RISKFLIX

WHITEPAPER 2025

LEAN INFORMATION SECURITY RISK MANAGEMENT

EIN MANIFEST

Deine **8-Punkte-Agenda** für eine effektive & effiziente Cyber Security Risk Steuerung.

"Wenn Compliance zur Kultur wird."

Ein Whitepaper von RISKFLIX

WWW.RISKFLIX.DE

8-PUNKTE-AGENDA FÜR MEHR IMPACT

01
Das "WHY"
Warum ein neuer, schlanker Ansatz für ISRM notwendig ist.

02
Warum der Klassiker scheitert
Die 4 Symptome der Ineffizienz und Inakzeptanz im klassischen Risikomanagement.

03
Das Cyber Risk Manifest
4 Leitlinien, die den Prozess vor die Dokumentation stellen.

04
Deine 5 Game-Changer
Die konkrete Methodik zur praktischen Umsetzung des Manifests.

05
Praktische Einführung
Zwei Ankerpunkte, um sofort im Unternehmen zu starten.

06
Abgleich mit Standards
Wie der Lean-Ansatz ISO, NIS2 und CRA erfüllt.

07
Apropo Mensch & Kultur
Trainings als Schlüssel zur Beschleunigung der Risikokultur.

08
Fazit & Ausblick
Zusammenfassung und die Vision von RISKFLIX.

00

Intro: Executive Summary

ZUSAMMENFASSUNG (EXECUTIVE SUMMARY)

Dieses Whitepaper beschreibt einen **leanen Ansatz** für Information Security Risk-Management (ISRM), welcher konsequent auf Wertbeitrag, Pragmatismus und Zusammenarbeit setzt – und gleichzeitig die formalen Anforderungen der relevanten Standards (ISO 27001/27005/31000) und Richtlinien (NIS2, CRA, IEC 62443) erfüllt.

Anstelle schwerfälliger, rein dokumentengetriebener Risiko-Routinen werden:

- leane, teil-automatisierte Prozesse,
- gut moderierte Workshops zwischen Menschen (Risk-Talks) und
- transparente, nachvollziehbare Risiko-Analysen

in den Mittelpunkt gestellt.

"Das Risk Manifest for Lean Information Security Risk Management ist Ihr Leitbild, um manuelle Aufwände drastisch zu reduzieren, die Risikokultur zu stärken und Ihr ISRM vom Audit-Gatekeeper zum strategischen Business Enabler zu transformieren."

01

Das "WHY"

Information Security Risk Management kann auch sexy sein

Informationssicherheitsrisiken sind heute ein Dauerthema in jedem C-Level-Meeting. Doch die Prozesse, die dieses Risiko steuern sollen, leiden oft unter mangelnder Akzeptanz und fehlender Attraktivität.

Die Kernthese:

*Information Security Risk-Management in der Informationssicherheit darf den Frust ablegen und zur **Inspiration** werden.*

DIESE INSPIRATION IST DER NOTWENIGE MOTOR FÜR DEN WANDEL & BEINHALTET:

Inspiration für die Allokation

Die Fähigkeit und der Antrieb, die wirklichen Informationssicherheitsrisiken präzise zu allokieren und zu priorisieren.

Inspiration für die Gegenseite

Das tiefgreifende Verständnis der Angreifer-Perspektive (Taktiken, Motive, Ziele) um die eigene Verteidigung strategisch zu stärken.

Inspiration für die Gestaltung

Die aktive Etablierung von Informationssicherheit als Business Enabler, welcher Innovation schützt und Geschäftsprozesse ermöglicht.

Was bedeutet "Sexy"?

R **RELEVANT**
Es spricht die Sprache des Business und adressiert messbare Werttreiber.

E **EFFIZIENT**
Es entlastet die Mitarbeitenden durch smarte Automation.

K **KULTURELL**
Es ist inspirierend, nicht belehrend – es motiviert zur proaktiven Mitarbeit.

Ziel ist es, den Fokus von der reinen "Pflichtübung Audit" auf die "leidenschaftliche Sicherung des Geschäftserfolgs" zu lenken.

