

GRC Interview & Study Guide

Governance & Policy

Prepared by **Naresh Thalla Mudhiraj** · thallanaresh.com

Personal learning project. Views are my own and do not represent any employer.

Basic to Advanced · scenario-based questions · practical examples · why each topic matters

Version 2.0 · generated 21 October 2026

How security and risk are directed, overseen and documented — boards, committees, policies and accountability.

Study material written in plain language. Framework and regulatory details change; always confirm against the official, current publication before relying on them.

Governance & Policy

How security and risk are directed, overseen and documented — boards, committees, policies and accountability.

Q: What is IT / information security governance?

Basic

Information security governance is the system by which an organisation's security activities are directed and controlled. It makes sure security supports business objectives, risks are managed to an acceptable level and resources are used responsibly.

Typical elements:

- Clear roles and accountability (board, executive sponsor, CISO, risk owners).
- Approved strategy, policies and risk appetite.
- Committees and reporting lines (e.g. a security or risk steering committee).
- Performance measurement and independent assurance.

Frameworks such as COBIT 2019, ISO/IEC 27014 and the Govern function of NIST CSF 2.0 describe governance practices.

Practical example: A CISO presents a quarterly cyber dashboard to the executive committee, which approves the security strategy and budget and decides which top risks to fund. That decision-making and oversight loop is security governance.

Why this matters: Without governance, security becomes a collection of tools with no clear priorities or ownership. Governance turns it into a managed business function.

Q: What is the role of the board in cyber risk?

Basic

The board does not manage security day to day, but it is accountable for oversight. Its role includes:

- Setting or approving risk appetite and strategic priorities.
- Making sure there are adequate resources and clear accountability (e.g. a CISO with access to leadership).
- Receiving regular, business-focused reporting on top risks, incidents and programme progress.
- Challenging management and seeking independent assurance (internal audit, external assessments).
- Understanding regulatory obligations and the organisation's crisis response.

Practical example: A board approves the cyber risk appetite statement, asks the CISO why critical-patch SLAs slipped last quarter, and requests a tabletop exercise for directors. That is oversight, not hands-on management.

Why this matters: Regulators globally increasingly expect boards to demonstrate cyber oversight. GRC teams prepare the reporting that makes this possible.

Q: Why is security awareness training a governance topic and not just an HR one?

Basic

People are both a major source of risk (phishing, mistakes, misuse) and a key control. Governance makes sure:

- Training is mandatory and role-based (e.g. developers, finance, privileged admins).
- Completion and effectiveness are measured (completion rates, phishing simulation trends).
- Policies are acknowledged and consequences for non-compliance are clear.

Most frameworks (ISO 27001, NIST, HIPAA, PCI DSS, SOC 2) include awareness and training requirements.

Practical example: After phishing simulations show a 15% click rate in finance, the executive committee makes awareness completion a manager KPI and links it to performance reviews. The training becomes accountable at leadership level rather than an HR tick-box.

Why this matters: Training is one of the most cost-effective controls, and it is a near-universal compliance requirement.

Q: What is an information security policy framework (policy hierarchy)?

Basic

A policy framework is the structured set of documents that direct security, from high-level intent down to daily steps:

- **Top level:** an information security policy approved by leadership, stating objectives, scope and commitment (ISO 27001 clause 5.2).
- **Topic-specific policies:** access control, acceptable use, cryptography, supplier security, incident management, and so on (ISO 27001:2022 control 5.1).
- Standards, procedures and guidelines underneath them.
- **Supporting elements:** document control (owner, version, review date, approval), a policy library and acknowledgement tracking.

Practical example: A company replaces a 90-page 'security manual' with a 3-page top-level policy, 14 topic-specific policies of 2–4 pages each and separate technical standards. Annual review becomes much faster and staff actually read them.

Why this matters: A clear hierarchy keeps policies short and stable while the detailed standards change more often. Auditors also expect to see document control and approval.

Q: What are the typical roles in security governance (CISO, DPO, risk owner, control owner, asset owner)?

