Cyber Security GRC Specialist interview questions

careertips.com.au: common questions and what they're really testing

What to expect

Interviews for cyber security GRC specialist roles typically focus on your ability to interpret frameworks, manage risk and communicate with stakeholders. You may be asked to walk through your approach to a risk assessment, explain how you have handled resistance to a control, or respond to a scenario where a business unit wants to bypass a security requirement.

- **Process:** How you conduct a risk assessment, compliance review or audit coordination.
- **Behavioural:** A time you influenced stakeholders, managed an audit finding or handled a difficult conversation.
- **Scenario:** A business unit wants to bypass a control, or a new regulation creates competing priorities.
- **Technical:** Knowledge of specific frameworks such as the Essential Eight, ISM or ISO 27001.
- **Regulatory:** How you interpret and apply new obligations or changes to legislation.
- **Client-facing:** Explaining a complex risk to a non-technical audience or senior executive.

The process often starts with a phone screen with a recruiter, followed by a technical and competency interview with the hiring manager and possibly a peer. Some organisations include a case study or a walkthrough of a framework you have implemented. Final interviews may involve senior stakeholders such as the CISO or a risk committee member.

1. Can you walk me through your approach to conducting a risk assessment for a new system or process?

Why they ask

Assesses your methodology and understanding of risk frameworks.

How to structure your answer

Use a step-by-step walkthrough: scope, identify assets and threats, assess likelihood and impact, evaluate existing controls, determine residual risk, and document in a risk register. Mention how you engage stakeholders and prioritise actions.

Example answer

“First, I clarify the scope with the system owner and identify the information assets involved. Then I map threats and vulnerabilities using the ISM and relevant regulatory obligations. I assess likelihood and impact, often with a workshop, and evaluate the effectiveness of existing controls. I calculate residual risk, document it in the risk register, and propose treatment options. I always validate findings with the business and set a review date.”

2. Tell me about a time you had to influence a business unit to adopt a security control they were resisting.

Why they ask

Tests stakeholder management and your ability to balance security with business needs.

How to structure your answer

Use STAR: Situation, Task, Action, Result. Focus on how you understood their concerns, presented risk in business terms, and negotiated a workable solution.

Example answer

“A marketing team wanted to use a new cloud tool without going through security review. I met with them to understand their deadline and explained the risks in terms of data privacy and potential regulatory breaches under the Privacy Act. I offered a fast-track assessment that focused on the critical controls, and we agreed on a conditional approval with a 30-day review. They met their deadline, and we maintained compliance.”

3. How do you stay current with changes to frameworks like the Essential Eight or the ISM?

Why they ask

Shows commitment to professional development and regulatory awareness.

How to structure your answer

Describe your sources: ASD alerts, industry newsletters, professional networks, training. Give an example of how you applied a recent update.

Example answer

“I subscribe to ASD notifications and follow updates from the ACSC. I also participate in a local ISACA chapter and read analysis from legal firms. When the Essential Eight maturity model was updated, I reviewed our assessment approach and ran a gap analysis, then briefed the security team on the changes and adjusted our remediation roadmap.”

4. Imagine a senior manager asks you to approve a policy exception that would leave a critical system non-compliant. What do you do?

Why they ask

Scenario question testing judgement, integrity and communication under pressure.

How to structure your answer

Acknowledge the request, clarify the risk, explore alternatives, escalate if necessary, and document the decision. Show you can say no while maintaining relationships.

Example answer

“I would thank them for raising it and ask for the business context. I would explain the specific compliance gap and the potential consequences, such as regulatory penalties or data loss. I would explore compensating controls or a temporary risk acceptance with a clear expiry. If it still left unacceptable risk, I would escalate to the CISO or risk committee and document the advice. My goal is to find a safe path, not just block.”

5. How do you coordinate an external audit or certification activity?

Why they ask

Assesses project management, attention to detail and audit experience.

How to structure your answer

Outline the phases: planning, evidence gathering, auditor liaison, findings management, and corrective actions. Mention how you keep stakeholders informed.

Example answer

“I start by confirming the audit scope and criteria with the auditor. Then I build a project plan, assign evidence owners, and set up a shared repository. During fieldwork, I act as the main point of contact, clarifying requests and tracking progress. After the audit, I manage findings through to closure, ensuring corrective actions are implemented and verified. I also run a lessons-learned session to improve next time.”

6. How would you explain a complex security risk to a non-technical executive?

Why they ask

Tests communication skills and ability to influence at senior levels.

How to structure your answer

Focus on clarity, relevance and outcomes. Avoid jargon, use analogies, link to business objectives and regulatory obligations.

Example answer

“I would start with the business impact: what could happen, how likely it is, and what it means for customers or compliance. I would use a simple analogy, like comparing a missing control to leaving a door unlocked. I would then present options with clear trade-offs and recommend a course of action. Finally, I would check understanding and offer to provide more detail if needed.”