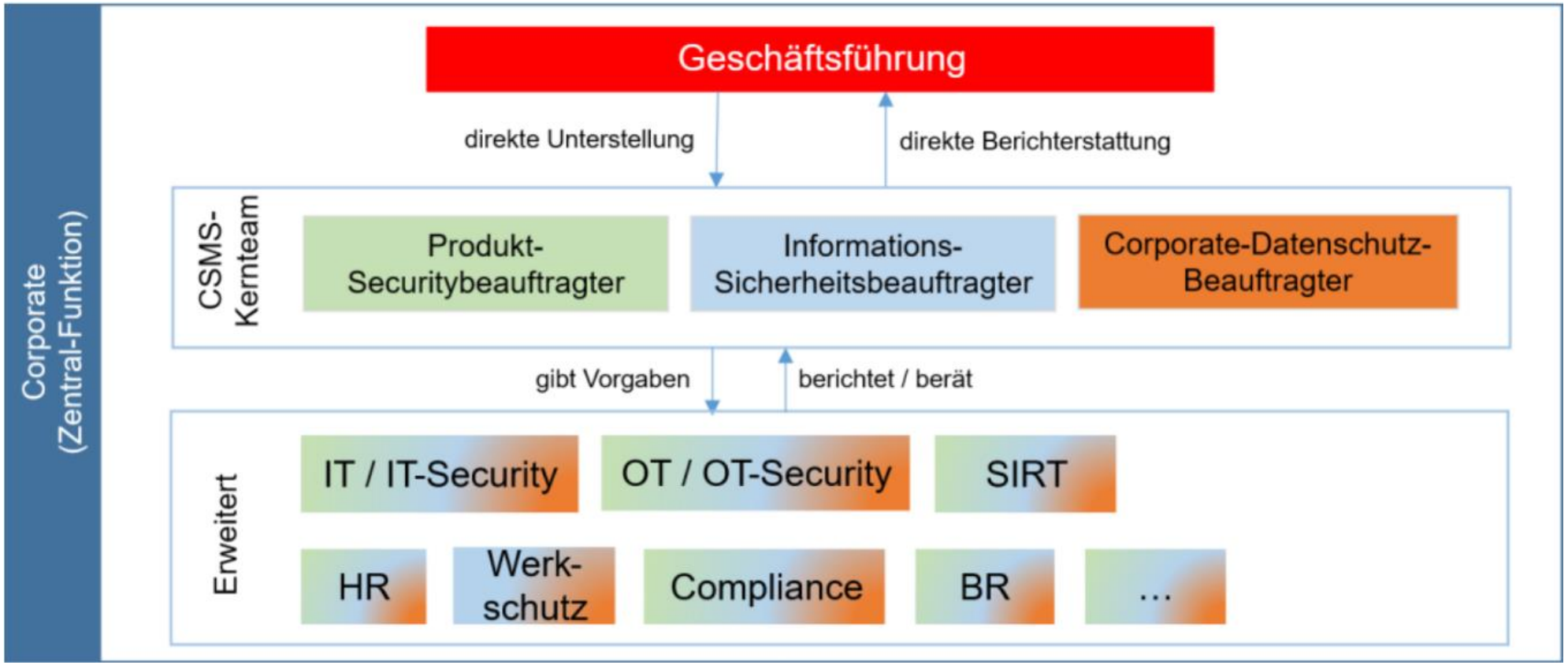
„… und die Erkenntnis: Nach dem Audit ist vor dem Audit!“

Das Ergebnis: „Wo stehen wir heute?“

- Erfolgreiche Erstzertifizierung (in Time & in Budget)
- Kunden reagieren positiv auf die Zertifizierung
- Synergie mit IEC 62443 in folgenden Bereichen:
  - Organisation
  - Sichere Softwareentwicklung
  - Schwachstellenmanagement
  - Incident-Management
  - Aufbau und Struktur aller Richtlinien (z.B. einheitliche Klassifizierung)
- Richtlinien sind in Kraft
- ISMS Prozesse sind aktiv
- Mitarbeiter sind geschult

