

THORSTEN SCHMIDT

IT-Security-, Governance-, Risk- & Compliance-Berater

Münster · t@tsmondo.de · +49 162 9691436 · www.tsmondo.de · Deutsch (Muttersprache), Englisch (fließend)

PROFIL

Senior IT-Security- und Compliance-Berater mit über 25 Jahren IT-Erfahrung, davon 20+ Jahre Projekt- und Führungsverantwortung und 8+ Jahre Schwerpunkt Cybersecurity Governance, Risk & Compliance. Zertifizierter ISO 27001 Lead Auditor und Lead Implementer, ISACA CISM. Mehrere NIS2-Implementierungen in produzierender Industrie, Medien und kritischer Telekommunikationsinfrastruktur: Betroffenheits- und Gap-Analyse gegen die Sicherheitsanforderungen der Richtlinie, Control-Framework-Implementierung, BSI-Registrierung, Evidence- und Audit-Readiness sowie Management-Schulungen zur Organhaftung. Langjährige Erfahrung in der Steuerung von Compliance-Programmen als Embedded Consultant gemeinsam mit interner IT, CISO-Funktion und externen Dienstleistern — technische Tiefe (M365-Security, Schwachstellenmanagement, Detection & Response) kombiniert mit Stakeholder-Management bis auf Geschäftsführungsebene. Früher Praxiseinsatz von KI-Governance mit einer ISO/IEC-42001-Implementierung. Tägliche Arbeit mit Jira- und Confluence-basiertem GRC-Tooling.

KERNKOMPETENZEN

- **NIS2 / ENISA & regulatorische Compliance:** Betroffenheitsanalyse, Gap-Analyse, Maßnahmenumsetzung, BSI-Registrierung & Meldepflichten, Management-Schulung (Organhaftung)
- **ISMS & Frameworks:** ISO 27001:2022 / :2013 (inkl. Migration), Annex A, Statement of Applicability, BSI IT-Grundschutz, BSI 200-4 (BCM), ISO 22301, ISO/IEC 42001 (KI-Governance)
- **Compliance-Programm-Management:** Control Ownership & Inventory, Evidence Collection und Qualitätsprüfung, Remediation-Tracking, KPI-Definition, internes Audit, Managementbewertung, Steering-Committee-Reporting
- **GRC-Tooling:** Jira- & Confluence-basiertes ISMS (Change-/Incident-Management, Workflows, Dashboards), Tenable Schwachstellenmanagement, Snyc DevSecOps; schnelle Einarbeitung in GRC-Plattformen (OneTrust: konzeptionelle Kenntnis)
- **Technische Security:** Microsoft 365 / Azure / Entra ID Security & Secure Score, Defender & Intune, Penetrationstests & Schwachstellenscans, KI-basierte NDR/XDR (Darktrace), Firewalls & Netzwerksicherheit
- **Führung & Stakeholder:** Ehemaliger IT-Leiter (45 MA) und Leiter IT-Operations & Security; Vendor-Auswahl und Vertragsverhandlung; Workshop-Moderation und Schulungen

ZERTIFIZIERUNGEN

- ISO 27001 Lead Auditor (2022)
- ISO 27001 Lead Implementer (2022)
- ISACA CISM — Certified Information Security Manager (2017)
- TÜV-zertifizierter Datenschutzbeauftragter / DSGVO-Experte (2018)
- TÜV-zertifizierter IT-Sicherheitsbeauftragter (2017)
- ITIL v3 Foundation; Microsoft MCSE; VMware VCP; Projektmanagement (Bertelsmann Management Development Program)

AUSGEWÄHLTE PROJEKT- & BERATUNGSERFAHRUNG

2026 – heute

NIS2 Compliance Lead — Gap-Analyse, Maßnahmenumsetzung & BSI-Registrierung

Hammelmann GmbH (internationaler Maschinenbauer, Interpump Group)

- NIS2-Betroffenheitsanalyse und Gap-Analyse gegen die Pflichtmaßnahmen der Richtlinie
- Umsetzungs-Roadmap, Zuordnung von Control Ownership über IT- und Fachbereiche
- Vorbereitung und Begleitung der BSI-Registrierung inkl. Melde- und

Nachweispflichten

- Management-Schulung der Geschäftsleitung zu NIS2-Pflichten und persönlicher Haftung
- Programm-Governance: Meilenstein-Tracking, Statusberichte, Stakeholder-Koordination in regelmäßigen Steering-Terminen

2025 – heute

Business Continuity Management Lead (ISO 22301 / BSI 200-4)

Hammelmann GmbH

- Business Impact Analyse (BIA) für kritische Geschäftsprozesse und IT-Services
- Definition von MBCO, RTO/RPO, MTPD; Kontinuitätsstrategien und Notfallplanung
- BCM-Dokumentation, Vorlagen und IT-Notfallhandbuch; Workshops mit IT und Fachbereichen

2024 – 2026

Leiter IT-Operations & Security

Deutsche Funkturm GmbH (DFMG) — kritische Telekommunikationsinfrastruktur, Deutsche-Telekom-Konzern

