



## IS Auditor/Security Engineer I

<b>Department:</b> Security & Risk Management	<b>Reports To:</b> Director, Security & Risk Management
---	---

### Basic Functions

Under general supervision, perform internal IT related audits, provide internal security consulting, assist with monitoring corrective action plans, perform daily review of operational and security logs. Assist in the preparation of draft reports, maintain work papers. Keep management informed of work activities by providing weekly status reports and/or attending status update meetings.

### Responsibilities:

- Daily; review logs and alerts generated from IT security infrastructure such as network firewalls, web application firewalls (WAF), intrusion prevention systems (IPS), user authentication systems, Internet filters, vulnerability scanning systems, email systems, network devices, etc and identify any potential relevant security issues.
- Investigate security issues and resolve in accordance with company policy. Document all activities in a tracking system.
- Under general supervision of the Director, conduct scheduled Information Technology audits including collecting audit evidence, evaluating internal controls, performing audit tests, communicating results, completing audit tests, work papers and audit reports.
- Develop an in-depth knowledge of company business and processes and build and maintain positive working relationships.
- Maintain professional and technical knowledge by attending educational workshops, reviewing professional publications, establishing personal networks and participating in professional societies.
- Construct and/or evaluate compensating controls based on business requirements.
- Other appropriate duties as assigned.

### Skills/Requirements

- As a professional who will have wide access to confidential and proprietary information, integrity is expected at all times.
- Familiarity with the following concepts or technologies: access controls, application development security, business continuity and disaster recovery, cryptography, risk management, information security governance, computer investigations, IT operations security, physical security, security architecture and design, telecommunications and network security.
- Adhere to *"ISACA Standards, Guidelines, Tools and Techniques for Audit, Assurance and Control Professionals"* as well as company standards and policies.
- Familiarity with the following security frameworks: PCI DSS, ISO/IEC 27001/27002.
- Excellent communication skills with the ability to write business communications in a clear and concise manner.
- Analytic ability to identify issues and arrive at appropriate solutions.

### Working Conditions:

Common office environment requiring extensive sitting and use of computers for up to 8 hours per day operating common office machines including keyboard/mouse, copying machines, faxes, etc. Travel is not anticipated for this position.

### Education and Training:

- Undergraduate degree from an accredited College or University in a relevant subject area. Verifiable job experience, 1 – 3 years, may be accepted in lieu of a degree.
- Highly desirable: Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified in the Governance of Enterprise IT (CGEIT).