[](http://www.iso27001security.com/)Job Description:   
Information Security Manager

Prepared by Gary Hinson

Version 1 June 16th 2009

# Purpose

This is an idealized job description template from which to generate your own job descriptions, vacancy notices *etc*.  Like the ISO/IEC 27000-series standards, it is generic and needs to be tailored to your specific organizational requirements. This is definitely not legal advice!

# Job description

**Reports to**: Chief Executive Officer or Chief Governance Officer.

**General description of the rôle**: the Information Security manager is in charge of the Information Security Management function, providing line management, leadership and strategic direction for the function and liaising closely with other managers. The purpose of the Information Security Management function, in turn, is to bring the organization’s information security risks under explicit management control through the Information Security Management System.

**Key responsibilities** [this is not an exhaustive list and the details are bound to change over time]:

* Routine line management and leadership of staff within the Information Security Management function
* Leadership and strategic direction for the function, ranging from planning and budgeting to motivational and promotional activities expounding the value of information security
* Liaison with and offers strategic direction to related governance functions (such as Physical Security/Facilities, Risk Management, IT, HR, Legal and Compliance) plus senior and middle managers throughout the organization as necessary, on information security matters such as routine security activities plus emerging security risks and control technologies
* Recruitment, leadership and direction for a loose network of information security ambassadors distributed throughout the organization
* Leads the design, implementation, operation and maintenance of the Information Security Management System based on the ISO/IEC 27000 series standards, including certification against ISO/IEC 27001 where applicable
* Forms a “centre of excellence” for information security management, for example offering internal management consultancy advice and practical assistance on information security risk and control matters throughout the organization and promoting the commercial advantages of managing information security risks more efficiently and effectively
* Leads or commissions the preparation and authorizes the implementation of necessary information security policies, standards, procedures and guidelines, in conjunction with the Security Committee
* Leads the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies *etc*. and applicable laws and regulations
* Leads or commissions suitable information security awareness, training and educational activities
* Leads or commissions information security risk assessments and controls selection activities
* Leads or commissions activities relating to contingency planning, business continuity management and IT disaster recovery in conjunction with relevant functions and third parties

**Key personal characteristics and competencies of the ideal candidate** [this is also not an exhaustive list, and some aspects may not be legal in some jurisdictions]:

* *At least 5 years* of full-time work experience in information security management and/or related functions (such as IT audit and IT Risk Management)
* Information security management qualifications such as CISSP or CISM
* Absolutely trustworthy with high standards of personal integrity (demonstrated by an unblemished career history, complete lack of criminal convictions *etc*.), and willing to undergo vetting and/or personality assessments to verify this if necessary
* Hands-on team leadership and management experience, ideally coupled with suitable management qualifications such as an MBA
* Typically a background in technical IT rôles such as IT architecture, development or operations, with a clear and abiding interest in information security

# Copyright

[](http://creativecommons.org/licenses/by-nc-sa/3)This work is copyright © 2009, [ISO27k Forum](http://groups.google.com/group/iso27001security), some rights reserved.  It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](http://creativecommons.org/licenses/by-nc-sa/3.0/).  You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum ([www.ISO27001security.com](http://www.ISO27001security.com)), and (c) if shared, derivative works are shared under the same terms as this.