ISMS im Kontext OT und NISG

Bernhard Heinzle | Devoteam Consulting
Reinhard Kucera | VERBUND

IT-SECX 2019
FH St. Pölten, 08.11.2019

Agenda

- IT vs. OT - Begriffsklärungen
- Gesetzliche Landschaft in AT und DE
- Anforderungen an die Definition des Geltungsbereichs
- Anforderungen an das Risikomanagement
- Erfahrungsbericht VERBUND
- Prüfung und Nachweiserbringung

Überblick Devoteam Consulting

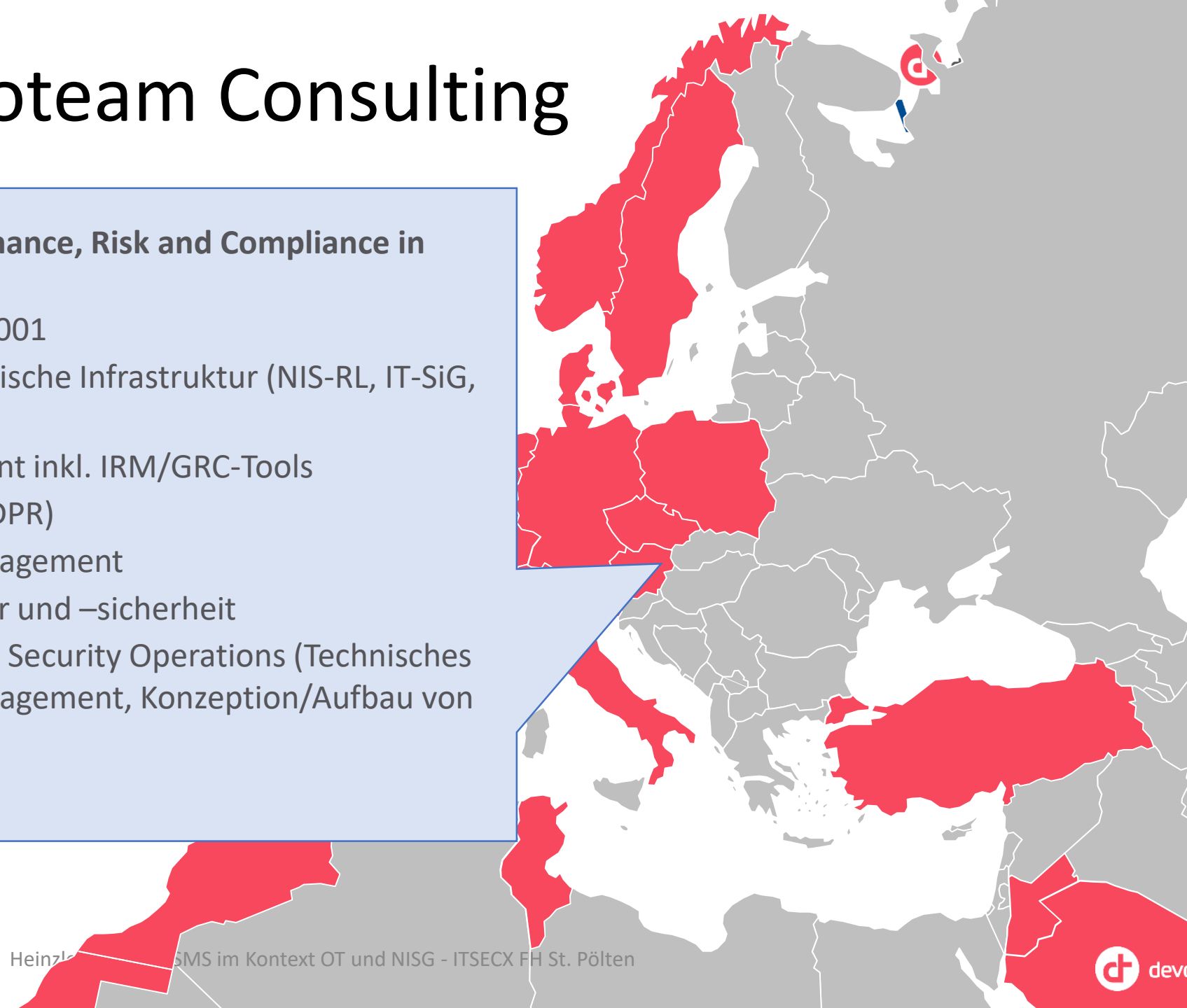
7.200
Mitarbeiter

652 Mio.€
Umsatz 2018

18
Länder

Practice Area Governance, Risk and Compliance in Österreich

- ISMS gemäß ISO 27001
- IS in der OT und kritische Infrastruktur (NIS-RL, IT-SiG, NIS-G)
- IT-Risikomanagement inkl. IRM/GRC-Tools
- Datenschutz (EU-GDPR)
- BCM, IT-Notfallmanagement
- Netzwerkarchitektur und –sicherheit
- Prozesse im Bereich Security Operations (Technisches Schwachstellenmanagement, Konzeption/Aufbau von SOCs, …)
- …



VERBUND auf einen Blick

devoteam

Verbund

~95%
Erzeugung aus erneuerbaren Energien

51%
im Besitz der Republik **Österreich**

~469.000 Privatkunden
Nr. 1 bei Industriekunden

Erster rein nach **Nachhaltigkeit** bewerteter Kredit weltweit

Verbund Verbund
2.700
Mitarbeiter

Österreichs **führendes Stromunternehmen**

Nummer 1 beim **Klimaschutz** unter europäischen EVUs

Energienahe
Produkte & Dienstleistungen

Österreichweite SMATRICS **Ladeinfrastruktur** für E-Fahrzeuge

Soziale Verantwortung:
2,5 Mio. € Unterstützung für VERBUND-Stromhilfefonds der **Caritas** seit 2009

Erste **Green-Bond-Unternehmensanleihe** im deutschsprachigen Raum

Starkes Umweltmanagement:
In den **Top 10** von weltweit 105 analysierten Energieunternehmen bei **oekom research**

128
Wasserkraftwerke

Ökologische Maßnahmen:
280 Mio. € Investition bis 2027

Größter Wasserkraft-Erzeuger **Bayerns**

Marktführer bei Flexibilitäts- und Grünstromvermarktung in Österreich und Deutschland

