Information Security Manager Job Description Template

As per National Information Assurance Policy v2.0

Job Title	Information Security Manager
Department	
Reports to	CEO / Head of Risk / Head of Audit

Job Description

The ISM is responsible for establishing and maintaining a corporate wide information security management program to ensure that information assets are adequately protected. This position is responsible for identifying, evaluating and reporting on information security risks in a manner that meets compliance and regulatory requirements, and aligns with and supports the risk posture of the enterprise.

The ISM position requires a visionary leader with sound knowledge of business management and a working knowledge of information security technologies. The ISM will proactively work with business units to implement practices that meet defined policies and standards for information security. He or she will also oversee a variety of IT-related risk management activities.

The ISM serves as the process owner of all assurance activities related to the availability, integrity and confidentiality of customer, business partner, employee and business information in compliance with the organization's information security policies. A key element of the ISM's role is working with executive management to determine acceptable levels of risk for the organization. The ISM must be highly knowledgeable about the business environment and ensure that information systems are maintained in a fully functional, secure mode.

The ISM's role is to act as an interface between the Management's strategic and process-based activities and the work of the technology-focused analysts, engineers and administrators in the IT organization. The ISM must be able to translate the IT-risk requirements and constraints of the business into technical control requirements and specifications, as well as report on ongoing performance. The ISM coordinates the IT organization's technical activities to implement and manage security infrastructure, and to provide regular status and service-level reports to management.

The ideal candidate is a thought leader, a consensus builder, and an integrator of people and processes. While the ISM is the leader of the security program, he or she must also be able to coordinate disparate drivers, constraints and personalities, while maintaining objectivity and a strong understanding that security is just one of the business's activities. It cannot be undertaken at the expense of the enterprise's ability to deliver on its goals and objectives.

Expertise in leading project teams and developing and managing projects is essential for success in this role. The ISM must be able to prioritize work efforts — balancing operational tasks with longer-term strategic security efforts. Other project management tasks will include resource balancing across multiple IT and security teams, task prioritizing and project reporting. Vendor relationship management — ensuring that service levels and vendor obligations are met — is also an important aspect of the position.

ISMs are responsible for managing highly technical staff as they work to accomplish company and personal development goals and must, therefore, have proven leadership skills. Documentation and presentation skills, analytical and critical thinking skills, and the ability to identify needs and take initiative are key requirements of the ISM's position.

Roles and Responsibilities

The ISM's job is composed of a variety of activities, including very tactical, operational and strategic activities in support of the ISM's program initiatives, such as:

- Strategic support
- Security liaison
- Architecture/engineering support
- Operational support

Strategic Support and Management

- Develop, implement and monitor a strategic, comprehensive enterprise information security and IT risk management program to ensure that the integrity, confidentiality and availability of information is owned, controlled or processed by the organization.
- Manage the enterprise's information security organization, consisting of direct reports and indirect reports (such as individuals in business continuity and IT operations). This includes hiring, training, staff development, performance management and annual performance reviews.
- Facilitate information security governance through the implementation of a hierarchical governance program, including the formation of an information security steering committee or advisory board.
- Develop, maintain and publish up-to-date information security policies, standards and guidelines. Oversee the approval, training, and dissemination of security policies and practices.
- Create, communicate and implement a risk-based process for vendor risk management, including the assessment and treatment for risks that may result from partners, consultants and other service providers.
- Develop and manage information security budgets, and monitor them for variances.
- Create and manage information security and risk management awareness training programs for all employees, contractors and approved system users.
- Work directly with the business units to facilitate IT risk assessment and risk management processes, and work with stakeholders throughout the enterprise on identifying acceptable levels of

residual risk.

- Provide regular reporting on the current status of the information security program to enterprise risk teams, senior business leaders and the board of directors as part of a strategic enterprise risk management program.
- Create a framework for roles and responsibilities with regard to information ownership, classification, accountability and protection.
- Develop and enhance an information security management framework based on the **National Information Assurance Policy**
- Provide strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls.
- Liaise with the enterprise architecture team to ensure alignment between the security and enterprise architectures, thus coordinating the strategic planning implicit in these architectures.
- Coordinate information security and risk management projects with resources from the IT organization and business unit teams.
- Ensure that security programs comply with relevant laws, regulations and policies to minimize or eliminate risk and audit findings.
- Define and facilitate the information security risk assessment process, including the reporting and oversight of treatment efforts to address negative findings.
- Manage security incidents and events to protect corporate IT assets, including intellectual property, regulated data and the company's reputation.
- Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action.
- Develop and oversee effective disaster recovery policies and standards to align with enterprise business continuity management program goals. Coordinate the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of a security event. Provide direction, support and in-house consulting in these areas.
- Facilitate a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation, and increase the maturity of the security.
- Understand and interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services, including, but not limited to, privacy, risk management, compliance and business continuity management.

Security Liaison

- Liaise among the information security team and corporate compliance, audit, legal and HR management teams as required.
- Liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure that the organization maintains a strong security posture.
- Assist resource owners and IT staff in understanding and responding to security audit failures reported by auditors.

- Work as a liaison with vendors and the legal and purchasing departments to establish mutually acceptable contracts and service-level agreements.
- Manage security issues and incidents, and participate in problem and change management forums. Ensuring timely reporting and adequate participation in investigation for ICT security incidents, with Q-CERT and / or Law Enforcement agencies as applicable.
- Work with various stakeholders to identify information asset owners to classify data and systems as part of a control framework implementation.
- Work with the IT and business stakeholders to define metrics and reporting strategies that effectively communicate successes and progress of the security program.