Inspiriert dieses Whitepaper zu schreiben hat mich folgende Fragestellung, welche ich bei zahlreichen Unternehmen beobachten durfte:

> *„Wie schafft es eine Organisation, ein wirkliches Information Security Risk Management zu etablieren, welches auf der einen Seite die Risiko-Kultur **stärkt** und auf der anderen Seite den Prozess kontinuierlich betreibt – statt Ihn nur „kurz vor knapp“ zwei Wochen vor einem Audit zu reaktivieren?“*

02

Warum der Klassiker scheitert

Trotz steigender Budgets und komplexer GRC-Tools wird das klassische ISRM (Information Security Risk Management) von der Praxis oft abgelehnt. Die Ursachen sind u.a. strukturell und kulturell.

Aktuelle Studien zeigen den Misserfolg:

Fehlendes Know-how (techconsult, 2024)

Es mangelt an ausreichend Personal, mit den nötigen Kompetenzen und einem ausreichenden Budget, um definierte Maßnahmen wirksam und nachhaltig umzusetzen.

Druck (Trend Micro, 2024)

Viele IT-Sicherheitsverantwortliche fühlen sich unter Druck gesetzt, Cyber-Risiken herunterzuspielen, da die Geschäftsleitung die Risiken erst nach einem schwerwiegenden Vorfall entschlossen angehen würde.

Mangelnde Resilienz (PwC & WEF 2025)

Die Studie: PwC Global Digital Trust Insights 2024 & WEF Global Cybersecurity Outlook 2025 haben aufgezeigt, dass trotz steigender Budgets weniger als 3% der Unternehmen als wirklich „resilient“ gegen moderne Angriffe sind.

Diskrepanz (Deloitte)

Große Beratungsfirmen bestätigen regelmäßig: Die Hauptprobleme liegen in der Diskrepanz zwischen wahrgenommenem Risiko und der Reaktion darauf.

Die 4 Symptome der Ineffizienz

01

Symptom 1: Die Kluft

Die Kluft zum Business (Silo-Arbeit): Risikoanalysen finden "kurz innerhalb der IT" statt, ohne Vertreter aus Fachbereichen & das Business einzubeziehen. Die Folge: Fehlende Kontextualisierung und mangelnde Akzeptanz für Maßnahmen.

02

Symptom 2: GRC-Tool

Das GRC-Tool-Dilemma: der Risk Manager wird zum "Dateneintippen" verdammt ("Ich muss schon wieder in mein GRC Tool..."), wodurch der Fokus auf die Dokumentation und nicht auf die Minderung liegt.

03

Symptom 3: Vollständigkeit

Der Trugschluss der Vollständigkeit: Es wird versucht, jedes kleine Risiko-Szenario zu erfassen (statt sich auf die Top 3 oder Top 5 Risiko-Szenarien zu konzentrieren), was zu seitenlangen Reports führt, die niemand liest und die keine klaren Entscheidungen liefern.

04

Symptom 4: Kalender

Kalender- vs. Ereignisgetrieben: Risiko-Reviews sind kalendergetrieben ("einmal im Jahr fürs Audit"), statt auf dynamische Veränderungen (Projekte, neue Produkte, Akquisitionen) zu reagieren.

Das Ergebnis:

- Risiko-Management wird als Pflichtübung wahrgenommen, statt als Steuerungsinstrument.
- Entscheidungen sind schwer nachvollziehbar – intern, wie extern (z.B.: gegenüber Auditoren & Aufsichtsbehörden).
- Es entsteht eine Kluft zwischen formaler Compliance & gelebter Cyber-Security.

*"**Steigt** denn dadurch unser Deckungsbeitrag oder etwas überspitzer „verdienen wir dadurch einen Euro mehr?"*

