AUDITTRAILS

NIS-2 & ISO 27001 – mit automatisiertem ISMS zum (Sales) Asset für Ihr Unternehmen

Dr. Nicholas Derra

it-sa Expo & Congress

AUDITTRAILS Networks GmbH
Wunsiedler Straße 7
95032 Hof/Saale
www.audittrails.com

Wofür braucht man ein (zertifiziertes) ISMS?

- Resilienz bei Cyber-Angriffen / Notfallmanagement
- Schutz von Informationen als Unternehmens-Assets
- Zentrales Vertriebsargument zur Erfüllung von Kundenanforderungen (Lieferfähigkeit / Cyber-Sicherheit)
- Gesetzliche Anforderungen, u. a. NIS-2
- Management-Haftung
- Lieferkette: Kunden mit ISMS-Standards (ISO 27001 / TISAX® / NIS-2) "reichen Anforderungen durch"
- Abschluss von Cyberversicherungen
- Bank- / Finanzpartner (ISMS als Voraussetzung für Kreditvergabe)
- Außendarstellung (als vertrauensvoller Partner & attraktiver Arbeitgeber)

AUDITTRAILS

Die NIS-2 Richtlinie

- Kriterien: Sektor & Größe („Size-Cap-Rule“)
- Besonders wichtige Einrichtungen mit >249 MA oder >50 Mio. € Jahresumsatz / >43 Mio. € Bilanzsumme
- Wichtige Einrichtungen mit >49 MA oder >10 Mio. € Jahresumsatz / Bilanzsumme
- Strengere Grenzen für öffentliche Telekommunikation / DNS / TLD-Namensregister
- Relevanz der Lieferketten – Weitergabe von (EU-) Anforderungen durch (internationale) Kunden bedeutet eine deutlich höhere Anzahl mittelbar betroffener Unternehmen (~150.000)
- Unpräzise Anforderungen ohne klare Handlungsempfehlungen

Besonders wichtige Einrichtungen (>8.000 in D) aus den Sektoren:	**Wichtige Einrichtungen (>20.000 in D) aus besonders wichtigen Sektoren + zusätzlich:**
Energie / Gesundheit	Post / Kurier
Banken / Finanzmärkte	Abfallwirtschaft
Wasser / Abwasser	Chemie / Ernährung
IKT-Services / Digitale Infrastruktur	Industrie (Machinenbau, Medizintechnik etc.)
Transport und Verkehr	Digitale Dienste (Plattformen, Suchmaschinen etc.)
Raumfahrt	Forschung

Die ISO 27001

Goldstandard der Informationssicherheit

- Klare Anforderungen an Dokumentation und technische Umsetzung von Cyber-Security
- Seit 20 Jahren mit weltweiter Akzeptanz (>70.000 gültige Zertifikate im Jahr 2022 bei massiv steigender Tendenz) erfolgreich im Einsatz
- State of the Art dank Normrevision ISO 27001:2022 (BCM / Cyber-Security / Verfügbarkeit)
- ~85% der notwendigen NIS-2 Maßnahmen mit klarem Bezug zu Controls der ISO 27001

Wesentlicher Baustein für weitere Richtlinien

- TISAX® Kapitel referenzieren im Bereich Informationssicherheit auf ISO 27001 (~60%)
- Unterkapitel Informationssicherheit anderer Normen auf Basis der ISO 27001 (ISO 17025 / ISO 15189 etc.)

Hochrelevant im DACH-Raum

- Viele IKT Service Provider (Data Center, Cloud, große Systemhäuser) sind ISO 27001-zertifiziert
  → Vorsicht bei der Tool-Auswahl: Software-Anbieter noch nicht flächendeckend!
- Forderungen nach ISO 27001-Zertifizierungen werden entlang der Lieferketten weitergegeben

AUDITTRAILS

Die ISO 27001 als optimale ISMS-Grundlage

- Auch ohne Zertifizierung oder Vorkenntnisse ideal für ISMS-Aufbau geeignet (NIS-2 / Sales Asset)
- Klare Dokumentationsanforderungen
- State-of-the-Art Prozessstandards zu Cyber-Security
- Technische / prozessuale / mitarbeiterbezogene Maßnahmen
- Organisatorische Maßnahmen / Awareness- / Schulungsmaßnahmen
- Informationssicherheit in Betrieb und Projekten / Schutz der Unternehmens-IP
- Notfallplanung / Business Continuity Management
- Reduzierung der Zeiten für Wiederanlauf nach Störungen / Angriffen
- Optimierung der Norm via Revision auf ISO 27001:2022

