Bonuskapitel 2

Sicherheitskultur und Security-Champions-Programme

Als Chief Information Security Officer bin ich fest davon überzeugt: Technologie skaliert nur durch Menschen. Technische Maßnahmen – so robust, automatisiert oder KI-gestützt sie auch sein mögen – entfalten ihre Wirkung nur dann vollumfänglich, wenn sie durch das Verhalten, das Verständnis und die Akzeptanz der Mitarbeitenden getragen werden. Sicherheitskultur ist daher kein »weiches Thema» am Rande des Sicherheitsprogramms, sondern ein zentrales Führungsinstrument zur Reduktion von Cyberrisiken.

Wir betrachten Sicherheitskultur nicht als etwas, das »organisch» entsteht, sondern als strategische Disziplin, die wie jede andere unternehmerische Funktion geführt, gemessen und weiterentwickelt werden muss. Sie ist messbar durch gezielte Metriken (z. B. Sicherheitsverhalten, Incident-Response-Reife, Awareness-Rückläufe), steuerbar durch gezielte Initiativen und Kommunikation, und unmittelbar verknüpft mit unserem Risikoprofil, Reputationsschutz und regulatorischer Belastbarkeit.

In diesem Kapitel beleuchten wir die konkrete Vorgehensweise, mit der wir als Security Leadership Team:

- eine nachhaltige Sicherheitskultur aufbauen,
- sie systematisch im Alltag verankern,
- und sie über gezielte Security Champions Programme skalieren, um genau dort operative Wirkung zu entfalten, wo zentrale Sicherheitsteams keinen unmittelbaren Einfluss mehr haben — in Produktteams, Fachabteilungen, DevOps-Umgebungen oder im Geschäftsbetrieb.

Security Champions sind für uns keine »Nebenrolle», sondern strategisch eingesetzte Multiplikatoren. Sie agieren als kulturelle Brückenbauer, technische Übersetzer und lokale Change Agents, die Sicherheitsanforderungen in ihren Teams verankern, Sicherheitsbewusstsein fördern und als Frühwarnsysteme für organisationale Schwachstellen fungieren.

Kurz gesagt: Wenn Sicherheitskultur das Betriebssystem einer resilienten Organisation ist, dann sind Security Champions die verteilten Sensoren und Aktoren, die dieses System lebendig halten und weiterentwickeln.

Warum Sicherheitskultur strategisch ist

In der Rolle des CISO tragen wir eine doppelte Verantwortung: Wir sind Architekten von Steuerungsmechanismen und zugleich Führungskräfte für Verhaltensveränderung. Diese beiden Perspektiven — Steuerung und Führung — müssen sich in einem modernen Sicherheitsprogramm ergänzen und verstärken.

- Risikominimierung durch Steuerung:

  Hierzu zählen die klassischen Disziplinen der Informationssicherheit — die Entwicklung und Durchsetzung von Policies, die Implementierung technischer und organisatorischer Controls, sowie der Aufbau von Detektions- und Response-Fähigkeiten. Diese Steuerung erfolgt durch klare Vorgaben, Standards, Auditierbarkeit und Eskalationsmechanismen.

- Verhaltensänderung durch Führung:

  Technische Steuerung reicht jedoch nur so weit, wie sie im Alltag akzeptiert und gelebt wird. Deshalb liegt unsere zweite, oft vernachlässigte Verantwortung in der Führung von Menschen: dem Aufbau von Vertrauen, dem Fördern von Ownership, dem Schaffen psychologischer Sicherheit für das Melden von Incidents und dem gezielten Einsatz von Kommunikation als kulturellem Hebel.

Sicherheitskultur ist der strategische Multiplikator beider Aufgaben. Sie entscheidet, ob unsere Policies tatsächlich in gelebtes Verhalten übersetzt werden — nicht nur auf dem Papier, sondern in den alltäglichen Mikroentscheidungen jedes Einzelnen.