Gleichzeitig steigen die Anforderungen

ISO 27001	ISO/IEC 27001:2022 erwartet ein systematisches Informationssicherheits-Risikomanagement mit definierter Methodik, dokumentierten Bewertungen und nachvollziehbaren Entscheidungen.
NIS2	NIS2 erweitert den Kreis der betroffenen Unternehmen deutlich und verlangt ein angemessenes, verhältnismäßiges Risiko-Management für Netz- und Informationssysteme, sowie den Nachweis getroffener Maßnahmen.
CRA	Risikomanagement ist DER Schlüssel, um den CRA (Cyber Resilience Act) zu erfüllen & nachhaltige Cyber-Security zu erreichen. Risiken müssen systematisch bewertet & adressiert werden (über den gesamten Lebenszyklus).
MaschinenVO	Die Maschinenverordnung (ab Januar 2027 verbindlich in allen EU-Mitgliedsstaaten). Risikomanagement ist hier ebenfalls auch ein integraler Bestandteil, denn es gibt eine sogenannte Risikobewertungspflicht, z.B.: Sicherheitsfunktionen dürfen nicht durch Angriffe deaktiviert werden und Hochrisiko Maschinen (z.B.: AI gestützte Systeme) unterliegen strengeren Anforderungen.
IEC 62443	Die IEC 62443 hat folgendes Prinzip: Sicherheit orientiert sich an der konkreten Risikolage, nicht an generischen Mindeststandards. Mit der IEC 62443-3-2, 3-3 kann ein vollständig valider risikobasierter Ansatz erreicht werden.

Die Herausforderung lautet daher:

Wie kann ein Information Security Risk Management schlank, lebendig und wertestiftend sein – und trotzdem ISO- NIS2 usw. konform?

03

Das Cyber Risk Manifest

Als Antwort auf diese Herausforderung formulieren wir ein Manifest, das den Charakter eines Leitbildes hat – weniger Formalismus, mehr Wirkung, ähnlich dem Agile Manifest, welches sich jedoch auf Informationssicherheitsrisiken fokussiert.

Wir entdecken bessere und schlankere Wege, Informationssicherheitsrisiken zu bewerten & zu managen, indem wir den aktuellen Status Quo in Frage stellen und mutig genug sind, andere damit zu inspirieren. Durch diese Arbeit haben wir folgende Leitlinien entwickelt:

Leane, teil-automatisierte Prozesse und gut moderierte Workshops zwischen Menschen

STEHEN ÜBER

schwerfälligen, rein dokumentengetriebenen Risiko-Routinen und isolierte Bewertungen durch das Sec-Team selbst.

Der traditionelle Ansatz ist toolgetrieben und starr. Dieses Manifest stellt den Menschen und den Wert in den Mittelpunkt. Die Zeit des Cyber Security Risk Managers wird nicht mit Copy-Paste-Tabellen verschwendet, sondern in bilateralen Dialogen mit dem Business investiert.

Isolierte Bewertungen durch das Sec-Team selbst ist fatal – bricht die Cyber-Security Silos auf und holt das Business, den Fachbereich, Product, OPS & DEV an den Tisch. Teil-Automatisierung von Routineaufgaben (wie der Datenerfassung) ist lediglich ein Mittel zum Zweck, um Zeit für die eigentliche Risikobewertung in fokussierten, gut moderierten Workshops zu gewinnen.

Gut ausgebildete Cyber Security Risk Manager sind der Schlüssel, die Workshops schlagkräftig zu moderieren und die richtigen Fragen zu stellen, um wirklich an den Kern des Problems zu kommen. Dokumente sind wichtig und richtig, jedoch folgen Sie dem Prozess, nicht umgekehrt.

Transparente, nachvollziehbare Risiko-Analysen

STEHEN ÜBER

seitenlangen Reports, die niemand liest.

Die Qualität einer Risikoanalyse wird nicht an ihrer Dicke, sondern an ihrer Entscheidungsfähigkeit gemessen. Hochkomplexe Scorings, welche einer Bedingungsanleitung gleicht und mehr Verständnisfragen aufruft sollten der Vergangenheit angehören.

Der Lean-Ansatz fordert Analysen, die auf wenigen Seiten oder in einem Dashboard die wesentlichen Risiken und die gewählten Maßnahmen auf den Punkt bringen. Transparenz bedeutet hier, dass die Begründung der Eintrittswahrscheinlichkeit & des Business Impacts für alle Stakeholder – vom Fachbereich bis zum externen Auditor – gleichermaßen verständlich ist. Lieber ein schlanker Report, der Entscheidungen auslöst, als ein dicker Report, welcher niemand öffnet.

Storytelling und Kultur

STEHEN ÜBER

FUD (Fear, Uncertainty, Doubt) und Checkbox-Compliance.

