Cyber Security GRC Analyst

Cyber Security GRC Analyst

We are looking for a capable Cyber Security Governance, Risk & Compliance (GRC) Analyst, who enjoys security work and possesses a solid depth and breadth of expertise in the information security space. Join our growing team and become part of a Canberra success story.

In this full time role you will evaluate and manage the processes and controls required by the Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM).

Responsibilities

- Identify and define system security requirements
- Review and improve system security architecture and develop detailed security designs
- Prepare and document security policies, plans, and procedures as required by relevant security governance frameworks
- Assess, monitor and report security measures for the protection of computer systems, networks and information
- Engage with executive and technical stakeholders
- Write comprehensive reports including assessment-based findings, outcomes and propositions for further system security enhancement

Requirements

- Demonstrated knowledge of the processes and controls required by the Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM)
- Proven working experience in developing security policies, risk management plans, system security plans, statements of applicability and security procedures
- Knowledge of contemporary and emerging information security issues and threats
- Knowledge of network, operating system and application security
- Knowledge of security systems, including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, etc
- Understanding of the latest security principles, techniques, and protocols
- Understanding of web related technologies (Web applications, Web Services, Service Oriented Architectures) and of network/web related protocols
- Awareness of security management systems such as ISO/IEC 27001 and PCI DSS
- Problem solving skills and ability to work under pressure
- Bachelor degree in Information Systems, Computer Science or related field
- Australian citizen able to receive government security clearance

Self improvement

The cyber security field is highly dynamic and requires committed professionals who seek to continually learn and improve. Ionize recognises the importance of self-improvement and invests heavily in its people so they can be the best in their respective disciplines. As such, the successful candidate is expected to complete the $(ISC)^2$ CISSP exam within six months of starting, and ISACA CRISC exam six months

after that. Study materials will be provided and reasonable study leave will be approved during each period the candidate is pursuing each certification. Future education requirements will be guided by the successful candidate's domain specialisation.

Workplace Culture

Ionize is an equal opportunity employer seeking representation from all areas of the community. We believe a diverse set of people with varied perspectives give us a significant advantage and a great place to work!

Application Process

If you want to be a part of a team working in a challenging and rewarding environment apply now by emailing your CV and an introduction of yourself to careers@ionize.com.au quoting reference GRC0516. Salary is negotiable based on skill and expertise.

Please note, due to the nature of this work, eligibility to obtain an Australian security clearance is mandatory.

Disclaimer: Ionize does not accept unsolicited agency resumes. Ionize is not responsible for any fees related to unsolicited resumes.