AUDITTRAILS

Effizient zum ISMS – interne Ausgangssituation

Priorisierung

- Limitierte Budgets
- Fokus auf Kerngeschäft
- ISMS-Dokumentation rudimentär bzw. nicht vorhanden

Personelle Ressourcen

- Personalkapazität stark limitiert
- Erfahrung & Kompetenz ausreichend vorhanden?
- Preisniveau externer Ressourcen; Beratung via „Pay-per-Hour"

Interessierte Parteien

- Kunden erwarten sichere Lieferfähigkeit
- Banken & Versicherungen bewerten Cyber-Security
- Geschäftsleitung fehlt Bewusstsein für Notwendigkeit / Haftung
- Gesetzliche Anforderungen / Justification

Interner & externer Druck bei gleichzeitiger Notwendigkeit maximaler Effizienz

AUDITTRAILS

ISMS-as-a-Service – Anforderungsprofil

Ebene 1 – Geschäftsführung / CISO / ISB / DSB

- Management Rahmenwerk / Richtlinien im Kontext ISO 27001 / NIS-2 / TISAX®
- Dokumentation der Risikobetrachtung / Maßnahmen

Ebene 2 – ISMS-Team

- Prozesse / Richtlinien / Periodische Prüfungen (Nichtkonformitäts-/Dokument-/Kompetenzmanagement uvm.)
- Sicherheitskonzepte / BCM / Notfallhandbücher

Ebene 3 – IT-Teams / Fachabteilungen / Geschäftsbereiche

- Unternehmensspezifische Verfahrens- & Arbeitsanweisungen / Checklisten / Formulare / Standards

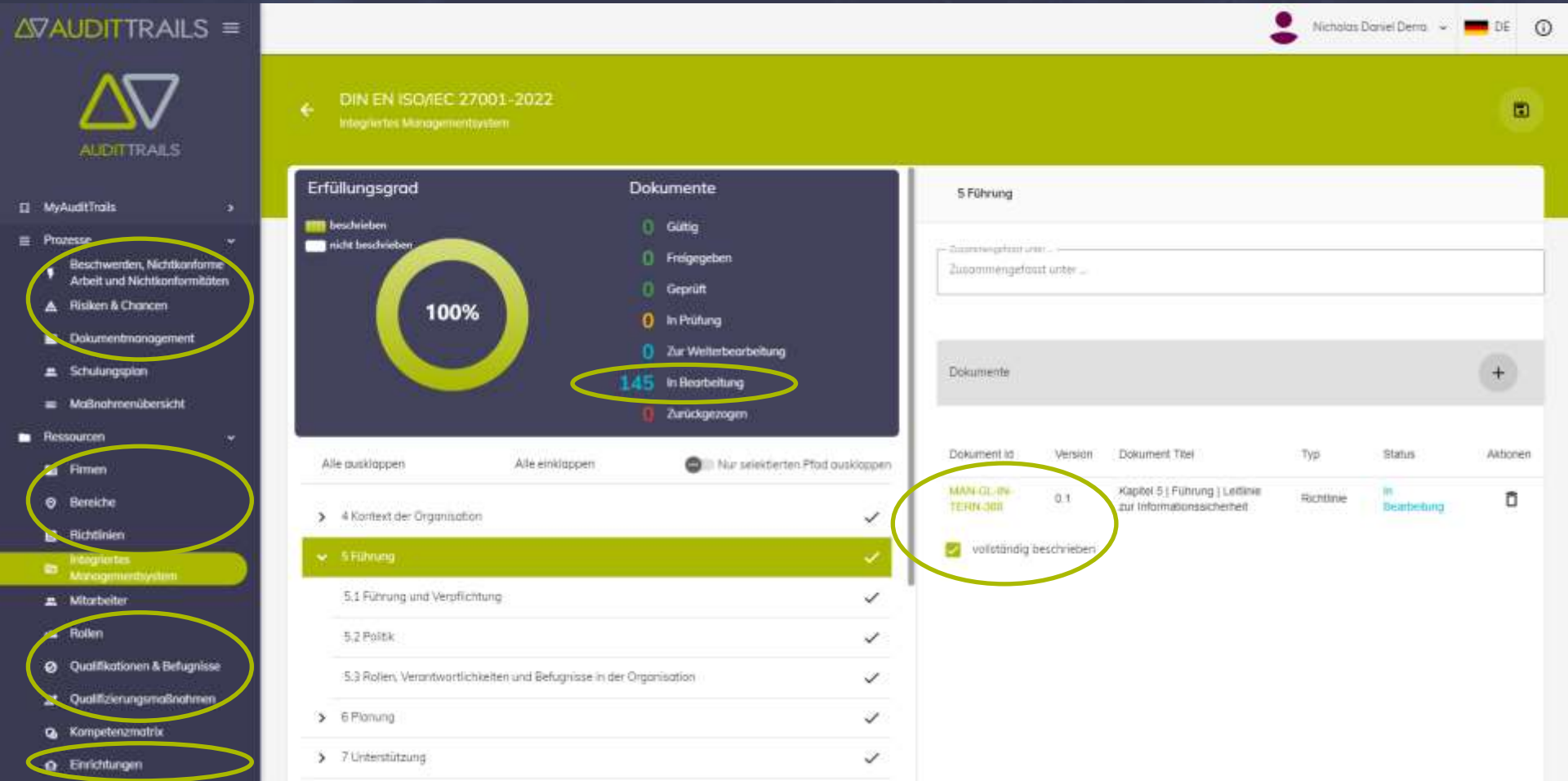
Ebene 4 – IT-Teams / Fachabteilungen / Geschäftsbereiche / Haustechnik / Sicherheitsdienst / …