FUD erzeugt kurzfristige Angst, aber keine langfristige, intrinsische Motivation und Kultur. Die Risikokultur wird erst dann lebendig, wenn das Risiko relevant und emotional greifbar wird.

Wir wollen weg von abstrakten Risikobeschreibungen und hin zu persönlichen, kontextualisierten Geschichten (Storytelling). Compliance wird zur "Checkbox-Compliance", wenn sie nur aus Angst vor dem Audit abgearbeitet wird. Eine starke Kultur hingegen erfüllt Compliance als glücklichen Nebeneffekt einer gelebten Sicherheit.

Cyber-Risk-by-Design

STEHT ÜBER

nachträglicher Dokumentation ("kurz vor knapp").

Die teuersten Fehler sind jene, die in der Konzeptionsphase ignoriert und erst kurz vor der Inbetriebnahme eines Systems entdeckt werden.

Der Lean-Ansatz erfordert die Integration der Risiko-Betrachtung in den frühestmöglichen Zeitpunkt des Entwicklungs- oder Change Prozesses (z. B. im Rahmen von Projektvorlagen oder Architekturentscheidungen). Risiko-Management wird damit von einer Bremsspur am Ende des Prozesses zu einem Beschleuniger am Anfang.

04

Deine 5 Game-Changer

Die „philosophischen Leitlinien“ des Manifests werden durch fünf konkrete, sofort umsetzbare Game-Changer in die Tat umgesetzt. Diese Game-Changer definieren die neue, leane Methodik.

GC 1 Storytelling statt FUD

KULTUR-HEBEL

Dies ist der wichtigste Hebel, um die Kluft zwischen Security und Business zu schließen. Anstatt über abstrakte Risiko-Szenarien zu sprechen, übersetze die Risko-Szenarien in relevante Geschichten (Micro-Learning) (à la RISKFLIX), um eine spezifische Attacke zu verankern. Das Business darf das „WHY“ dahinter verstehen.

Als Beispiel könnten wir folgende Leitfragen bei einer Erstellung eines Risiko-Szenarios helfen:

- Wer oder Was greift euch an? Z.B.: Organisierte Gruppen, Staatliche Akteure, Hacktivisten, Wettbewerber oder einfache Skript-Kiddies? Vielleich aber auch Interne Angreifer oder ein Third Party Supplier?
- Welche Motivation hat ein potentieller Angreifer die Vertraulichkeit, Verfügbarkeit und Integrität zu beeinträchtigen?
- Wie leicht kann ein potenzieller Angreifer die Schwachstelle ausnutzen?
- Was ist der wirkliche „Attack Path“? Beschreibe das Risiko-Szenario daraus resultierend und gebe dediziert an, wie ein potentieller „Attack Path“ aussehen kann?
- Beschreibe den dazugehörigen Business-Impact. Wieso hast du dich mit dem Business, Fachbereich & der IT darauf geeinigt?

GC 2 Teil-Automatisierung

EFFIZIENZ-HEBEL

Die Zeit des Cyber Security Risk Managers ist zu wertvoll, um sie mit der Pflege und Dokumentationen von Listen zu verbringen. Die Lösung liegt in der Standardisierung und Teil-Automatisierung, sowie der Reduzierung der Komplexität:

Blueprints und Vordefinierte Szenarien:

Nutzen Sie wiederverwendbare Bausteine für Standardtechnologien oder bekannte Angriffsvektoren.

Beispiel BluePrint im OT/Shopfloor:

Ein vordefiniertes Risko-Szenario wie „Fehlendes Patch-Management." oder „Fernwartungszugang kompromittiert" hat bereits die typische Auswirkungen (Produktionsstopp, Anlagenschaden) und eine initiale Risikobewertung hinterlegt.

Beispiel BluePrint (Windows 7 Clients):

Ein BluePrint für Windows 7 Clients in einer kritischen Umgebung (z.B.: Teststände) enthält vordefinierte, erhöhte Risiko-Einstufungen für Viren/Malware und Patches, sowie Standard-Kompensationsmaßnahmen (Netzwerk-Segmentierung, fehlender Internetzugang). Der Cyber Security Risk Manager kann hier auf vordefinierte Risiko-Szenarien inkl. Bedrohungs- und Schwachstellenbeschreibung zugreifen, um effizienter zu arbeiten.

