Junior Cyber Security Consultant

Type: Permanent
Location: Sydney (Hybrid)
Salary: $65,000 – 75,000 + super + salary packaging (commensurate with experience)

About the Role

This is a junior consulting role supporting cyber security assessments, project coordination, and client relationship management for Not-for-Profit organisations across Australia.

The role suits someone early in their cyber career who enjoys learning quickly, working with people, and translating security concepts into practical, achievable actions for resource-constrained environments. You'll gain exposure to real-world cyber security challenges across a diverse NFP client base, while developing strong consulting, communication, and delivery skills.

Role Overview

Reporting to the Cyber Security Lead, you'll support the end-to-end delivery of cyber security engagements. This includes planning and coordinating client work, supporting assessments and reviews, documenting findings, developing recommendations, and tracking remediation actions.

You'll be hands-on across risk and vulnerability assessment, governance and policy uplift, incident readiness, security awareness training, and stakeholder engagement. As the cyber function grows, you'll also contribute to improving delivery processes, templates, and consistency.

This role does not require deep engineering or SOC experience, but it does require comfort working with technical evidence, controls, and system information with guidance from senior team members.

Key Responsibilities

1. Client Cyber Security Assessments

- Support and/or conduct vulnerability assessments and risk analyses for client environments
- Assist with cyber security assessments, including evidence collection and review
- Help translate assessment outcomes into clear, prioritised recommendations and uplift roadmaps

2. Policy, Procedure and Governance Uplift

- Assist in drafting and improving security policies, standards, procedures, and best-practice guidance

- Support governance and control reviews, uplift planning, and remediation/action tracking
- Assist with mapping controls and practices to recognised frameworks (e.g. Essential Eight, NIST, ISO 27001)

3. Incident Response Readiness

- Assist clients to develop and review incident response plans and supporting documentation
- Support basic tabletop exercises and capture outcomes, lessons learned, and improvement actions

4. Security Awareness Training

- Collaborate with clients to design and deliver cyber security training for staff
- Manage WorkVentures' cyber security training platform, including phishing simulations and training modules
- Monitor participation and effectiveness, and support continuous improvement

5. Technology Evaluation and Security Support

- Support evaluation of security tools and software appropriate to client needs and budgets
- Assist with reviewing findings and identifying practical remediation strategies for vulnerabilities and gaps

6. Reporting and Communication

- Prepare clear, client-ready reports and presentations covering risks, vulnerabilities, and recommendations
- Communicate technical concepts to non-technical stakeholders in a practical, actionable way

7. Project Coordination and Delivery Support

- Coordinate and schedule assessments, workshops, and client engagements
- Use **Asana** to manage tasks, timelines, dependencies, and follow-ups across multiple concurrent projects
- Maintain timelines, track deliverables, and manage task lists across engagements
- Prepare and maintain project documentation (risk registers, action plans, progress updates, meeting notes)
- Track compliance requirements and document outcomes during client reviews

- Support basic effort and budget tracking where required

8. Client Relationship and Stakeholder Engagement

- Act as a day-to-day point of contact to support smooth client communication
- Facilitate meetings and workshops to understand client needs and present updates and findings
- Respond to client queries and escalate issues to senior or technical team members as needed

9. Process Improvement

- Identify inefficiencies in delivery processes and recommend improvements
- Build and maintain templates, guides, and checklists to strengthen quality and consistency
- Contribute inputs to grant and sector reporting by providing delivery evidence, impact data, and case examples from client engagements as required

What Success Looks Like

In your first 6–12 months, success in this role looks like:

- Supporting multiple client engagements with increasing confidence and independence
- Producing clear, accurate assessment documentation and client-ready reports
- Building trusted relationships with Not-for-Profit clients
- Demonstrating strong follow-through on actions, timelines, and reporting
- Growing confidence mapping controls to frameworks and explaining gaps clearly
- Receiving positive client feedback through satisfaction surveys, testimonials, or direct stakeholder feedback

Qualifications and Experience

- 1–3 years' experience in cyber security, information security, IT risk/GRC, IT support, or project coordination
  (or equivalent capability demonstrated through study, placements, or certifications)
- Experience supporting client-facing work and stakeholder engagement
- Strong written and verbal communication skills, including report writing

- Familiarity with cyber security frameworks and compliance practices (e.g. NIST, ISO 27001, Essential Eight)
- Strong organisational skills, with demonstrated experience managing tasks, timelines, and priorities using project or task management tools (e.g. Asana or similar)

What You Bring

You bring a curious, practical mindset and a willingness to learn. You communicate clearly, build trust with stakeholders, and translate cyber security concepts into simple, usable guidance—particularly for Not-for-Profit organisations supporting vulnerable communities.

You are highly organised, comfortable working in structured task management tools, and reliable in following through actions and deadlines. You take pride in high-quality client outcomes and value clear communication and follow-through.

Desirable

- Interest in counter-surveillance technologies and approaches to combat Technology-Facilitated Abuse (TFA)
- Entry-level cyber security certifications (e.g. Security+, Cert IV Cyber Security, or similar)