- Aufbau und Gestaltung der IT-Operations- und Security-Organisation; Teamführung und -entwicklung
- Sicherheitsrichtlinien und -verfahren gemäß VS-NfD (Geheimschutz), BSI IT-Grundschutz und ISO 27001
- Schwachstellenscans und Penetrationstests; priorisierte Maßnahmensteuerung
- Kontinuierliche Verbesserung des M365 Secure Scores und der Security-KPIs; Einführung von SOC-Services
- Implementierung eines KI-Managementsystems nach ISO/IEC 42001: KI-Governance-Framework, KI-Risikobewertung und Richtlinien für den sicheren Einsatz von KI-Systemen
- Steuerung externer Dienstleister (RZ, Security); Einführung von ITIL-Prozessen

2024 – 2025

Berater Security Management (M365, DevSecOps, Schwachstellenmanagement)

Landwirtschaftsverlag-Konzern (eines der größten Medienunternehmen Deutschlands)

- Security-KPI-Reporting und Verbesserung des M365 Secure Scores im Konzern
- Schwachstellenscans mit Tenable; priorisierte Behebung mit Administratoren und Dienstleistern
- Einführung von DevSecOps (Snyk) in den Entwicklungseinheiten

2023 – 2024

NIS2 Implementation Lead

Landwirtschaftsverlag GmbH & LV Digital GmbH (Tochtergesellschaft)

- NIS2-Betroffenheitsanalyse für Konzern und Digital-Tochter; Gap-Analyse gegen die Sicherheitsanforderungen der Richtlinie
- Umsetzung der NIS2-Maßnahmen integriert in das ISO-27001:2022-Control-Set und das BCM-Programm (ein Control-Framework, keine Doppelstrukturen)
- Governance- und Meldestrukturen, Incident-Reporting-Readiness und Management-Briefing zur Organhaftung

2023 – 2024

ISO 27001:2022 Migration & ISMS Lead

Landwirtschaftsverlag GmbH

- Migration des ISMS von ISO 27001:2013 auf :2022; Umsetzung der Anforderungen und Maßnahmen des Annex A
- Risikobewertung und Referenzierung der Risiken auf Maßnahmen (Statement of Applicability)

- Richtlinien, Verfahren und Prozesse; Einbindung von Assets und Lieferanten; DSGVO-Verarbeitungsverzeichnis
- Change- und Incident-Management mit Jira umgesetzt; KPI-Definition und -Überwachung
- Schulungsunterlagen; internes Audit und Managementbewertung

2023 – 2024

Projektleiter Business Continuity Management (BSI 200-4)

Landwirtschaftsverlag GmbH

- Einführung eines BCMS zum Schutz produktionskritischer Prozesse vor Ransomware-Szenarien
- Notfallorganisation, BIA, Notfall-Betriebsszenarien, Notfallübungen und Notfallhandbuch (Confluence)

2022 – 2023

Projektleiter — KI-basierte Angriffserkennung & Autonomous Response (Darktrace)

Landwirtschaftsverlag GmbH

- Budgeteffiziente Alternative zum 24/7-SOC: Systemauswahl, Proof of Concept, Vertragsverhandlung
- Implementierungsleitung; Anbindung an Kernnetzwerk, Server, Firewalls, Salesforce, M365 und Tenable
- Kontinuierliches Monitoring, Modell-Tuning und Verbesserung der Reaktionsfähigkeit

2022 – 2023

Projektleiter — Microsoft 365 Security Stack (E5), Intune, Defender

Landwirtschaftsverlag GmbH

- Konzernweiter Rollout der M365-E5-Security-Suite; Umsetzung hunderter Sicherheitsempfehlungen
- Intune Device Management, ASR- und Netzwerkregeln, DLP/App Protection; Migration SCCM auf Intune
- Management-Risikoberichte und Risikobehandlungsplan

2021 – 2022

ISO 27001 Einführung & Zertifizierung + DSGVO-Management

Henworx GmbH & Co. KG (digitale Gesundheitsanwendung / DiGA-Start-up)

- ISO-27001-Umsetzung bis zur Zertifizierung; externer Datenschutzbeauftragter
- M365-Sicherheitskonzept, Penetrationstests, Jira/Confluence-basierte Dokumentation

2019 – 2023

Leiter IT (45 Mitarbeiter)

Landwirtschaftsverlag GmbH

- IT-Strategie (ERP, CRM, Online), IT Service Management, Projektcontrolling, Rechenzentrumsbetrieb
- Leitung der Stabsstelle IT-Sicherheit; erste ISMS-Einführung (ISO 27001, 2017–2018)

2000 – 2018

IT-Führungspositionen

Arvato / Bertelsmann (2000–2010), Landwirtschaftsverlag (2010–2018)

- Leiter IT-Operations für mehrere nationale und internationale Standorte (u. a. Liverpool, Malmö)
- Leiter IT-Systeme, Security & Servicedesk; stellv. IT-Leiter; IT-Security-Verantwortlicher

AUSBILDUNG

Fachinformatiker, Computer & Software GmbH, Münster — 1999

EINSATZDETAILS

- Verfügbarkeit: ab sofort, 3–4 Tage pro Woche (50–80%)
- Arbeitsmodell: Remote-first; regelmäßige Vor-Ort-Präsenz und internationale Reisen möglich
- Arbeitserlaubnis: Europäische Union und Schweiz
- Sprachen: Deutsch (Muttersprache), Englisch (fließend), Französisch (Grundkenntnisse)