Maßnahmen-Katalog:

Legen Sie Standard-Maßnahmen (z. B. "MFA für alle Cloud-Zugänge") fest. Der Risk Manager wählt nur noch aus und passt an, anstatt jede Kontrolle neu zu definieren.

Die Teil-Automatisierung entlastet das Team von Routineaufgaben und erlaubt es, die freigewordene Zeit in den Dialog (GC 4) zu investieren.

GC 3 80/20 Regel: Fokus auf die Top 10 PRIORISIERUNG

Der Trugschluss der Vollständigkeit lähmt. Deshalb ist es wichtig innerhalb einer Risiko-Analyse einen Scope zu definieren (IN-Scope, sowie OUT-of-Scope). Das Scoping hilft den Stakeholdern (Business, Fachbereich, IT & Management) im ersten Ansatz zu verstehen, welche Prozesse, Systeme und/oder Schnittstellen tatsächlich betrachtet werden.

Konzentrieren Sie sich innerhalb einer Risiko-Analyse auf die Top 5 oder je nach Komplexität auf die Top 10 Risiko-Szenarien. Diese erhalten 90% Ihrer Analysezeit, werden dem Management klar kommuniziert und dürfen im Nachgang kontinuierlich überwacht werden. Dies erhöht auch die Transparenz der Risikosteuerung.

GC 4 Risk-Talks statt Risk-Tools KOMMUNIKATION

Die gewonnene Zeit aus der Teil-Automatisierung (GC 2) muss in den Dialog bzw. Workshop fließen. Risk-Talks oder Risk-Workshops sind kurze, strukturierte und gut moderierte Sessions mit dem Fachbereich, dem Business & der IT.

Im ersten Workshop ist es elementar wichtig, so viel wie möglich Daten zu sammeln, um sich ein Big-Picture zu erschaffen. In den weitergehenden Workshops dürfen dann die Risiko-Szenarien kreiert werden, in welchem eine gemeinsame Entscheidung der Bewertung durchgeführt und die Risikobehandlung abgestimmt wird.

> *An diesem Punkt differenziert sich ein exzellentes und leanes Risikomanagement vom Durchschnitt. Die wahre Königsdisziplin liegt in der Kommunikation: Effektives Storytelling, gezieltes Stakeholder-Management und die verständliche Übersetzung komplexer „Attack Paths" sind Fähigkeiten, welche es zu meistern gilt. Dies wiederum schafft echten Impact, stärkt die Risiko-Kultur und schafft den Effekt einer gelebten Cyber-Security. Daher: investieren Sie hier in gute Cyber Security Risk Managers – dies bringt Ihr Unternehmen aufs nächste Level.*

GC 5 Cyber-Risk-by-Design INTEGRATION

Risikomanagement muss zum Frühwarnsystem werden. Die Integration in den Change- und Projektprozess (z. B. im Rahmen von Architektur-Reviews oder der Auswahl kritischer Lieferanten) ist essenziell.

Statt aufwendiger Analysen am Ende nutzen Sie **Light-Analysen** (basierend auf GC 2-Blueprints) zu Beginn. Dies stellt sicher, dass Risiken nicht nachträglich dokumentiert, sondern aktiv vermieden werden. Dies ist der Schlüssel zur Erfüllung von CRA und IEC 62443.

05 Praktische Einführung

„Risikomanagement in der Informationssicherheit darf den Frust ablegen und muss zur Inspiration werden“

Dies ist die Kern-These des Manifests.

Zwei elementar wichtige Ankerpunkte, wie Sie in Ihrem Unternehmen starten können:

1. Manifest offiziell machen

- In ein **einseitiges** PDF oder „Mural Board“ packen.
- In einem Security- oder Steering-Committee vorstellen und beschließen: „So wollen wir Information Security Risk Management jetzt denken“.
- Gekoppelt mit der Verfahrensanweisung innerhalb des ISMS (Information Security Management System).

