GRC Foundations

Governance Responsibilities Guide

Practical onboarding guide for junior GRC roles

Who this guide is for

- Junior GRC analysts and security governance coordinators
- New joiners in security, IT, risk, audit, or privacy roles
- Anyone needing clarity on ownership and decision paths

What you will be able to do

- Explain what Governance covers in a GRC model
- Know who approves what and when to escalate
- Run governance routines: meetings, reporting, and follow-up

Version 1

Contents

About risQera

risQera supports organizations with cybersecurity consulting across ISMS implementation, risk management, and compliance programs aligned with ISO/IEC 27001 and broader GRC practices.

Beyond Risk: turning requirements into decisions, actions, and audit-ready evidence.

What we deliver

- ISMS lifecycle support: design, implementation, operation, and continual improvement
- Risk management and assurance: methodology, registers, treatment planning, and reporting
- Integrated compliance: governance and reporting across security and GRC programs

How risQera can help

Core services	Typical outputs and evidence
ISMS implementation and improvement	• Gap assessment and implementation roadmap • Scope, context, and stakeholder requirements • Statement of Applicability and control implementation support • Audit readiness and corrective action follow-up
Risk management and assurance	• Risk methodology and assessment workshops • Treatment planning and decision support • Third-party and cloud risk support • Reporting aligned with governance needs
Training and enablement	• Templates and guidance to standardize evidence • Coaching for ISMS owners and process leads • Support for certification transitions and surveillance audits

Follow us for more GRC insights

LinkedIn: risQera

1. Purpose and audience

This document explains Governance in a Governance-Risk-Compliance (GRC) model. It is written for newcomers in security, IT, risk, audit, privacy, or compliance roles. The primary goal is to make responsibilities, decision paths, and ownership expectations easy to understand and apply. This is an informational guide that clarifies governance responsibilities and typical governance tasks. It is not a tool and it does not replace your organization's approved policies, standards, or procedures.

2. What Governance means in GRC

Governance is the part of GRC that sets direction, defines rules, and ensures accountability. It clarifies what the organization is trying to achieve, which principles apply, and who has authority to approve or reject decisions.

Governance in one sentence

Governance makes decisions possible by defining objectives, decision rights, and oversight mechanisms.

3. Outcomes Governance must deliver

1. Clear accountability: each control, risk decision, policy, and system has a named owner.
2. Consistent decisions: similar issues follow the same approval path every time.
3. Visible priorities: teams know what matters most and why.
4. Effective oversight: leadership can see progress, gaps, and blockers.
5. A repeatable operating model: onboarding is fast because responsibilities are documented.

4. Governance principles

- One accountable owner per decision. Others contribute, but one person remains accountable.
- Decisions are made at the right level. Routine items stay operational; material items escalate.
- Evidence follows the decision. Approvals, exceptions, and accepted risks are recorded.
- Policy is stable; standards evolve. Policies change rarely; standards adapt to technology and context.
- Governance supports delivery. It exists to enable action and accountability, not to create bureaucracy.

5. Governance structure

Governance typically uses a small number of bodies with clear scopes. The names vary by organization, but the intent remains the same: maintain oversight while keeping operations efficient.

5.1 Typical governance bodies

- Board or Senior Leadership: sets high level risk appetite and approves material risk acceptance and major investments.
- Executive Sponsor: ensures authority, resources, and executive visibility for GRC priorities.

- Security Steering Committee: reviews top risks, incidents, audit status, and roadmap decisions that affect multiple departments.
- Operational Security Meeting: tracks delivery, exceptions, remediation progress, and assigns actions.

5.2 Decision flow

- Operational decisions: handled in the operational security meeting.
- Cross-functional decisions: handled in the steering committee.
- Material risk or budget decisions: handled by the executive sponsor or senior leadership.

6. Roles and responsibilities

This section defines roles in plain language. In smaller organizations, one person may hold multiple roles. Even then, the responsibilities remain the same and must be explicitly assigned.

Executive Sponsor

- Ensures the GRC program has authority, resources, and visibility.
- Approves major priorities and escalated decisions.

CISO or Head of Security

- Defines the security governance approach, policy framework, and security roadmap.
- Ensures risk reporting and decision-making are structured and consistent.
- Owns escalation to executives.