Architecture/Engineering Support

- Consult with IT and security staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software.
- Recommend and coordinate the implementation of technical controls to support and enforce defined security policies.
- Research, evaluate, design, test, recommend or plan the implementation of new or updated information security hardware or software, and analyze its impact on the existing environment; provide technical and managerial expertise for the administration of security tools.
- Work with the enterprise architecture team to ensure that there is a convergence of business, technical and security requirements; liaise with IT management to align existing technical installed base and skills with future architectural requirements.
- Develop a strong working relationship with the security engineering team to develop and implement controls and configurations aligned with security policies and legal, regulatory and audit requirements.

Operational Support

- Coordinate measure and report on the technical aspects of security management.
- Manage outsourced vendors that provide information security functions for compliance with contracted service-level agreements.
- Manage and coordinate operational components of incident management, including detection, response and reporting.
- Maintain a knowledgebase comprising a technical reference library, security advisories and alerts, information on security trends and practices, and laws and regulations.
- Manage the day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans and communicate information about residual risk.
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and comply with policies and audit requirements.

- Design, coordinate and oversee security-testing procedures to verify the security of systems, networks and applications, and manage the remediation of identified risks.

Experience and Qualifications

- A minimum of seven years of IT experience, with five years in an information security role and at least two years in a supervisory capacity.
- A bachelor's degree in information systems or equivalent work experience; an M.B.A. or M.S. in information security is preferred.
- Certification from **[list of required vendor certifications, if any**].

Certification from **[list of required independent security organizations offering certification]** or other certifications at the discretion of direct line manager. Refer Note 1 Below

- Strong leadership skills and the ability to work effectively with business managers, IT engineering and IT operations staff.
- The ability to interact with **[Company Name]** personnel, build strong relationships at all levels and across all business units and organizations, and understand business imperatives.
- Knowledge and understanding of relevant legal and regulatory requirements, such as *National Information Assurance Policy, Cloud Security Policy, Qatari legislations etc.* ***Insert relevant local or global laws, standards and regulations.***
- Exhibit excellent analytical skills, the ability to manage multiple projects under strict timelines, as well as the ability to work well in a demanding, dynamic environment and meet overall objectives.
- Project management skills: financial/budget management, scheduling and resource management.
- Ability to lead and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals.
- A strong understanding of the business impact of security tools, technologies and policies.
- Strong leadership abilities, with the capability to develop and guide information security team members and IT operations personnel, and work with minimal supervision.
- Excellent verbal, written and interpersonal communication skills, including the ability to communicate effectively with the IT organization, project and application development teams, management and business personnel; in-depth knowledge and understanding of information risk concepts and principles as a means of relating business needs to security controls; an excellent understanding of information security concepts, protocols, industry best practices and strategies.
- Experience working with legal, audit and compliance staff.
- Experience developing and maintaining policies, procedures, standards and guidelines.
- Experience with common information security management frameworks, such as International Standards Organization (ISO) 2700x, the IT Infrastructure Library (ITIL) and Control Objectives for Information and Related Technology (COBIT) frameworks **[Substitute as appropriate].**

- Proficiency in performing risk, business impact, control and vulnerability assessments, and in defining treatment strategies.
- Knowledge of and experience in developing and documenting security architecture and plans, including strategic, tactical and project plans.
- Strong analytical skills to analyze security requirements and relate them to appropriate security controls.
- An understanding of operating system internals and network protocols.
- Familiarity with the principles of cryptography and cryptanalysis.
- Experience in system technology security testing (vulnerability scanning and penetration testing).
- Familiarity in application technology security testing (white box, black box and code review).

Note 1: Certifications with Worldwide Visibility

Certifications for information security professionals and adjacent disciplines fall into three categories.

- ✓ Many vendors issue their own certificates, which typically means that a certified individual knows how to operate that vendor's product. Check Point, Cisco, Microsoft, RSA and Guidance Software (EnCase) are the most prominent examples.
- ✓ Most of the security certifications today are vendor-neutral, issued by for-profit organizations (that earn a living with certification, renewal and training fees). Virtually a certificate covers every aspect of information security, risk management and BC — and most of them are unknown to job applicants and employers. Only a handful (see Note 1) have gained worldwide visibility. The SANS Institute (GIAC) reported 25,000 plus certified individuals in June 2009, while The International Information Systems Security Certification Consortium (ISC2; CISSP) and the ISACA (CISA) have each certified more than 60,000 individuals. Certified Business Continuity Professional (CBCP) and Member Business Continuity Institute (MBCI) are known to BC professionals.
- ✓ There is an increasing interest in specialty certifications for specific jurisdictions. For example, in Australia, doing security assessments of federal government systems requires an Infosec Registered Assessor Program (IRAP) certification. Obviously, the certification is useless anywhere else, but it is an absolute requirement for certain types of Australian government security work. This is a method by which governments can exert quality control (of a sort), without stifling free competition in the commercial sector. Other country-specific certifications are the BSI Lead Auditor (U.K.), TeleTrusT Information Security Professional (TISP; Germany), and the U.S. Department of Defense Directive (DOD) 8570.

Role-specific certifications:
Certified Information Systems Security Professional (CISSP) issued by ISC2
Certified Information Systems Auditor (CISA) issued by ISACA
Certified Information Security Manager (CISM) issued by ISACA
Global Information Assurance Certification (GIAC) issued by SANS
Certified business Continuity Professional (CBCP) issued by the DRI International
Member of Business Continuity Institute (MBCI) issued by BCI

Vendor-specific certifications:
CCSP issued by Cisco
MCSE – Security issued by Microsoft
http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications