SECURITY GOVERNANCE · ISMS · AUDIT READINESS · RESILIENCE

# Informationssicherheit steuerbar, prüfbar und managementfähig machen.

A.R.C. verbindet technische Realität, organisatorische Verantwortung und regulatorische Anforderungen zu belastbaren Governance-, Betriebs- und Entscheidungsstrukturen.

**33+**
historisch belegte Kunden-/ Leistungsfälle mit Projekt-, Auftrags-oder Artefaktspuren.

NIS2 / KRITIS · ISO 27001 / BSI · TISAX · SOC / SIEM · Incident / Resilience

## WANN A.R.C. UNTERSTÜTZT

### Regulierung operationalisieren
NIS2, KRITIS, ISO 27001, BSI oder TISAX müssen in Rollen, Prozesse, Maßnahmen und prüfbare Nachweise übersetzt werden.

### Sicherheitsfunktionen betreibbar machen
SOC, SIEM, Monitoring, Sicherheitsarchitektur oder GRC benötigen ein tragfähiges Betriebs- und Entscheidungsmodell.

### Handlungsdruck beherrschbar machen
Vorfall, Audit oder Managemententscheidung erfordern Priorisierung, fachliche Steuerung und belastbare Evidenz.

## LEISTUNGSFELDER

### 1 · Security Governance
Mandat, Rollen, Entscheidungswege, CISO Office und Managementsteuerung.

### 2 · ISMS & GRC
Scope, Struktur, Schutzbedarf, Risiken, Framework-Mapping und Nachweise.

### 3 · Audit Readiness
Gap-Analyse, Anforderungsschließung, SoA, Evidenzqualität und Auditbegleitung.

### 4 · Security Architecture
SOC/SIEM, Monitoring-Auswahl, Segmentierung, WAF und technische Governance.

### 5 · Incident & Resilience
Erstreaktion, Remediation, BCM, Notfallmanagement und Disaster Recovery.

## VORGEHEN

### 1 · Mandat
Entscheidung, Systemgrenze und Verantwortungsrahmen klären.

### 2 · Realität
Technik, Prozesse, Organisation, Risiken und Evidenzen gemeinsam erfassen.

### 3 · Zielmodell
Rollen, Governance, Maßnahmen, Datenobjekte und Nachweise verbinden.

### 4 · Umsetzung
Arbeitspakete, Verantwortliche, Abhängigkeiten und Entscheidungen steuern.

### 5 · Rückkopplung
Wirksamkeit, Auditfähigkeit und verbleibende Risiken sichtbar machen.

### Geeignete Mandate
- mehrere Unternehmensbereiche oder technische Gewerke
- Regulierung, Technik und Organisationsrealität passen nicht zusammen
- Management benötigt eine belastbare Entscheidungsvorlage

### Arbeitsprinzip
- Evidenz statt Compliance-Theater
- Governance vor Tool
- Umsetzung bis zur Nachweisfähigkeit

AUSGEWÄHLTE ERFAHRUNG · ANONYMISIERT

# Erfahrung an der Schnittstelle von Management, Regulierung und Technik.

## End-to-End

Von Mandat und Analyse über Steuerung und Umsetzung bis zu Audit- oder Entscheidungsfähigkeit.

### AUSGEWÄHLTE, BELEGTE MANDATSMUSTER

KRITIS / NIS2 / GRC

**Organisationsweite Sicherheits- und GRC-Transformation**

Fachlich-organisatorische Gesamtverantwortung für ISMS-Weiterentwicklung, Cross-Framework-Mapping, Struktur- und Schutzbedarfsmodell, Richtlinien, Risiko- und Evidenzintegration sowie Umsetzungsplanung.

Belegt: Der Kunde bestätigte den maßgeblichen Beitrag und empfahl die Zusammenarbeit für vergleichbare Projekte.

SOC / OPERATING MODEL

**SOC als Sicherheitsfunktion statt Toolprojekt**

Ganzheitliche SOC-Konzeption einschließlich Projektmanagement, Prozess- und Organisationsdesign sowie Koordination mehrerer technischer Spezialgebiete.

Belegt: Konzeption und fachliche Gesamtsteuerung; keine unbelegte Teamgröße oder vollständige Produktivsetzung.

TISAX / AUDIT READINESS

**Anforderungen bei zwei Industrieunternehmen schließen**

Gap-Analyse, priorisierte Anforderungsschließung, Qualitätssicherung von Richtlinien, SoA und Evidenzen sowie Auditvorbereitung.

Ergebnis: Beide Unternehmen bestanden ihre Audits; für einen Fall liegt eine ausdrückliche Kundenbestätigung vor.

INCIDENT LEADERSHIP

**Cyberangriff bei einem regulierten Versicherer**

Management der Erstreaktion und anschließenden Bewältigung, fachliche Koordination mehrerer technischer Gewerke und Unterstützung der regulatorischen Kommunikation.

Grenze: Keine Veröffentlichung von Vorfalldetails; keine unbelegte Aussage zu vollständiger Remediation.

TECHNISCHES AUDIT

**WAF-Audit nach BSI IT-Grundschutz**

Dokumentarische und technische Prüfung von Governance, Berechtigungen, Kryptographie, Administration, Logging, SIEM-Anbindung, Patchmanagement und Netzarchitektur.

Belegt: Auditbericht und technische Feststellungen; keine eigenen Penetrationstests oder Schwachstellenscans.

CISO / ISMS

**Mehrjährige Begleitung im regulierten Umfeld**

Begleitung einer CISO-Funktion beim ISMS-Aufbau einschließlich Security-Konzeption, Risiko- und Bedrohungsanalyse, Awareness und technischer Vertiefungen.

Belegt: Mehrjährige Zusammenarbeit und wiederkehrende Beauftragung; keine unbelegte Zertifizierungsaussage.

### ARBEITSPRINZIPIEN

**Evidenz statt Compliance-Theater**

Aussagen, Entscheidungen und Auditfähigkeit müssen durch belastbare Quellen gestützt sein.

**Governance vor Tool**

Werkzeuge unterstützen ein Betriebsmodell; sie ersetzen weder Rollen noch Prozesse.

**Technik und Organisation gemeinsam**

Konfiguration, Betrieb, Verantwortung und Managemententscheidung werden verbunden.

**Frameworks integrieren**

Kontrollen und Evidenzen werden wiederverwendet statt in parallelen Welten dupliziert.

**Managementfähig entscheiden**

Risiken, Optionen, Abhängigkeiten und Unsicherheit werden entscheidbar dargestellt.

**Bis zur Nachweisfähigkeit**

Analyse endet nicht bei der Gap-Liste, sondern bei Maßnahmen, Verantwortlichen und Evidenz.

Leistungsgrenze: A.R.C. ersetzt keine Rechtsberatung, Abschlussprüfung oder technische Produktinstallation, sofern dies nicht ausdrücklich vereinbart ist. Zertifizierung, regulatorische Anerkennung oder vollständige Risikofreiheit werden nicht garantiert.

**Nächster Schritt: Entscheidungsbedarf und nächsten belastbaren Meilenstein klären.**

Ein strukturiertes Erstgespräch ordnet Ausgangslage, Scope, verfügbare Evidenzen und den sinnvollen Einstieg ein: Analyse, Managemententscheidung, Umsetzungssteuerung oder Audit Readiness.

www.a-r-c.me
a.ruehl@a-r-c.me