GRC Lead or Security Governance Manager

- Runs governance processes: calendars, agendas, reporting, and follow-up actions.
- Maintains policy and standard lifecycles and ownership mappings.
- Maintains the central register for exceptions, approvals, and key decisions.

Risk Owner (business)

- Owns the impact if the risk occurs.
- Decides on treatment options when business trade-offs are required.
- Accepts residual risk within delegated authority.

Control Owner

- Ensures a control is defined, implemented, and operating effectively.
- Clarifies evidence expectations and testing readiness.

System Owner or Product Owner

- Accountable for security of a system or product in day-to-day operation.

- Implements required standards and coordinates remediation work.

Data Owner

- Sets rules for data classification, access, retention, and sharing.
- Approves sensitive data use cases and data-handling exceptions.

Audit and Compliance Liaison

- Coordinates external audit and customer assurance requests.
- Ensures evidence is available and aligns testing activities with governance cadence.

Next, use the RACI matrix on the next page to align local role names and confirm who approves key decisions.

7. Responsibilities at a glance (RACI)

The RACI table below helps newcomers understand who is Responsible (R), Accountable (A), Consulted (C), and Informed (I). Update the role names to match your organization. Note: A* indicates Authority and depends on the delegation model in Section 8.

RACI matrix

Activity	Exec Sponsor	CISO	GRC Lead	Risk Owner	Control Owner	System Owner	Audit/Compliance
Define security objectives	A	R	C	C	I	I	I
Define risk appetite and thresholds	A	R	C	C	I	I	I
Approve security policy	A	R	R	C	C	I	I
Maintain standards and baselines	I	A	R	C	R	R	C
Assign control ownership	I	A	R	C	R	C	I

Accept residual risk within authority	I	C	R	A	C	C	I
Accept material risk above authority	A	R	C	C	C	C	I
Approve exceptions and waivers	A	R	R	A	C	C	I
Steering committee reporting	A	R	R	C	C	I	C

7.1 What governance work looks like for a junior GRC analyst

If you are new to GRC, your governance contribution is mainly about clarity, cadence, and traceability. Your goal is to make ownership explicit, keep decisions recorded, and ensure follow-up actions close on time.

Cadence	What you do	Why it matters	Typical output
Daily / as needed	Triage governance questions, identify the right owner, and record approvals or decisions once made.	Questions and decisions must not stay informal. Traceability protects the organization.	Decision log updated; owner assigned; decision recorded with date and scope.
Weekly	Prepare the operational governance agenda, capture minutes, and follow up on assigned actions.	Governance only works when actions close and ownership stays explicit.	Agenda; minutes; action list with owners and due dates.
Monthly	Compile a short governance status pack: expiring waivers, overdue actions, policy review status, and key metrics.	Leadership needs a consistent view of what needs attention.	Steering pack draft; exceptions summary; KPI/KRI snapshot.
Quarterly	Coordinate policy or standard reviews, confirm owners are still correct, and support steering committee decisions.	Governance must stay current as the organization and technology evolve.	Review notes; updated ownership map; steering decisions recorded.

Before an audit or customer review	Compile governance evidence: policies list, meeting cadence proof, decision records, and action follow-up.	Audits often fail due to missing governance traceability rather than missing technical controls.	Evidence pack; decision log extracts; governance artifacts list.

7.2 What you do not approve as a junior

- Do not accept or reject risk on behalf of the business (you prepare the decision; the Risk Owner approves).
- Do not approve exceptions or waivers (you validate completeness and route for approval).
- Do not change security policy on your own (you coordinate reviews and document approvals).
- Do not commit to audit conclusions (you provide evidence and context; auditors conclude).

7.3 Definition of done for governance work

A governance task is done when the owner is named, the scope is clear, and the outcome is recorded.

- The decision or action has a named owner and a due date.
- The rationale and scope are captured (what, where, and for how long).
- Evidence or references are linked or stored in the agreed location.
- Any expiry date or review date is recorded for waivers and accepted risks.
- Stakeholders are informed according to the RACI (not everyone, only the right people).

8. Decision rights and approval rules

Newcomers often see delays because approval paths are unclear. A delegation model solves this by defining who can approve which type of decision. The tiers below are examples and should be adapted to your organization.