- Wenn ein Software-Engineer entscheidet, Secrets aus dem Git-Repository herauszuhalten, ist das keine rein technische Maßnahme — es ist Ausdruck eines kulturell verankerten Sicherheitsbewusstseins.
- Wenn eine HR-Mitarbeiterin eine verdächtige E-Mail nicht nur erkennt, sondern aktiv meldet, ist das ein Zeichen für gelebte Verantwortung und Vertrauen in die Prozesse.
- Wenn ein Team Sicherheitsbedenken frühzeitig kommuniziert, statt sie zu verschweigen, ist das ein Symptom für eine gesunde Sicherheitskultur — nicht für Policy-Compliance.

Ohne eine belastbare Kultur bleiben Policies Papiertiger. Sie mögen regulatorisch korrekt sein, helfen aber im Ernstfall nicht weiter, wenn sie nicht verstanden, akzeptiert und proaktiv gelebt werden. Sicherheitskultur ist damit kein »weiches» Add-on, sondern das soziotechnische Fundament, auf dem jede wirksame Cybersecurity-Strategie aufbaut.

Governance-Modell für Sicherheitskultur

Eine wirksame Sicherheitskultur entsteht nicht durch punktuelle Awareness-Maßnahmen oder gelegentliche Kommunikation, sondern durch strukturelle Verankerung innerhalb des Sicherheitsprogramms. Um Sicherheitsverhalten systematisch zu fördern und langfristig im Unternehmen zu etablieren, braucht es klare Zuständigkeiten, Steuerungsmechanismen und Reportingstrukturen — analog zu jedem anderen strategischen Steuerungsfeld im Unternehmen.

Wir empfehlen ein Governance-Modell, das auf vier zentralen Elementen basiert in Tabelle 1 dargestellt ist:

Governance-Element	Umsetzung in der Organisation
Ownership auf Führungsebene	Sicherheitskultur ist explizit als Bestandteil der übergreifenden Security-Strategie definiert. Die Verantwortung liegt beim CISO, der konkrete Kulturziele in seinen persönlichen OKRs führt. Das schafft Top-Down-Verbindlichkeit und signalisiert: Kultur ist Chefsache.
Dedizierte Verantwortlichkeit	Die operative Verantwortung liegt bei einer klar benannten Rolle – z. B. einem »Security Culture Lead» oder »Security Enablement Manager», verankert im GRC-, Awareness- oder Security Strategy-Team. Diese Funktion ist zuständig für Programmkonzeption, cross-funktionale Koordination, Stakeholdermanagement und Erfolgsmessung.
Steuerung über OKRs	Kulturelle Sicherheitsziele werden auf Quartalsebene operationalisiert, z. B. durch den Aufbau eines Security Champions Netzwerks in bestimmten Geschäftsbereichen, das Erreichen definierter Phishing-Erkennungsquoten, oder die Durchführung teambasierter Sicherheits-Retrospektiven. So wird Sicherheitskultur in konkrete, teamnahe Maßnahmen überführt.
Regelmäßiges Reporting	Die Ergebnisse kultureller Initiativen werden in einem strukturierten Reporting-Prozess erfasst und im Rahmen der regulären Risiko- und Performance-Reports an C-Level, Vorstand und/oder Audit Committee kommuniziert. Berichtet werden sowohl quantitative KPIs (z. B. Teilnahmequoten, Trainingsabschlüsse, Detektionsraten) als auch qualitative Indikatoren (z. B. Kulturbarometer, Lessons Learned aus Incidents).

Tab. 2.1: Governance-Bausteine zur Verankerung der Sicherheitskultur

Durch diese Governance-Struktur wird sichergestellt, dass Sicherheitskultur nicht als begleitende Maßnahme, sondern als strategisch steuerbares Programmfeld etabliert ist — mit klarer Verantwortlichkeit, regelmäßiger Fortschrittsmessung und hoher Managementvisibilität.

Diese Herangehensweise stärkt nicht nur die kulturelle Resilienz der Organisation, sondern verbessert auch die Operationalisierbarkeit von Sicherheitsanforderungen und die Erfüllung regulatorischer Erwartungen, z. B. im Rahmen von ISO 27001, DORA, TISAX oder NIS2.