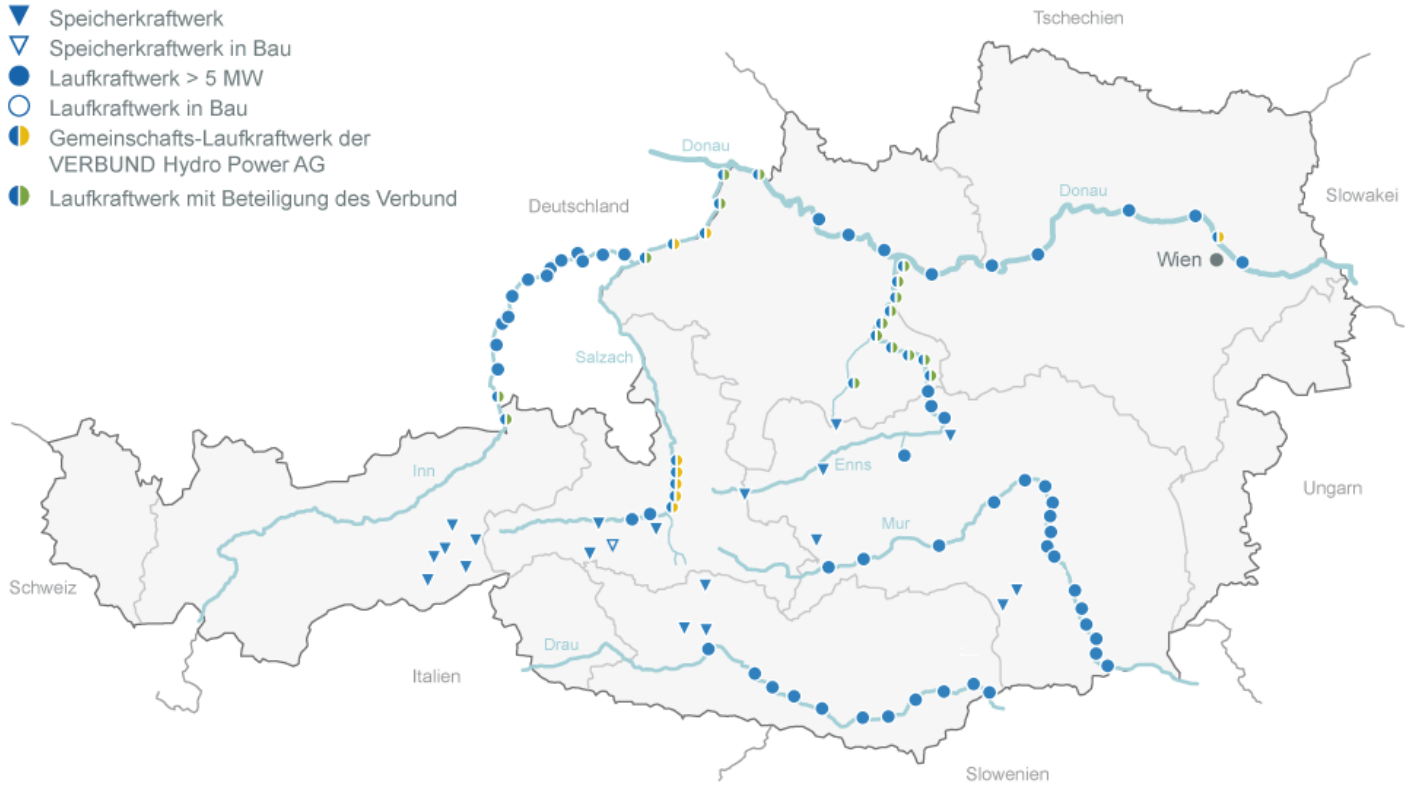
Strategischer Fokus
AT & DE

Börsenotiertes Unternehmen mit ausgezeichneter **Compliance-Kultur**

mehr als **2.000 Lehrlinge** in den vergangenen 70 Jahren ausgebildet

Kompetenz auf allen Wertschöpfungsebenen rund um Strom

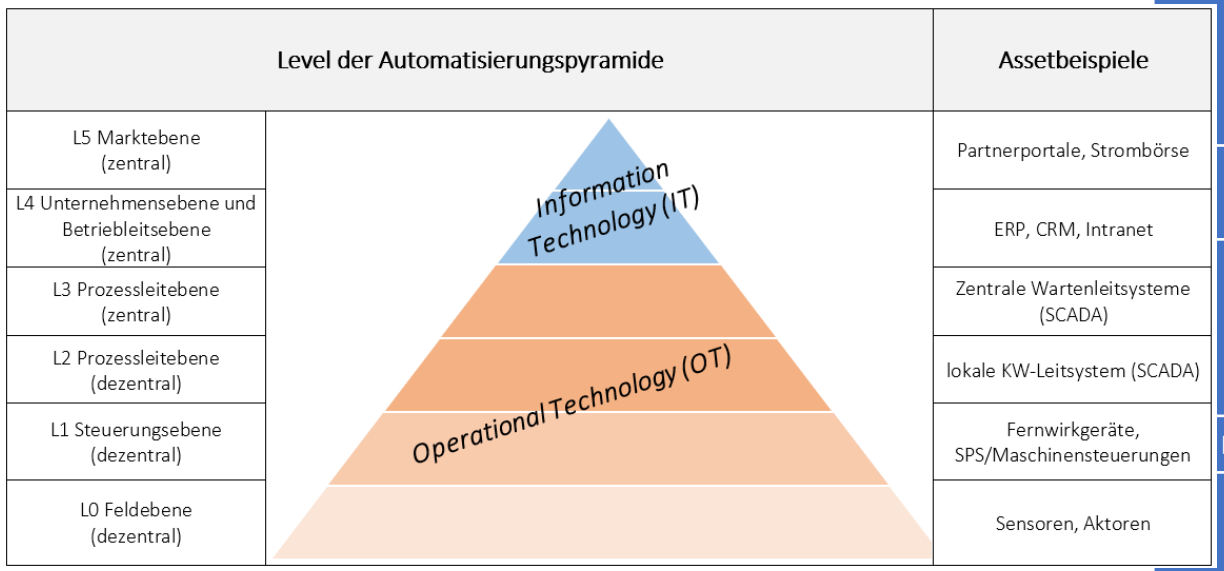
Mit Wasserkraft führend in Europa



VERBUND-Wasserkraft in Österreich und Bayern

- Führendes Stromunternehmen in Österreich
- Größter Erzeuger von Strom aus Wasserkraft in Bayern, Nr. 2 in Deutschland
- Eines der größten Wasserkraft-Unternehmen in Europa
- 128 Wasserkraftwerke in Österreich und Deutschland (Bayern) - Engpassleistung: 8.215 MW