8.1 Delegation model (example)

- Tier 1 - Operational: low impact, limited scope, short duration. Approved by Control Owner and System Owner, recorded by GRC.
- Tier 2 - Significant: impacts customer commitments, sensitive data, or major systems. Approved by Risk Owner and CISO, visible to Steering.
- Tier 3 - Material: regulatory impact, high financial or reputational impact, or broad scope. Approved by Executive Sponsor or Senior Leadership.

8.2 What must always be documented

- Risk acceptance decisions: scope, duration, rationale, and approver.
- Exceptions and waivers: requirement, reason, compensating measures, expiry date, and review date.
- Steering decisions: decision, action owners, deadlines, and dependencies.

9. Governance artifacts

Governance runs on a small set of repeatable artifacts. Newcomers should know which ones exist, who owns them, and how they are maintained.

9.1 Policy hierarchy

- Policy: high-level mandatory rules that rarely change.
- Standard: measurable requirements that explain how policy is implemented.
- Procedure: step-by-step operational process.
- Guideline: recommended practices for consistency and quality.

9.2 Minimum set of governance artifacts

- Security policy framework (list of policies and owners).
- Standards and baselines (identity, logging, encryption, secure configuration, vendor security).
- Ownership map (systems, data, controls, and risks).
- Decision log (approvals, exceptions, and risk acceptances).
- Steering pack (KPIs, KRIs, top risks, audit status, and major initiatives).

10. Reporting and oversight

Reporting should help leadership make decisions quickly. A good governance report is short, consistent month to month, and focused on what needs attention.

10.1 What a good governance report includes

- Top risks: trend, treatment status, residual risk, and decision required.
- Control health: coverage, test results, and recurring gaps.
- Exceptions: count, aging, upcoming expiries, and compensating measures.
- Audit and customer assurance: open findings, owners, deadlines.
- Major initiatives: progress, blockers, and resource needs.

11. Escalation rules

Escalation protects the organization. It is expected when material impact is possible or when ownership and remediation are unclear.

- The issue impacts regulatory obligations or customer commitments.
- The issue affects sensitive data or critical systems.
- A control gap has no owner, no plan, or no realistic due date.
- A waiver would exceed the maximum duration defined by governance.
- There are signs of repeated non-conformance or systemic breakdown.

12. How a newcomer should operate in the first 30 days

Week 1: understand the landscape

- Confirm your role: control owner, system owner, contributor, reviewer, or coordinator.
- Request the ownership map and current top risks.

- Learn the governance calendar and meeting cadence.

Week 2: learn decision paths

- Understand how to request an exception and who approves it.
- Learn how actions are tracked and reported in your organization.

Week 3: know your evidence and responsibilities

- If you own a control, confirm the control description, expected evidence, and testing frequency.
- If you own a system, confirm required standards for identity, logging, patching, and configuration.

Week 4: contribute confidently

- Clarify one ownership gap, improve one metric, update one standard, or reduce one exception backlog item.
- Document the change so future newcomers benefit from the same clarity.

13. Glossary

Accountability: Being answerable for an outcome. One accountable owner per decision or control.

Control: A measure that modifies risk (administrative, technical, or physical).

Control owner: Accountable for the control definition, operation, and evidence.

Decision log: Record of decisions: what, who, when, rationale, actions, and due dates.

Decision rights: Rules stating who can approve what and when escalation applies.

Escalation: Raising an issue for a higher-level decision due to impact, urgency, or blockers.

Evidence: Proof that a control or process operates (approvals, tickets, reports, or logs).

Exception or waiver: Time-bound approval to deviate from a policy or standard, with conditions.

Governance: Direction, accountability, and oversight through defined roles, forums, and rules.

Metrics (KPI/KRI): KPIs track performance; KRIs signal rising risk exposure.

Policy: High-level mandatory rule approved by leadership.

Residual risk: Remaining risk after controls and treatments are applied.

Risk acceptance: Documented decision to keep residual risk within agreed limits and timeframe.

Risk appetite: Amount and type of risk leadership is willing to accept.

Risk owner: Business owner accountable for impact and for deciding treatment or acceptance.

Standard: Mandatory, measurable requirements that implement a policy consistently.

Steering committee: Leadership forum that reviews risks, priorities, and progress and resolves cross-functional issues.

System owner: Accountable for a system or product and its compliance with required security standards.