2. Top 5 Game-Changer als „kleines Programm“ aufsetzen

Für jeden Game-Changer 1 Mini-Task definieren:

- **GC1:** Standard-Situationen + 2-seitiges Standard-Template bauen. Storytelling ist nicht schwierig, es bedarf Übung. Bei Bedarf: alle bestehenden Risiken werden in „Human-Sprache“ umformuliert.
- **GC2:** Top 5 BluePrints und die Top 10 vordefinierten Risiko-Szenarien etablieren. Wenn Windows 7 noch im Einsatz ist und/oder sämtliche unsichere Protokolle, dann etabliere nachvollziehbare, gut beschriebene Risiko-Szenarien.
- **GC3:** Workshop mit dem Fachbereich, Business & IT, sowie dem Management, um die Top 10 Risiko-Szenarien zu definieren. Dahinter steckt: kennen wir unsere kritischen Geschäftsprozesse, unsere unterstützenden Prozesse und Management-Prozesse? Kennen wir unsere Top 20 kritischen Assets? Welche Prozesse / Systeme / Applikationen sind wirklich wichtig? Kennen wir unsere Angreifer? Haben wir eine Informations-Klassifizierung im Einsatz? Kennen wir den Schutzbedarf? Kurz, prägnant, präzise. Ein tendierendes Risiko-Szenario kann tatsächlich sein: wir haben kein Asset-Management.
- **GC4:** Einheitliche Vorgehensweise hinsichtlich der EWS (Eintrittswahrscheinlichkeit) + BI (Business-Impact) definieren. Reflektieren, ob Know-How aufgebaut werden muss oder vorhanden ist und ggf. nachjustieren.
- **GC5:** Aufbau auf GC3: Risikomanagement in den Change- und Projektprozess so integrieren, dass das „WHY“ vom Business verstanden wird. Im CRA (Cyber Resilience Act) ist dies nicht verhandelbar, jedoch kommuniziert ein guter Cyber Risk Manager immer das „WHY“ & dann das „HOW“ & „WHAT“.

Nach 3-6 Monaten eine Retrospektive durchführen

Was hat funktioniert?
Wo sind wir wieder in Bürokratie abgerutscht?
Manifest leicht anpassen

5.1 Was Sie tun sollten, um das Manifest audit-sicher zu machen

Wenn Sie das Manifest offiziell nutzen, würde ich drei Dinge zusätzlich festhalten:

1) Methodik-Dokument (Klassiker: Verfahrensanweisung im ISMS):
- Wie identifizieren Sie Risiken?
- Welche Skalen / Kriterien werden genutzt?
- Wie läuft ein typischer Risiko-Workshop / teil-automatisierter Prozess ab?
- Wie kommen Entscheidungen in Ihr Risiko-Register?

2) Risk-Register / Tool-Ansicht als „Single Source of Truth”:
- Für ISO-Audit / NIS2-Prüfung:
- Liste der Risiken, Bewertung, Verantwortliche
- Maßnahmen & Status, Datum der letzten Überprüfung

3) Einen Satz im ISMS bzw. innerhalb der ISRM Policy:
"Das Unternehmen verfolgt ein leanes, teil-automisiertes und kollaboratives Risikomanagement gemäß dem „Risk Manifest for lean Information Security". Umfang und Form der Risikoanalysen richten sich nach Angemessenheit, Transparenz und Nachvollziehbarkeit und erfüllen die Anforderungen von ISO/IEC 27001, sowie der umgesetzten NIS2-Regulierung. Damit zeigen Sie in einem Audit Konformität auf und machen es zeitgemäß und effizient."

06

Abgleich mit Standards

Das Lean-Manifest ist kein Gegensatz zu formalen Anforderungen. Im Gegenteil: Die Effizienzsteigerung und der Fokus auf Wirkung sind die zeitgemäße Interpretation dieser Standards und Regularien.