Basic

- **CISO:** leads the security programme, advises leadership and reports on cyber risk.
- **DPO (Data Protection Officer):** independent adviser on privacy law compliance, required in some cases under GDPR and similar laws.
- **Risk owner:** the business leader accountable for a risk and its treatment decisions.
- **Control owner:** the person responsible for operating a control and providing evidence.
- **Asset or information owner:** decides classification and who may access the asset.
- **Internal audit:** provides independent assurance to the audit committee.

Practical example: The HR director owns the employee-data risk, the IAM lead owns the access-review control, and the HR system owner approves who gets access. The CISO reports the combined picture to the risk committee.

Why this matters: Many governance failures are role confusion: IT 'owns' every risk, or no one owns a control. Clear roles make accountability real.

Q: Why do policies need an owner, review cycle and version control?

Basic

- **Owner:** someone accountable for keeping the policy accurate and answering questions about it.

- **Review cycle:** usually at least annually and after significant changes (new regulation, major incident, reorganisation), as ISO 27001 expects.
- **Version control:** a change history, approver, effective date and a single published version so staff never follow an old copy.
- **Communication:** staff must be told about material changes and, for key policies, acknowledge them.

Practical example: An auditor finds the incident response policy still names a CISO who left two years ago and a phone number that no longer works. With an owner and an annual review in place, this would have been caught.

Why this matters: Out-of-date or unowned policies are an easy audit finding and, worse, they mislead staff about what is actually required.

Q: How would you develop or update an information security policy?

Intermediate

1. **Understand drivers:** business objectives, risk assessment results, laws, regulations, contracts and frameworks (e.g. ISO 27001, NIST, HIPAA).
2. Benchmark existing documents and identify gaps or overlaps.
3. Draft in clear, concise language — say what is required and who is responsible, not how every tool is configured.
4. Consult stakeholders (IT, legal, HR, privacy, business units) so the policy is realistic.
5. Get formal approval from the right authority (e.g. executive leadership or a governance committee).
6. Communicate and train; make it easy to find.
7. Define exceptions, enforcement and review cycle (commonly at least annually or after significant change).
8. Map the policy to control frameworks so it can be evidenced in audits.

Practical example: When updating an acceptable-use policy to cover generative AI tools, you gather input from legal, HR and IT, map it to ISO 27001 Annex A 5.10, publish it after leadership approval, run awareness sessions and track staff acknowledgement.

Why this matters: Policies are the authority for every control. A well-built policy gets adopted; a copied template gets ignored and fails audits.

Q: How do you handle policy exceptions?

Intermediate

A policy exception process allows justified, temporary deviations without losing control:

- Formal request explaining the business reason, scope and duration.
- Risk assessment of the deviation and any compensating controls.
- Approval by the risk owner at an authority level that matches the risk.
- Recorded in an exception register with an expiry date.
- Periodic review; renewal requires re-justification.

A large number of exceptions against one policy is a signal the policy or standard may need to change.

Practical example: A lab instrument runs an unsupported OS that cannot be patched. The exception is approved for 12 months with compensating controls (network isolation, no internet, monitoring), signed by the business owner and reviewed by the CISO before renewal.

Why this matters: Exceptions are inevitable. Managing them transparently keeps risk visible and prevents 'shadow' non-compliance.

Q: What is a RACI matrix and how is it used in GRC?

Intermediate

RACI defines roles for each activity or control:

- **Responsible:** does the work.
- **Accountable:** owns the outcome and signs off (only one person).
- **Consulted:** gives input before decisions.
- **Informed:** kept up to date.

In GRC, RACIs are used for control ownership, policy maintenance, risk acceptance, incident response and audit preparation.

Practical example: For quarterly user access reviews: the application owner is Accountable, team managers are Responsible for reviewing, the IAM team is Consulted on revocations, and GRC is Informed of completion for evidence.

Why this matters: Many audit findings come from unclear ownership. A RACI makes accountability explicit and evidence easier to collect.

Q: What makes a good governance committee for security and risk?

Intermediate

- **A clear charter:** purpose, authority, membership, quorum and frequency.
- **Cross-functional membership:** IT, security, risk, legal, privacy, compliance, business leaders.
- Decision-making authority (e.g. approving policies, accepting risks above a threshold, prioritising investment).
- **Good inputs:** risk dashboards, KRIs, audit findings, incident trends, project status.
- Minutes and action tracking so decisions are evidenced.
- Escalation path to the executive team or board.

Practical example: A monthly Security & Risk Steering Committee with a written charter, the CIO as chair, business-unit heads as voting members, a set quorum, a standing agenda (top risks, exceptions, audit status) and minutes with action owners.

Why this matters: Committees are where governance actually happens. Auditors often ask for minutes as evidence that risks are overseen.

Q: How do you write a risk appetite statement for cyber risk?

Intermediate

A good cyber risk appetite statement connects the board's attitude to risk with measurable limits:

- Start with qualitative statements by risk category, such as 'We have a very low appetite for risks that could compromise patient safety or the confidentiality of health data.'
- Add measurable tolerances (KRIs with thresholds), such as 'no critical internet-facing vulnerability open longer than 7 days'.
- **Define escalation:** what happens when a tolerance is breached, and who is told.
- Have it approved by the board and reviewed at least annually.

Different categories can have different appetites. Innovation may be moderate while regulatory compliance is very low.

Practical example: 'Low appetite for loss of service availability for clinical systems: tolerance is no more than 4 hours of unplanned downtime per quarter for the EHR, and any breach is reported to the risk committee within 5 working days.'

Why this matters: Without an appetite statement, every risk decision is subjective and the board cannot see whether management is operating within agreed limits.

Q: What should a security strategy and roadmap contain?

Intermediate

- **Business context:** the strategy, growth plans, regulatory landscape and threats.
- Current state vs target state, often measured with a framework such as NIST CSF 2.0 profiles.
- Prioritised initiatives that close the biggest risk gaps, each with an owner, cost, timeline and expected risk reduction.
- A 12–36 month roadmap with quick wins and longer programmes.
- **Governance:** how progress is measured (KPIs/KRIs) and reported, and when the strategy is revisited.

Practical example: Because the company plans to sell into hospitals in a new country next year, the roadmap prioritises ISO 27001 certification, data localisation in an in-country cloud region and alignment with the local health-data security standard ahead of less urgent tooling upgrades.

Why this matters: A strategy linked to business goals is what gets funded. A list of tools is not a strategy.

Q: How do you measure whether a security policy is actually followed?

Intermediate

- **Technical enforcement data:** for example, the percentage of devices compliant with the encryption standard, read from the MDM tool.
- Control testing and internal audit results.
- **Exceptions register:** many or long-running exceptions suggest the policy is unrealistic.
- Incidents and near-misses linked to policy breaches.
- Acknowledgement and training completion. These are necessary but weak signals on their own.
- Spot checks and staff interviews during audits.

Practical example: The policy requires screen locks after 10 minutes. MDM data shows 22% of Mac laptops are non-compliant because a configuration profile was never deployed. The fix is technical, not another awareness email.

Why this matters: A policy that is published but not followed creates false assurance and legal exposure, because it shows you knew what should happen.

Q: What is the role of internal audit versus the GRC (second-line) function?

Intermediate

- The GRC/second line designs the risk and control framework, advises the business, monitors compliance and reports on risk. It is part of management.
- Internal audit (third line) gives independent, objective assurance to the board/audit committee that governance, risk management and controls work, including over the GRC function itself.
- Internal audit should not design or operate the controls it audits, to protect independence.
- The two coordinate (shared risk taxonomy, combined assurance maps) but do not merge.

Practical example: The GRC team runs quarterly access-review monitoring. Internal audit separately tests a sample in its annual audit and also assesses whether GRC's monitoring is reliable, then reports to the audit committee.

Why this matters: Blurring the lines weakens independence, and auditors and regulators will challenge it.

Q: The business wants a policy exception that has already been renewed three times. What do you do?