- Aufzeichnungen / Nachweise / Logfiles / KPIs / Interne Audits / Lieferantenbeurteilungen …
- **Muster & Vorlagen für alle notwendigen Nachweisdokumente (!)**

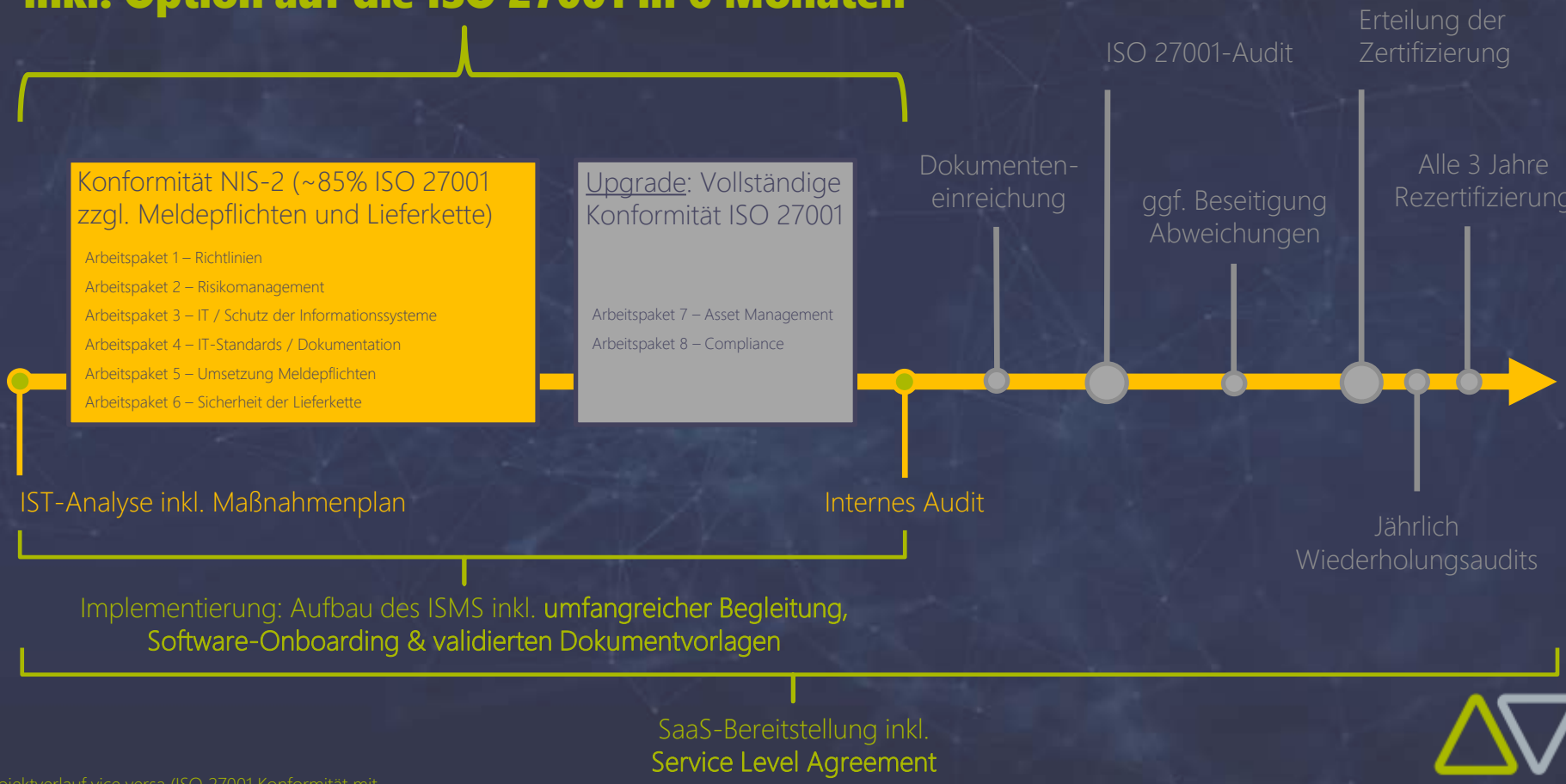
Farbige Markierung = von leistungsfähigen ISMS bereitgestellte Services