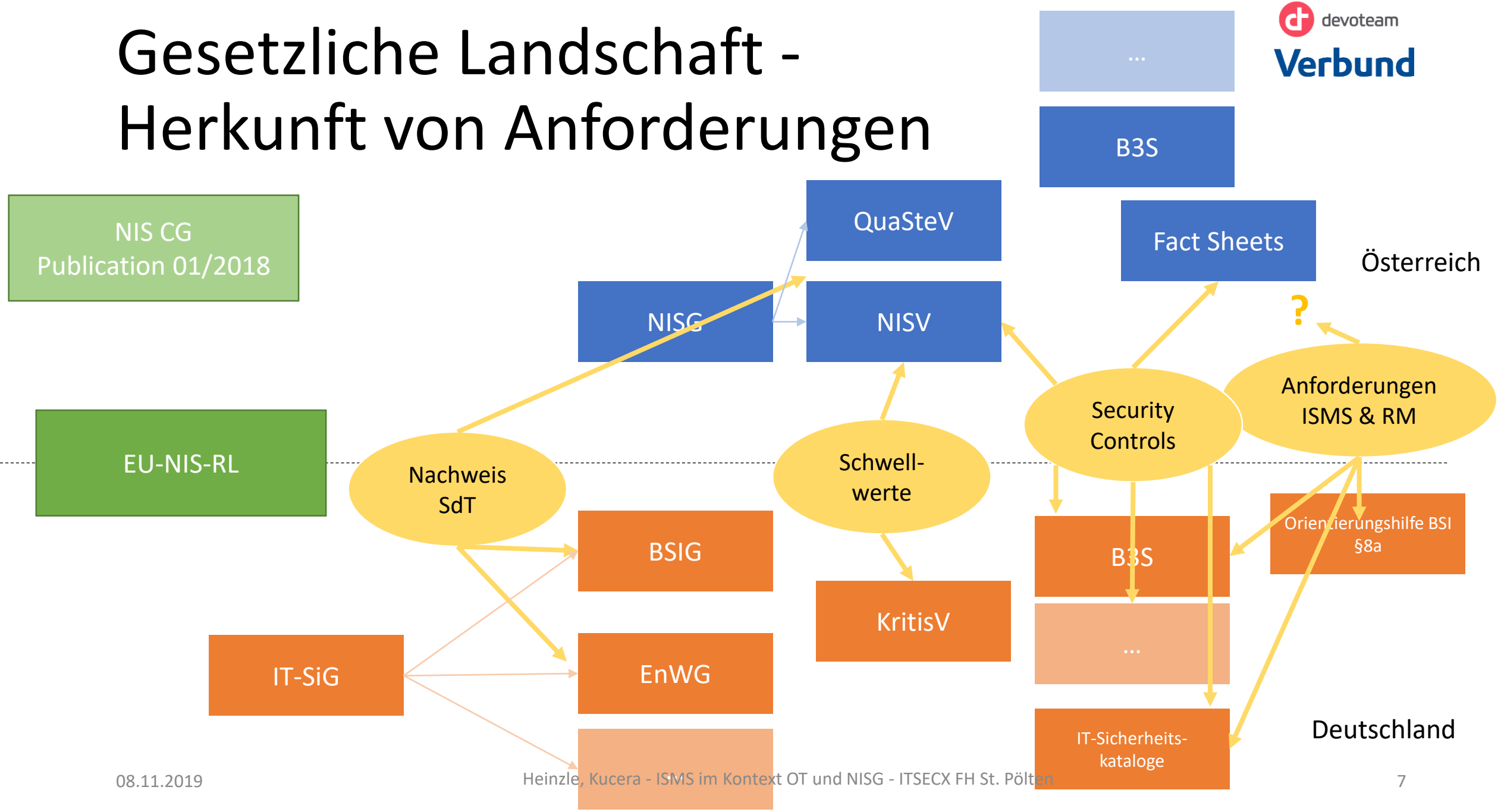
IT vs. OT - Begriffsdefinitionen



Quelle: Devoteam in Anlehnung an PERA/ISA-99/IEC 62264

Kategorie	IT	OT
Risiko/Auswirkung	Geschäftskritisch (finanziell, rechtlich,..) Datenverlust Supportprozesse	Kernprozesse (Erbringung wesentlicher Dienst) Auswirkung auf physische Prozesse Leib und Leben
Systembasis	Gängige Betriebssysteme	Oft proprietäre Betriebssysteme/Firmware
Change/Patch Management	Updates regelmäßig verfügbar	Updates selten verfügbar, kein zeitnahes Einspielen Seltene Update- und Wartungsfenster
Fokus Schutzziele	Vertraulichkeit, Integrität	Verfügbarkeit, (Integrität)
Entwicklung	Security oft im SDLC etabliert	Systeme lange Zeit als Inseln betrieben – Security als Anforderung „neu“
Produktressourcen	Ausreichend Ressourcen für Security-Funktionen	Knapp bemessene/nicht aufrüstbare Ressourcen
Produktlebenszyklus	3-5 Jahre Produktlebenszyklus	>10 Jahre Produktlebenszyklus
Systembetrieb	Sicherheitslösungen erhältlich und etabliert	Neuland für Sicherheitslösungen
Kommunikation	Etablierte Standardprotokolle mit Security Features	Proprietäre und Standardprotokolle oft ohne Security Features

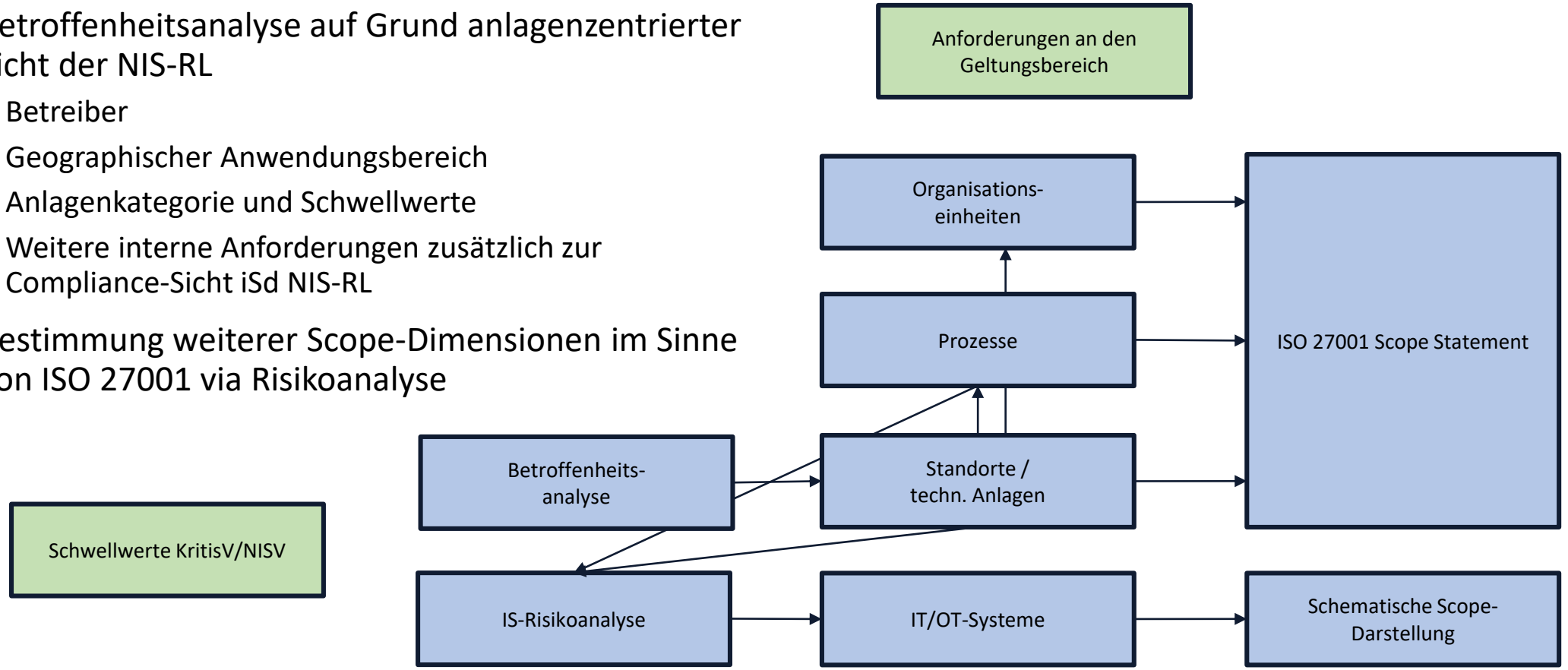
Gesetzliche Landschaft - Herkunft von Anforderungen