STANDARD / REGULIERUNG	KERNANFORDERUNG	ERFÜLLUNG DURCH LEAN-ANSATZ
ISO/IEC 27001 & 27005	Systematisches Verfahren zur Risikobewertung und -behandlung.	Die schlanke, dokumentierte Methodik (GC 2 & GC 3) und die nachvollziehbaren Entscheidungen (GC 4) erfüllen diese Anforderungen mit minimalem bürokratischem Aufwand.
NIS2-Richtlinie	Angemessenes Risikomanagement und Aufbau einer starken Sicherheitskultur.	Storytelling (GC 1) beschleunigt die Risikokultur. Die kontinuierliche Betrachtung (GC 5) durch Integration in den Alltag sorgt für die nötige Angemessenheit und Nachweisfähigkeit.
Cyber Resilience Act (CRA)	Security-by-Design und Management des Risikos über den gesamten Produktlebenszyklus.	Cyber-Risk-by-Design (GC 5) ist die direkte Umsetzung des zentralen CRA-Mandats. Es stellt sicher, dass Cybersicherheit von Anfang an in das Produkt "hineinkonstruiert" wird.
ISO IEC 62443	Sicherheit industrieller Automatisierungs- und Steuerungssysteme (OT/Shopfloor).	OT-spezifische Risk-Talks (GC 4) und die Anwendung von Risk-by-Design (GC 5) gewährleisten, dass Risiken in OT-Systemen (die Verfügbarkeit erfordern) frühzeitig in Zonen- und Conduit-Modellen berücksichtigt werden.

07

Apropo Mensch & Kultur

Der größte Hebel für ein leanes, wertschöpfendes Risikomanagement ist der Mensch. Die Rolle des Cyber Security Risk Managers ist eine Königsdisziplin, welche die Technik, aber auch das Business verstehen darf. Innerhalb unserer Trainings thematisieren wir sämtliche Standards und verpacken dies mit praxisorientierte Case-Studies, sodass Sie nach dem Training eine aussagekräftige Risiko-Analyse für Ihr Management schreiben können.

Wir bei RISKFLIX entwickeln Menschen, welche in Ihrer Organisation den Reifegrad der Cyber-Security schlagkräftig beschleunigen möchten. Der Paradigmenwechsel vom Compliance-Check Beauftragten hin zum Business-Enabler erfordert gezielte Schulungen, die wir mit unseren Kursen abdecken.

Training mit dem RISKFLIX-Effekt

Durch unsere Storytelling-Kurse trainieren Sie nicht nur technische Prozesse, sondern schaffen emotional verankerte Akzeptanz für Risikothemen. Das ist der direkteste Weg zur Beschleunigung Ihrer Risikokultur. Unsere Kurse qualifizieren die Schlüsselpersonen, welche Sie in Ihrem Unternehmen händeringend benötigen:

Global OT/IT Cyber Security Risk Manager

unsere Master-Class für ganzheitliches Information Security Risk Management im OT & IT-Umfeld. Der Goldstandard für Risk-Profis.

Global OT/IT Cyber Security Risk Champion

der kompakte Einstieg mit direkter Praxisrelevanz. Wird auch der "kleine Bruder" vom Risk Manager genannt – ideal für Multiplikatoren.

Global AI Risk Officer

AI ist gekommen, um zu bleiben. Der Global AI Risk Officer spezialisiert auf AI-bezogene Cyber-Security Risiken und bringt Ihnen den passenden Wissensvorsprung, wenn es um AI bezogene Informationssicherheitsrisiken geht.

08

Fazit & Ausblick

Das Cyber Risk Manifest ist die Einladung, den Frust des traditionellen Risikomanagements hinter sich zu lassen. Weniger Formalismus, mehr Wirkung und mutig genug zu sein, um andere damit zu faszinieren oder inspirieren. Die 5 Game-Changer bieten eine klare, praxisnahe Anleitung, um Impact zu schaffen und Compliance als natürlichen Nebeneffekt zu erzielen.

Ein leanes Information Security Risiko-Management ist kein Wunschtraum, sondern eine Business Enabler, welcher Ihre Organisation effizienter und resilienter macht.

RISKFLIX bietet hierfür die Plattform, Menschen zu befähigen, den Cyber-Security Reifegrad in Ihrer Organisation schlagkräftig zu erhöhen.

"Building legendary Cyber Risk Champions"

ist damit eine Herzensangelegenheit, Teilnehmenden in die Lage zu versetzen, direkt nach dem Training fundierte, aussagekräftige Risiko-Analysen zu erstellen und in die Umsetzung zu gehen.

Manuel Blessing

Founder RISKFLIX

Buchen Sie gerne mit mir eine kostenfreie 15-20 minütige „Cyber-Security Risk Talk-Session".

Manuel.Blessing@riskflix.de

www.riskflix.de

...und lassen Sie sich inspirieren.