AUDITTRAILS

ISMS-as-a-Service mit AUDITTRAILS



Ein Beispiel: Zum effizienten ISMS nach NIS-2 inkl. Option auf die ISO 27001 in 6 Monaten*



*Projektverlauf vice versa (ISO 27001 Konformität mit optionalem NIS-2 Upgrade) ebenfalls umsetzbar

AUDITTRAILS

ISMS-as-a-Service mit AUDITTRAILS

- ✓ **Bis zu 67% schneller** – ISMS-Aufbau nach Norm mit >140 Dokumentvorlagen & automatisierten Workflows
- ✓ **Fokus auf wertschöpfende Tätigkeiten** bei minimalen Personalkosten für ISMS-Aufbau und Betrieb
- ✓ **Ressourceneffizienz** und **transparentes Investitionsbudget** bei **~50% Kostenoptimierung** durch vorgefertigtes ISMS-Framework
- ✓ **Minimaler Aufwand** für Software-Wartung und laufende Updates dank webbasierter Software-Architektur
- ✓ **Permanente Weiterentwicklung** der Vorlagen und Synchronisierung mit aktuellen Normversionen
- ✓ **Eine Datenbasis** (Single Source of Truth) für alle Prozesse – dank eigener ISO27001-Zertifizierung unter höchsten Standards der Informationssicherheit
- ✓ **Verfügbarkeit** der gesamten Dokumentation im Notfall
- ✓ **Sofort startklar – effiziente Nutzung des Systems ab dem ersten Projekttag**

AUDITTRAILS

Ihr ISMS als (Sales) Asset – Fazit

Wieso benötigen Unternehmen ein effizientes ISMS (mit / ohne Zertifikat)?

- Schutz vor Cyber-Angriffen & Notfallmanagement → **Resilienz!**
- Gesetzliche Anforderungen (NIS-2) → **Haftung!**
- Anforderung von neuen bzw. bestehenden Kunden → **Vertrieb!**
- Anforderung von Banken & Cyber-Versicherungen → **Partner!**

} oft Forderung nach ISO 27001 / TISAX®

Wie baut man ein ISMS mit minimalem Ressourceneinsatz?

- Richtlinienspezifisches ISMS-Framework mit automatisierten Workflows
- Hochwertige Dokumentvorlagen & stete Einbeziehung von Normrevisionen
- Vollständig Cloud-basiert (Verfügbarkeit & Updates!) mit höchstem Informationssicherheits-Standard

Wann startet man mit dem ISMS-Aufbau?

- ISMS mit konkretem Mehrwert für Unternehmen (Vertrieb / Verfügbarkeit & Lieferfähigkeit in Notfällen)
- Heute – starke Kundenpotenziale & Anforderungsdruck bzw. Haftungsrisiken von allen Seiten

AUDITTRAILS

AUDITTRAILS. Einfach sicher. Sicher einfach.

Dr. Nicholas Derra

VP ISMS / Sales Coordinator
AUDITTRAILS Networks GmbH

nd@audittrails.com

+49 (0) 162 9258732

Jetzt informieren & kostenloses Erstgespräch vereinbaren:

www.audittrails.com

AUDITTRAILS