Definition des ISMS-Geltungsbereichs

Herangehensweise

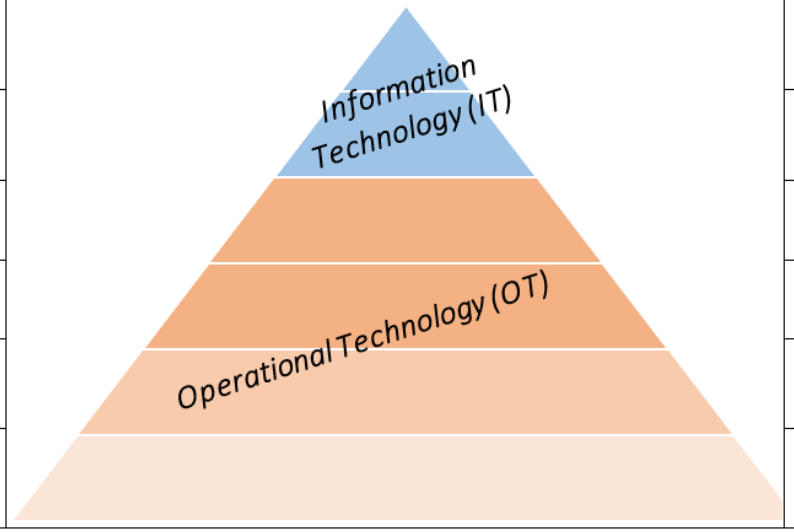
1. Betroffenheitsanalyse auf Grund anlagenzentrierter Sicht der NIS-RL
   - Betreiber
   - Geographischer Anwendungsbereich
   - Anlagenkategorie und Schwellwerte
   - Weitere interne Anforderungen zusätzlich zur Compliance-Sicht iSd NIS-RL
2. Bestimmung weiterer Scope-Dimensionen im Sinne von ISO 27001 via Risikoanalyse



Beispiele Abgrenzung Geltungsbereich und Automatisierungspyramiden

Abbildung 1: Zoneneinteilung von Anwendungen, Systemen und Komponenten in Energieanlagen (Quelle: in Anlehnung an VGB-Standard, S. 16)

Quelle: IT-Sicherheitskatalog § 11 Absatz 1b EnWG

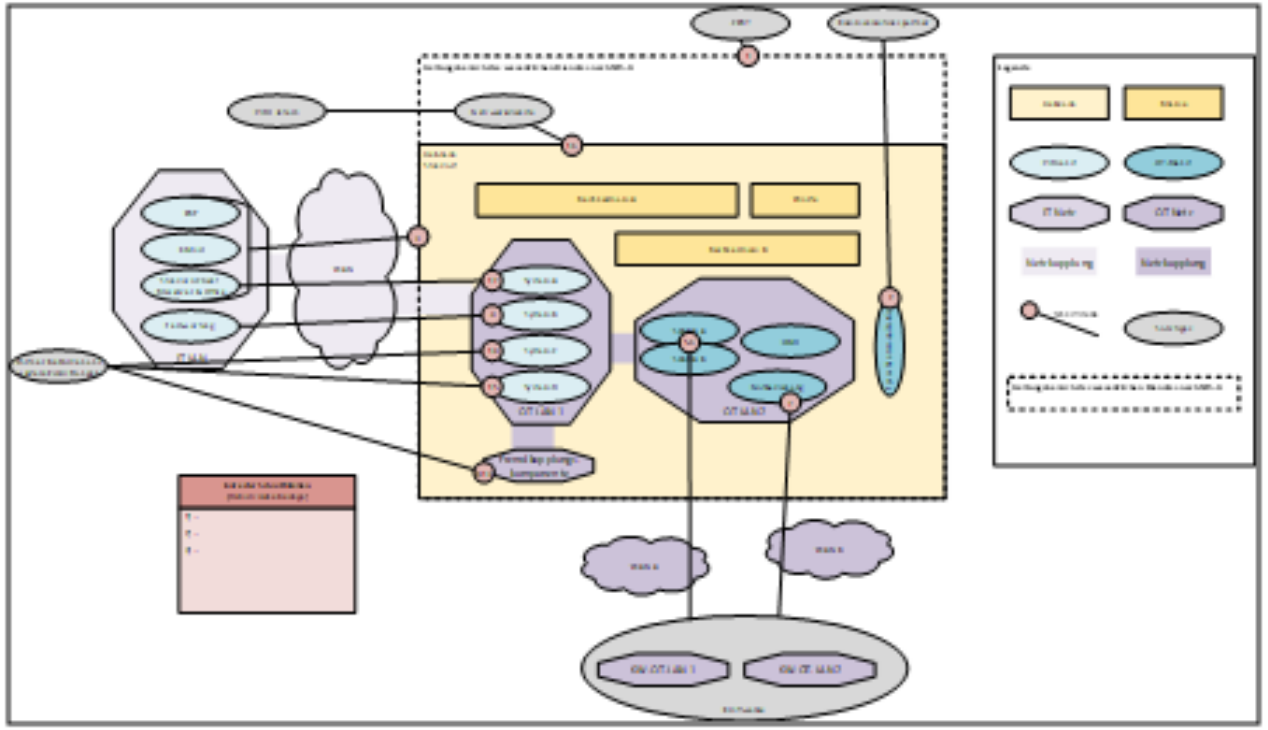
Level der Automatisierungspyramide		Assetbeispiele
L5 Marktebene (zentral)		Partnerportale, Strombörse
L4 Unternehmensebene und Betriebleitsebene (zentral)		ERP, CRM, Intranet
L3 Prozessleitebene (zentral)		Zentrale Wartenleitsysteme (SCADA)
L2 Prozessleitebene (dezentral)		lokale KW-Leitsystem (SCADA)
L1 Steuerungsebene (dezentral)		Fernwirkgeräte, SPS/Maschinensteuerungen
L0 Feldebene (dezentral)		Sensoren, Aktoren