Intermediate · Scenario

- **Treat repeated renewals as a signal:** either the policy is unrealistic, or the risk is being permanently accepted without proper visibility.
- Re-assess the current risk and whether compensating controls still work.
- Ask for a remediation plan with funding. If there is none, convert the exception into a formal risk acceptance at the right authority level.
- Consider whether the policy or standard needs updating for this use case.
- Report long-running exceptions as a metric to the governance committee.

Practical example: A legacy radiology system has been on exception for 3 years. You present it to the risk committee with the options: fund a replacement (cost estimate attached) or formally accept the risk at COO level with yearly review. The committee funds the replacement in next year's budget.

Why this matters: Exceptions are meant to be temporary. A permanent exception hidden in a register is unmanaged risk.

Q: You are asked to write an AI acceptable-use policy in two weeks. How do you approach it?

Intermediate · Scenario

1. Find out how AI is already used (survey, proxy logs, SaaS discovery) and what the business wants to do with it.
2. Bring in legal, privacy, HR, IT and a business representative early.
3. **Keep it short and practical:** approved tools, prohibited uses, what data can never be entered (patient data, customer PII, source code, secrets), human review of outputs, and how to request a new tool.
4. Align with existing policies (acceptable use, data classification, privacy) and with references such as ISO/IEC 42001 and the NIST AI RMF.
5. Get leadership approval, communicate with examples and plan an early review, because AI changes fast.

Practical example: The policy allows the company's licensed enterprise AI assistant for drafting and summarising internal documents, prohibits pasting patient or customer data into any public AI tool, and requires a human check before AI-generated content is sent to customers.

Why this matters: An imperfect policy published quickly and improved later is better than staff using AI with no guidance at all.

Q: Staff keep failing phishing simulations in one department, and its head says training is a waste of time. How do you handle it?

Intermediate · Scenario

- **Look at the data first:** which emails were clicked, which roles, and whether credentials were actually entered or reported.
- Meet the department head and present the risk in their terms. For example, finance staff with payment authority are prime targets for BEC.
- **Change the approach, not just the volume:** short role-specific sessions, just-in-time feedback after a click, and recognition for reporting suspicious emails.
- Strengthen technical controls so one click does less damage (phishing-resistant MFA, link rewriting, attachment sandboxing).

- If engagement stays low, report the department's KRI to the governance committee. Leadership accountability is a governance matter.

Practical example: After two months of tailored 10-minute sessions and a 'report phish' button, the department's report rate rises from 10% to 45% and credential submissions drop sharply. The department head now presents the improvement at the leadership meeting.

Why this matters: Awareness is a shared responsibility. Engaging leaders and combining training with technical controls works better than blaming users.

Q: What is COBIT and how does it differ from ISO 27001?

Advanced

COBIT (currently COBIT 2019, from ISACA) is a framework for the governance and management of enterprise information and technology. It separates governance objectives (Evaluate, Direct and Monitor) from management objectives and helps align IT with business goals.

ISO/IEC 27001 is a certifiable standard for an Information Security Management System (ISMS) focused specifically on information security risk.

- **Scope:** COBIT covers all of enterprise IT; ISO 27001 focuses on information security.
- **Use:** COBIT is often used for IT governance and IT audit; ISO 27001 for building and certifying a security management system.
- They are complementary and are often mapped to each other.

Practical example: A bank uses COBIT to structure how IT overall is governed and how value is delivered, and ISO 27001 to run its ISMS, so the information security objectives feed into COBIT's governance objectives.

Why this matters: Senior roles expect you to know which framework fits which problem rather than treating them as interchangeable.

Q: How do you set up governance for third-party, AI and data under one model without creating committee overload?

Advanced

- **Map decision rights first:** which decisions need committee approval and which can be delegated.
- Use one main risk committee with clear terms of reference, and specialist working groups (AI, data, vendors) that report into it rather than separate decision-making committees.
- **Share common tools:** one risk taxonomy, one register, one exception process.
- Set thresholds for escalation (for example, high-risk AI use cases or Tier 1 vendors go to the committee; others are approved by the working group).
- Review the model annually and close committees that no longer add value.

Practical example: Instead of creating a new AI Board, the company adds an AI working group under the existing Risk Committee. It approves low and medium-risk AI use cases itself and escalates high-risk ones, such as AI in clinical triage, with a standard paper template.

Why this matters: Too many committees cause slow decisions, duplicated papers and gaps between them. A clear decision-rights model keeps governance effective.

Q: How do emerging regulations such as the EU AI Act, DORA and NIS2 change governance expectations?

Advanced

The common theme is that management bodies are personally expected to understand and oversee cyber and technology risk:

- NIS2 (EU) requires management bodies of covered entities to approve and oversee cybersecurity risk-management measures and to undergo training, with possible liability for failures.
- DORA (EU financial sector, applicable from January 2025) puts ultimate responsibility for ICT risk management on the management body and requires ICT third-party risk oversight.
- The EU AI Act sets obligations based on AI risk categories, which pushes organisations to inventory and classify their AI systems and to assign accountability.

Governance therefore needs board training, clear accountability, documented approvals and evidence that oversight actually happened.

Practical example: A fintech outside the EU with EU clients is asked by a European bank customer to evidence DORA-aligned controls: ICT incident classification, exit plans for critical suppliers and board-approved ICT risk policies.

Why this matters: Even outside the EU, these laws influence customers, group policies and local regulators. Interviewers in multinational firms expect awareness of the direction of travel.

Q: Two senior leaders both claim ownership of a critical risk, and neither will accept the other's treatment plan. How do you resolve it?

Advanced - Scenario

- Clarify the risk definition first. Often two people are describing different risks that should be split.
- **Apply the ownership rule:** the owner is the person accountable for the business objective or process most affected and who controls the budget to treat it.
- **Facilitate a joint session with the facts:** impact, options, cost and timelines.
- If still unresolved, escalate to the risk committee or their common manager to assign ownership. That is what governance is for.
- Record the decision and the rationale in the register.

Practical example: The CIO and the COO both claim 'EHR downtime'. The risk is split into 'technical failure of EHR infrastructure' (CIO) and 'inability to deliver care during downtime' (COO, who owns downtime procedures). The committee approves the split.

Why this matters: A risk with two owners has no owner. GRC's job is to make accountability clear, not to pick sides.

Q: The board asks 'Are we secure?' How do you answer?

Advanced - Scenario

- Do not answer yes or no. No organisation is fully secure; the honest question is whether risk is within appetite.
- **Give a short structured answer:** our top risks, where we are within or outside appetite, what has improved, what is still exposed and what we are doing about it.
- **Back it with evidence:** independent assessments, KRIs, test results (for example ransomware recovery tests).
- End with any decision you need from them.

Practical example: 'Our biggest exposures are ransomware and third-party access. Ransomware resilience improved after a successful full restore test in September. Third-party access is still outside appetite: 8 vendors have standing remote access without MFA. We will close this by Q1, and we need your support for the vendor contract changes.'

Why this matters: Boards need an informed view of risk, not reassurance. A balanced answer builds trust and gets better decisions.

Q: Your company is acquired by a larger group with its own security policies. What governance steps do you take in the first months?

Advanced · Scenario

1. **Confirm the integration plan and decision rights:** which group policies apply immediately, which local ones remain, and who approves exceptions.
2. Compare the two policy frameworks and control sets (gap analysis), focusing on regulatory obligations that apply only locally, such as local data localisation rules or HIPAA.
3. Merge the risk registers using the group's taxonomy and scoring, and re-rate the top risks.
4. Agree interim controls for network and identity connections between the two companies.
5. Keep certifications valid during the transition. Tell the certification body about significant changes to scope.
6. Communicate clearly to staff which rules apply from which date.

Practical example: After the acquisition the group's access-control policy is adopted within 90 days, but the local ISO 27001 certificate is kept until the group certificate scope is extended. The certification body is informed of the change in ownership in writing.

Why this matters: Mergers are a high-risk period: controls lapse, duplicate processes confuse staff, and attackers know it. Clear governance keeps compliance intact.