Die Organisation: „Wie sind wir organisiert?“

„Aus ISMS und SPLMS wird CSMS.“



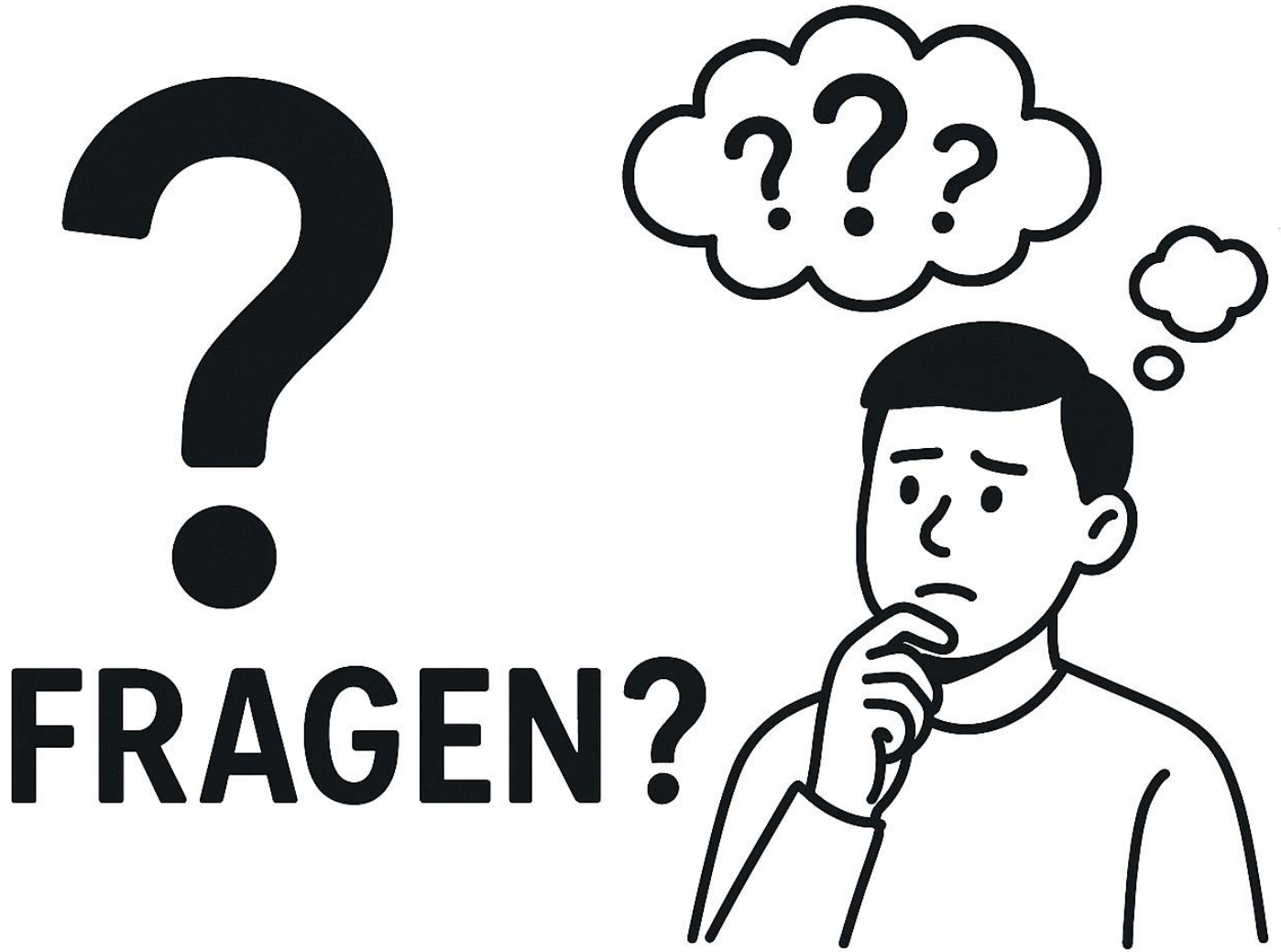
Die Erfolgsfaktoren: „Wie haben wir das geschafft?“

„Am Ende sieht es ganz einfach aus.“

- Reifegrad zum Start – „Der richtige Schritt zum richtigen Zeitpunkt“
- Unterstützung der Geschäftsführung – „Ohne Rückendeckung geht’s nicht“
- Der passende Partner
- Ein gutes Team
- Aufbau einer handlungsfähigen Organisation gleich zum Projektstart
- Trennung von ISB und IT

Ausblick: „Wie geht es jetzt weiter?“

- Nach dem Audit ist vor dem Audit (OFIs bearbeiten)
- Kontinuierliche Verbesserung der Informationssicherheit
- Informationssicherheit als Wettbewerbsvorteil nutzbar machen
- Scope international ausweiten
- Zertifizierung nach IEC 62443 abschließen


FRAGEN?