Quelle: Devoteam in Anlehnung an PERA/ISA-99/IEC 62264

Anforderungen an die Dokumentation des Geltungsbereichs

- Anforderung an detaillierte Scope-Dokumentation ergibt sich aus:
  - BSI-Orientierungshilfe zu §8a BSIG
    oder
  - IT-Sicherheitskatalog gemäß §11 1a EnWG (Netzstrukturplan)

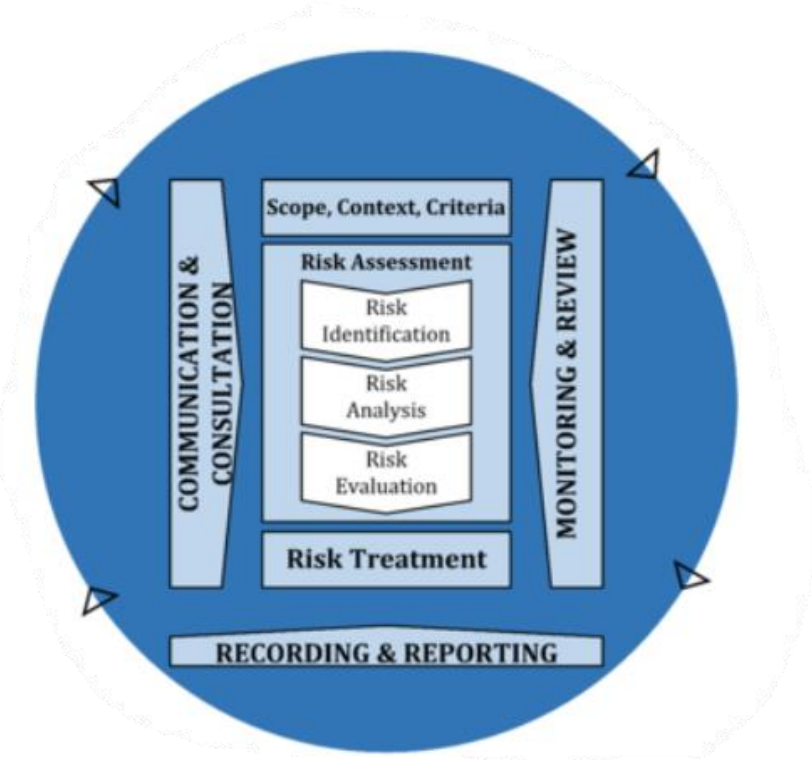
- Inhalte der Dokumentation
  - Anlage und kDL
  - Interne und externe Zuständigkeiten
  - Schnittstellen und Abhängigkeiten
  - Notwendige Systeme, Komponenten, Prozesse, Rollen, Organisationseinheiten



