SECURITY GOVERNANCE · ISMS · AUDIT READINESS · RESILIENCE

Make information security manageable, auditable and ready for management decisions.

A.R.C. connects technical reality, organizational accountability and regulatory requirements into reliable governance, operating and decision structures.

33+
documented client and service contexts supported by project, engagement or artifact evidence.

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

WHEN A.R.C. CAN HELP

Operationalize regulatory requirements
NIS2, KRITIS, ISO 27001, BSI or TISAX requirements need to be translated into roles, processes, actions and auditable evidence.

Make security functions operational
SOC, SIEM, monitoring, security architecture or GRC need a viable operating and decision model.

Manage immediate pressure
An incident, audit or management decision requires prioritization, subject-matter leadership and reliable evidence.

CAPABILITY AREAS

1 · Security Governance
Mandate, roles, decision paths, CISO Office and management oversight.

2 · ISMS & GRC
Scope, structure, protection needs, risks, framework mapping and evidence.

3 · Audit Readiness
Gap analysis, requirement closure, SoA, evidence quality and audit support.

4 · Security Architecture
SOC/SIEM, monitoring selection, segmentation, WAF and technical governance.

5 · Incident & Resilience
Immediate response, remediation, BCM, emergency management and disaster recovery.

DELIVERY APPROACH

1 · Mandate
Clarify the required decision, system boundary and accountability framework.

2 · Reality
Assess technology, processes, organization, risks and evidence together.

3 · Target model
Connect roles, governance, actions, data objects and evidence.

4 · Implementation
Manage work packages, accountable owners, dependencies and decisions.

5 · Feedback
Make effectiveness, audit readiness and residual risks visible.

Suitable engagements
- multiple business units or technical workstreams
- regulation, technology and organizational reality do not align
- management needs a reliable basis for decisions

Working principle
- Evidence instead of compliance theatre
- Governance before tools
- Implementation through to evidence readiness

SELECTED EXPERIENCE · ANONYMIZED

Experience at the intersection of management, regulation and technology.

End-to-End

From mandate and analysis through leadership and implementation to audit or decision readiness.

SELECTED EVIDENCED ENGAGEMENT PATTERNS

KRITIS / NIS2 / GRC

Enterprise-wide security and GRC transformation

Subject-matter and organizational lead responsibility for ISMS enhancement, cross-framework mapping, structure and protection-needs model, policies, risk and evidence integration, and implementation planning.

Evidence: The client confirmed the material contribution and recommended the engagement for comparable projects.

SOC / OPERATING MODEL

SOC as a security function rather than a tool project

End-to-end SOC design including project management, process and organizational design, and coordination of multiple technical specialties.

Evidence: Design and overall subject-matter leadership; no unsupported claim regarding team size or full production rollout.

TISAX / AUDIT READINESS

Closing requirements at two industrial companies

Gap analysis, prioritized requirement closure, quality assurance of policies, SoA and evidence, and audit preparation.

Outcome: Both companies passed their audits; explicit client confirmation is available for one engagement.

INCIDENT LEADERSHIP

Cyberattack at a regulated insurer

Management of the immediate response and subsequent handling, subject-matter coordination of multiple technical workstreams, and support for regulatory communications.

Boundary: No disclosure of incident details and no unsupported claim of complete remediation.

TECHNICAL AUDIT

WAF audit against BSI IT-Grundschutz

Documentation-based and technical review of governance, access controls, cryptography, administration, logging, SIEM integration, patch management and network architecture.

Evidence: Audit report and technical findings; no penetration testing or vulnerability scanning performed.

CISO / ISMS

Multi-year support in a regulated environment

Support to a CISO function during ISMS development, including security design, risk and threat analysis, awareness and technical deep dives.

Evidence: Multi-year collaboration and recurring engagements; no unsupported certification claim.

WORKING PRINCIPLES

Evidence instead of compliance theatre

Claims, decisions and audit readiness must be supported by reliable sources.

Governance before tools

Tools support an operating model; they replace neither roles nor processes.

Technology and organization together

Configuration, operations, accountability and management decisions are connected.

Integrate frameworks

Controls and evidence are reused instead of duplicated across parallel structures.

Enable management decisions

Risks, options, dependencies and uncertainty are structured for decision-making.

Through to evidence readiness

Analysis does not end with a gap list, but with actions, accountable owners and evidence.

Service boundary: A.R.C. does not replace legal advice, statutory audit services or technical product installation unless explicitly agreed. Certification, regulatory recognition or complete freedom from risk are not guaranteed.

Next step: Clarify the decision required and the next reliable milestone.

A structured initial conversation clarifies the current situation, scope, available evidence and the right starting point: analysis, management decision, implementation leadership or audit readiness.

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