Reifegradmodell und Steuerungskennzahlen für Sicherheitskultur

Um die Entwicklung und Effektivität einer Sicherheitskultur systematisch zu begleiten, bedarf es eines strukturierten Reifegradmodells sowie eines darauf abgestimmten Sets an Key Performance Indicators (KPIs). Diese ermöglichen es, kulturelle Fortschritte sichtbar zu machen, Trends frühzeitig zu erkennen und gezielte Steuerungsmaßnahmen zu ergreifen — sei es in der Kommunikation, im Training oder im Ressourceneinsatz.

Das in Tabelle 2 dargestellte Modell beschreibt fünf Entwicklungsstufen organisatorischer Sicherheitskultur. Es dient der Standortbestimmung und strategischen Zielsetzung:

Reifegrad	Beschreibung
1. Ignoriert	Sicherheitskultur wird nicht adressiert. Es existieren keine Awareness-Maßnahmen oder kulturellen Zielsetzungen. Verhalten ist unstrukturiert und reaktiv.
2. Reaktiv	Sicherheitsinitiativen erfolgen primär nach Vorfällen (»incident-driven«). Kommunikation ist unregelmäßig, Awareness punktuell. Vertrauen ist begrenzt.
3. Strukturiert	Es bestehen etablierte Awareness-Programme, erste Security Champions sind benannt. Sicherheitskultur ist als Thema präsent, aber nicht tief verankert.
4. Integriert	Kulturziele sind in Performance- und Führungsprozesse eingebettet (z. B. OKRs, Team-Ziele). Sicherheitsverhalten wird teamübergreifend gefördert und bewertet.
5. Selbstregulierend	Sicherheit ist Teil der Team-Identität. Mitarbeitende agieren proaktiv, sprechen Probleme offen an, und korrigieren sich gegenseitig im Sinne sicherheitsbewussten Handelns. Führung agiert als Enabler.

Tab. 2.2: Reifegradmodell Sicherheitskultur

Ziel sollte es sein, über einen Zeitraum von 12 bis 24 Monaten von einem strukturierten in einen integrierten oder gar selbstregulierenden Zustand zu kommen — angepasst an Unternehmensgröße, Reife und Risikolage.

Das in Tabelle 3 ausgelistete Set an Kennzahlen dient als Früh- und Spätindikator für den Zustand der Sicherheitskultur. Die Auswahl basiert auf ihrer Aussagekraft, Messbarkeit und Anschlussfähigkeit an bestehende Reportingprozesse (z. B. Risk Dashboards, Auditberichte):

KPI	Zielwert	Bedeutung und Steuerungslogik
Phishing-Erkennungsquote	> 80 %	Frühindikator für Awareness, Handlungskompetenz und aktives Sicherheitsverhalten. Korreliert mit Risikoreduktion im Alltag.
Incident-Meldungen durch Mitarbeitende	> 30/Monat	Signal für gelebte Vertrauenskultur und Aufmerksamkeit. Zeigt, ob Mitarbeitende aktiv Risiken erkennen und melden.
Abschlussquote von Awareness-Trainings	> 90 %	Basisanforderung für regulatorische Compliance (z. B. ISO 27001, DORA). Auch Frühwarnsignal für Führungslücken.
Champion-Netzwerkverbreitung	1 Champion je 10 FTE	Metrik zur dezentralen Verankerung der Sicherheitsverantwortung. Zeigt die operative Skalierbarkeit der Kulturinitiativen.

Tab. 2.3: 3 KPI-Set zur Steuerung der Sicherheitskultur

Optional können weitere KPIs integriert werden, z. B.:

- Sicherheits-KPIs in Performance-Reviews
- Rückläufe bei Security-Retrospektiven
- Response-Zeiten auf Sicherheitskommunikation
- Fehlerrate bei sicherheitsrelevanten Prozessen

Durch die Kombination aus qualitativen Reifegraden und quantitativen Steuerungskennzahlen schaffen wir ein belastbares Steuerungsmodell, das sowohl kulturelle Fortschritte als auch operative Wirksamkeit sichtbar macht — transparent, adaptiv und managementfähig.