Anforderungen an das Risikomanagement

Erfahrungen aus deutschen Projekten und deren Relevanz für Österreich

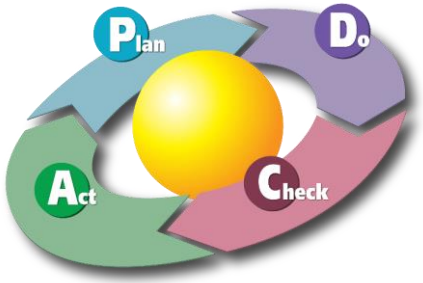
1. Auswirkung auf das Gemeinwesen vs. Auswirkungen auf den Betreiber *(NISV und BSIG)*
2. Abgrenzbarkeit von Risiken im NIS-Anwendungsbereich von anderen Risiken *(BSIG)*
3. Authentizität als 4. Schutzziel in RM-Methodik aufnehmen *(BSIG)*
4. bestimmte Gefährdungen berücksichtigen *(EnWG und DE-B3S)*
5. Verwendung vorgegebener Risikolevels *(EnWG)*
6. Risiken von / Abhängigkeiten zu Schnittstellen und Lieferanten explizit bewerten *(BSIG und NISV)*
7. Einschränkungen bei Risikoakzeptanz und Risikotransfer beachten *(BSIG und EnWG)*



Quelle: ISO 31000:2018

Erfahrungsbericht VERBUND

- Qualitative Risikoanalyse
- Tool „CRISAM“
  - Schneller Start möglich, Kataloge basierend auf ISO 270xx u. Branchen Best Practices (BDEW/OE Whitepaper)
- Vorgehensweise
  - Scope Definition
  - Festlegen eines Mindestsicherheitsniveaus „Stand der Technik“
  - Schutzbedarfsfeststellung (BIA)
  - Assetmodellierung / Risikobewertung (Kontrollfragen)
  - Maßnahmenvorschlag / Risikobehandlung
  - Management Review
- Lessons Learned
    - OT- und IT-Grundlagen beim jeweiligen Personal im Vorfeld angleichen
    - Quantitative Risikoanalyse möglichst von Anfang an mitbetrachten



Quelle: Karn G. Bulsuk

Erfahrungsbericht VERBUND Teil 2

- Veränderungen in der Organisation in den letzten Jahren
  - Am Beginn nur 1 FTE für Informationssicherheit (CISO)
  - Mit 2017/2018 Etablierung einer Security Abteilung
    - Derzeit (Nov. 2019) zentral 8 FTEs, Plan 2020 15 FTEs

- Aktueller Fokus auf:
  - Asset Management
  - Schwachstellenmanagement
  - Penetration Test und Red Teaming
  - ISMS und Security Governance
  - Patch Management
  - Netzwerksegmentierung/-architektur
  - Physische Sicherheit

Prüfung und Nachweiserbringung

Varianten in Deutschland

- EnWG: ISO 27001/19 + weitere Anforderungen Sicherheitskatalog
- BSIG: ISO 27001 + weitere Anforderungen BSIG-Orientierungshilfe
- BSIG: B3S (Final, Entwurf oder B3S-Orientierugnshilfe)

Aktuelle Situation in Österreich

- QuaSteV im Juli 2019 mit Anforderungen zu Prüfstellen, Prüfern, Prüfprozess und Antragsverfahren in Kraft getreten.
- Prüfung auf Basis NISV-Maßnahmenkategorien
- ISO 27001 Zertifikat als (Teil-)Ersatz für NISG-Prüfung (Voraussetzung QuaSte)
  - Ausmaß notwendiger Zusatzprüfungen unklar

Fazit

- Geltungsbereich muss ordentlich abgegrenzt und strukturiert (Asset-Modell) sein.
- Sprache des Geltungsbereich muss sich durch weitere Prozesse (Risikomanagement und IT/OT-Betrieb) ziehen.
- In DE greifen Anforderungen tief in Prozesse des ISMS wie Risikomanagement ein, in AT sind derartige Anforderungen noch nicht bekannt.
- Unklarheit besteht im Ausmaß notwendiger Zusatzprüfung, bei Anrechnung eines ISO 27001 Zertifikats
- Key Player beim ISMS frühzeitig abholen und mit der Thematik vertraut machen
- Quantitative Risikoanalysen erleichtern die Entscheidungen für das Management