Ein Reifegradmodell und ein aussagekräftiger KPI-Satz machen kulturelle Entwicklung sichtbar und steuerbar – sofern sie korrekt implementiert und genutzt werden. Folgende Empfehlungen helfen, die Kennzahlen wirksam einzusetzen:

Tipp 1 - Reifegrad regelmäßig peer-basiert validieren

Lass den Reifegrad nicht nur vom Security-Team bestimmen. Nutze Selbst- und Fremdeinschätzung (z. B. durch Champions oder Teamleads) als 360°-Validierung des kulturellen Fortschritts.

Tipp 2 - KPIs ins Security Dashboard integrieren

Kulturkennzahlen sollten Teil des regulären KPI-Dashboards sein – nicht als Sonderfall. Integriere sie z. B. neben Vulnerability Metrics, SOC-KPIs oder Audit-Findings.

Tipp 3 - Visualisierung für das Management anpassen

Nutze einfache Heatmaps oder Kultur-Scorecards für das C-Level. Vermeide technisches Overload – der Fokus liegt auf Risiko-, Reputations- und Reifeaussagen.

Security Champions Programme als Kulturmultiplikator

Security Champions Programme sind ein zentrales Instrument zur skalierbaren Verankerung sicherheitsbewussten Verhaltens in einer komplexen, dezentralen Organisation. Sie fungieren als operativer Verstärker der Sicherheitskultur, indem sie nicht nur Awareness fördern, sondern konkrete sicherheitsrelevante Verhaltensweisen in den Teams vorleben, verstärken und rückmelden.

Sie überbrücken die strukturelle Distanz zwischen dem zentralen Security-Team und den operativen Einheiten – insbesondere in agilen Produktteams, DevOps-Umgebungen oder lokalen Geschäftsbereichen – und schaffen eine bi-direktionale Rückkopplungsschleife: von der strategischen Sicherheitsebene hin zum operativen Alltag – und zurück.

Ein professionell aufgesetztes Security Champions Programm verfolgt mehrere strategisch und operativ relevante Ziele:

- Förderung sicherheitsbewussten Verhaltens im Tagesgeschäft

  Champions sensibilisieren ihre Teams für sicherheitsrelevante Aspekte im operativen Kontext (z. B. sichere Softwareentwicklung, Datenschutz bei Kundenprozessen, Umgang mit Shadow IT).

- Erhöhung der Sichtbarkeit und Präsenz von Sicherheit in operativen Teams

  Sicherheit wird als aktiver Teil der Teamkultur wahrgenommen, nicht als externe Kontrollinstanz.

- Beschleunigung der Incident-Erkennung und -Eskalation

  Durch lokale Ansprechpartner mit Grundverständnis für Security-Signale werden Bedrohungen früher erkannt und korrekt adressiert.

- Identifikation kultureller und technischer Schwachstellen in der Linie

  Champions fungieren als Sensoren für kulturelle »Blind Spots», fehlende Awareness oder technische Sicherheitslücken im operativen Betrieb.

Um Wirkung zu entfalten, benötigt ein Champions Programm eine strukturierte Ausgestaltung entlang zentraler Designprinzipien, wie in Tabelle 4 aufgeführt:

Aspekt	Ausgestaltung in der Praxis
Rollenprofil	Champions müssen keine Sicherheitsexperten sein, sollten jedoch Grundverständnis für Security-Themen, Kommunikationstalent und Teamakzeptanz mitbringen.
Teilnahme	Die Teilnahme erfolgt freiwillig, jedoch mit explizitem Buy-In des jeweiligen Team- oder Bereichsleiters, um Verbindlichkeit und Rückhalt sicherzustellen.
Zeitbudget	Champions benötigen ein dediziertes Zeitbudget von ca. 5–10 % ihrer regulären Arbeitszeit, das formell mit dem Vorgesetzten abgestimmt ist. Ohne dies bleibt das Programm symbolisch.
Enablement	Erfolgreiche Champions erhalten kontinuierliche Befähigung durch Bootcamps, Deep-Dive-Trainings, Zugriff auf Playbooks, Use Cases, Threat Intelligence und Shadowing.
Incentivierung	Anerkennung ist ein zentraler Erfolgsfaktor: Zertifikate, interne Sichtbarkeit, Feedback vom CISO, Spotlight im Intranet oder Bonuspunkte im Performance-Review.
Kommunikationskanäle	Das Programm lebt von Interaktion. Ein dedizierter Slack-Channel, ein interaktives Wiki sowie ein regelmäßiger Champions-Newsletter sind essentielle Bestandteile.

Tab. 2.4: Tabelle 4 Strukturmerkmale eines professionellen Champion-Programms

Ein solches Programm schafft skalierbare Sicherheitswirkung in der Fläche — nicht durch Zentralisierung, sondern durch Empowerment dezentraler Multiplikatoren. Richtig implementiert, wird das Security Champions Netzwerk zur kultu-

rellen Immunabwehr der Organisation – anpassungsfähig, responsiv und tief im operativen Alltag verankert.

Damit ein Security Champions Programm nicht nur formal existiert, sondern wirksame kulturelle Impulse im Tagesgeschäft setzt, braucht es mehr als gute Absicht: Es braucht klare Struktur, kontinuierliche Pflege und echte Teilhabe. Die folgenden praxisbewährten Empfehlungen unterstützen dabei, ein belastbares, skalierbares und motivierendes Champions Programm aufzubauen und langfristig erfolgreich zu betreiben:

Tipp 1 - Klein starten, iterativ skalieren

Beginne mit einem Pilot in einem motivierten Bereich (z. B. Engineering, Customer Operations) und optimiere Struktur, Kommunikation und Enablement iterativ, bevor du das Programm unternehmensweit ausrollst.

Tipp 2 - Champions nicht überfrachten – Fokus halten

Champions sind keine Mini-CISOs. Formuliere klare Erwartungshaltungen: z. B. ein monatliches Security-Standup im Team, ein konkretes Thema pro Quartal (z. B. Secrets Management, Phishing, Access Hygiene).

Tipp 3 - Champions in echte Entscheidungsprozesse einbinden

Nutze Champions aktiv in Retrospektiven, Incident-Reviews, Tool-Auswahlprozessen oder bei Policy-Rollouts. So entsteht Ownership und du erhältst wertvolles operatives Feedback.

Tipp 4 - Sichtbarkeit schaffen – intern und cross-funktional

Stelle die Champions im Intranet, auf Townhalls oder in All-Hands Calls regelmäßig vor. Fördere Austausch zwischen Champions durch monatliche Community-Calls oder ein »Champion-of-the-Month»-Format.

Tipp 5 - Sicherstellen, dass Führungskräfte mitziehen

Das Programm steht und fällt mit dem Support der Führungskräfte in den Fachbereichen. Kommuniziere klar, dass das Zeitbudget der Champions kein »nice to have», sondern Teil des Sicherheits-Commitments ihres Teams ist.

Tipp 6 - Playbooks & Micro-Learnings bereitstellen

Statt nur generischer Trainingsmaterialien: Stelle konkret einsatzbare Playbooks, One-Pager oder Mini-Guides zur Verfügung – z. B. »Wie spreche ich mit meinem Team über MFA?», »Security-Tipps für Onboarding», »Review-Checklist für Infrastructure-as-Code».

Erfolgsfaktoren und Risiken in der Umsetzung

Die erfolgreiche Implementierung und langfristige Wirksamkeit eines Security Champions Programms hängt wesentlich davon ab, ob es gelingt, Rahmenbedingungen, Führungssignale und operative Mechanismen kohärent auszurichten. Während viele Programme gut starten, scheitern sie später an fehlender Verbindlichkeit, Überlastung der Beteiligten oder unzureichender Skalierbarkeit.

Die folgenden Faktoren haben sich in der Praxis als entscheidend für nachhaltige Wirkung erwiesen:

1. **Leadership-Sponsoring durch CTO, COO und Linienführung**

   Ohne Top-Level-Unterstützung bleibt das Programm symbolisch. Idealerweise äußern sich CTO, COO oder CISO regelmäßig öffentlich zur strategischen Bedeutung des Programms, insbesondere gegenüber mittlerem Management.

2. **Sichtbare Anerkennung durch HR-Formate oder interne Awards**

   Verankerung von Security Champions in HR-Systeme, Karrierepfade oder Performanceformate (z. B. interne Awards, Entwicklungsgespräche) erhöht Status, Sichtbarkeit und Anreiz deutlich.

3. **Regelmäßiger Austausch und Community Building**

   Monatliche Sync-Calls, Retrospektiven oder "Champion Clinics" schaffen Plattformen für Wissensaustausch, Peer-Lernen und Identitätsbildung – entscheidend für Motivation und Kohäsion.

4. **Kultur-Monitoring durch kombinierte quantitative und qualitative Daten**

   Effektivität wird messbar, wenn KPI-Daten (z. B. Phishing-Quoten, Incident-Meldungen) mit qualitativem Feedback aus Surveys oder 1:1s trianguliert werden. Das schafft ein ganzheitliches Lagebild zur kulturellen Reife.

In Tabelle 5 sind zentrale Risiken aus der praktischen Umsetzung dargestellt – zusammen mit erprobten Gegenmaßnahmen, die auf Skalierbarkeit und Resilienz des Programms zielen:

Risiko	Gegenmaßnahme
Champion-Überlastung	Definiere klare Rollenprofile und verankere das Zeitbudget verbindlich im HR-System (z. B. über SAP SuccessFactors o. Ä.). Nur so lässt sich nachhaltiges Engagement sicherstellen.
Intransparente Wirkung	Etabliere ein KPI-Set und visualisiere Fortschritte in Dashboards, die monatlich im Security-Team und quartalsweise mit dem Management geteilt werden.
Fehlende Skalierbarkeit	Nutze bewährte DevOps- und Agile-Prinzipien: Starte mit einem MVP, iteriere pro Geschäftsbereich und fördere autonome Lokaleigentümerschaft.
Geringe Motivation	Implementiere Peer-Recognition-Mechanismen wie »Champion of the Quarter», Sichtbarkeit im Intranet, Zertifikate oder sogar Einbindung in Beförderungsgespräche.

Tab. 2.5: Tabelle 5 Typische Fallstricke und empfohlene Gegenmaßnahmen

Ein Champions-Programm ist kein einmaliges Projekt, sondern ein organisationaler Lern- und Führungsprozess. Wer ihn systematisch steuert, institutionell absichert und kulturell pflegt, schafft einen dauerhaften Multiplikator für Sicherheitsverhalten – resilient gegen Personalwechsel, Wachstum und Wandel.

Fazit: Sicherheitskultur als Steuerungs- und Resilienzfaktor

Sicherheitskultur ist kein Begleitthema – sie ist ein zentraler Steuerungsmechanismus im modernen Cybersecurity Operating Model. In einer zunehmend dynamischen, digitalen und dezentralen Unternehmenswelt reicht es nicht aus, Sicherheit nur technisch oder regulatorisch zu denken. Die kollektive Haltung, Entscheidungslogik und das Alltagsverhalten der Mitarbeitenden bestimmen maßgeblich, wie effektiv Sicherheitsmaßnahmen wirken – oder scheitern.

Deshalb muss Sicherheitskultur als strukturierter Bestandteil der Unternehmenssteuerung verstanden, geführt und kontinuierlich weiterentwickelt werden. Sie gehört nicht in den Projektbereich »Awareness», sondern in das Kernportfolio des CISO-Offices – mit klaren Zielen, Metriken, Rollen und Governance.

Security Champions Programme liefern die notwendige operative Tiefe, um diese Kultur dezentral, teamnah und skalierbar zu verankern. Sie ermöglichen es, Sicherheitsprinzipien dort wirksam zu machen, wo zentrale Policies und Tools allein nicht greifen: in konkreten Alltagssituationen, Entscheidungsprozessen und Teamritualen.

Richtig aufgesetzt, erzeugen sie eine messbare Wirkung auf:

- das Risikoprofil des Unternehmens (durch frühe Risikoerkennung und -vermeidung),
- die Reaktionsfähigkeit bei Incidents (durch informierte, vertrauensvolle Eskalationspfade),
- das regulatorische Standing (durch gelebte statt nur dokumentierte Compliance).

Denn am Ende gilt:

»Kultur ist nicht das, was auf dem Poster steht – sondern das, was im Incident passiert.«

Eine starke Sicherheitskultur zeigt sich nicht im Corporate Design, sondern in der kollektiven Reaktion auf Unsicherheit, Störungen und Bedrohungen. Wer Kultur operationalisiert, schafft nicht nur Awareness – sondern organisatorische Resilienz.

Referenzen

- Andrew Rose & Hellemann, N. (2024, August 6). Episode 8: Discover the perspective of a CISO on how to create a security culture and manage human risk effectively. SOSAFEAwareness. Abgerufen am 3. September 2025, von https://sosafe-awareness.com/blog/andrew-rose-security-culture-human-risk-management/ AdviseraSoSafeInfosec InstitutearXiv+1YouTube+10NinjaOne+10cybrela.com+10Wikipedia
- Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S., & Lopata, A. (2024). Holistic Information Security Management and Compliance Framework. Electronics, 13(19), 3955. https://doi.org/10.3390/electronics13193955 MDPI
- Infosec Institute. (2021, April 16). Your Company Needs a Security Champion Now. Infosec Institute. Abgerufen am 3. September 2025, von https://www.infosecinstitute.com/resources/security-awareness/what-is-a-security-champion-definition-necessity-andemployeeempowerment/ Wikipedia+6Infosec Institute+6cisotradecraft.substack.com+6
- Infosecurity Magazine. (2024, Oktober 14). How Security Champions Programs Lead to Cultural .... Infosecurity Magazine. Abgerufen am 3. September 2025, von https://www.infosecuritymagazine.com/newsfeatures/security-championscultural/ Infosecurity Magazine
- PivotPoint Security. (2024, August 6). The Role of Leadership in ISO 27001 Compliance. PivotPoint Security. Abgerufen am 3. September 2025, von htt-

ps://www.pivotpointsecurity.com/the-role-of-leadership-in-iso-27001-compliance/ Pivot Point Security+1

- Vanta. (2025, April 10). Key differences between ISO 27001 and NIS 2 explained. Vanta. Abgerufen am 3. September 2025, von https://www.vanta.com/resources/nis-2-and-iso-27001 A-LIGN+7Vanta+7Bright IT+7
- Advisera (Kosutic, D.). (2023?). NIS 2 vs. ISO 27001 mapping. Advisera. Abgerufen am 3. September 2025, von https://advisera.com/articles/nis-2-iso-27001-map/ Advisera
- Bright Global. (k. d.). NIS 2 and ISO 27001: What You Need to Know and How …. Bright Global. Abgerufen am 3. September 2025, von https://www.bright.global/en/blog/nis2-iso27001-comparison-cybersecurity Bright IT
- NinjaOne. (2025, August 4). NIS2 vs ISO 27001: What's the Difference?. NinjaOne Blog. Abgerufen am 3. September 2025, von https://www.ninjaone.com/blog/nis2-vs-iso-27001/ NinjaOne
- Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021, Juni 28). Developing a cyber security culture: Current practices and future needs (preprint). arXiv. Abgerufen am 3. September 2025, von https://arxiv.org/abs/2106.14701