



## **Information Security Policy, Awareness and Compliance Manager**

### **Role justification, job description and candidate specification**

#### **Executive summary**

The Information Security Policy, Awareness and Compliance Manager is a vital and integral element of the Information Security Management System (ISMS). The rôle enhances, supports and enables the technical information security controls by addressing human factors.

#### **Justification for this position**

The Information Security Policy Manual (ISPM) is intended to be a comprehensive and up-to-date suite of information security policies, standards, procedures and guidelines for the organization. It should explicitly define the organization's requirements for structuring and operating the ISMS, which in turn is needed to bring and maintain information security firmly under management control and to adopt good security practices. Unless it is properly managed by a responsible and capable individual, there may be gaps in the ISPM and it is unlikely to be of sufficient coherence and quality. Without adequate maintenance, the ISPM will decay if it fails to keep up with changes in the information security threats, vulnerabilities and the potential business impacts of security failures, and hence the ISMS will not fully meet the organization's information security requirements.

The ISPM is of little value unless our employees, and in some cases employees of external/third party organizations, are both aware of and comply with their information security obligations in the manual. Therefore suitable information security awareness and training activities are necessary to promote and enforce the ISPM, and these also need to be professionally managed and directed in order to ensure they are effective. You could say that security awareness and training are the glue that binds the whole ISMS together and sticks information security firmly in people's minds.

In addition to the organization's internal information security requirements, there are numerous obligations or intentions to comply with information security requirements defined by third parties, some of which explicitly demand information security policies, awareness and compliance activities. Examples include:

- Recognized good practice information security standards (e.g. the ISO/IEC 27000 and NIST SP800 series standards, ISACA's COBIT and the Information Security Forum's Standard of Good Practice for Information Security);
- Laws such as those relating to privacy/data protection (e.g. Privacy Act, Health Insurance Portability and Accountability Act), information security management (e.g. Federal Information Security Management Act, Computer Security Act), corporate governance (e.g. Sarbanes Oxley Act, Gramm-Leach-Bliley), fiscal/corporate management (e.g. Companies Act) and intellectual property (e.g. copyright, trademarks and patent laws);
- Industry regulations (e.g. NERC CIP-004, FFIEC, Basel II);
- Contractual clauses (e.g. PCI-DSS and security clauses in contracts with specific trading partners).



It makes sense to combine compliance with both internal and external requirements in a coherent fashion so as to avoid conflicts, duplication or gaps in the coverage, and utilize the similar skills required.

While information security policy development, awareness/training and related compliance activities *could* continue to be performed by existing employees in various parts of the organization as they currently are, this would make coordination and consistency more difficult and is unlikely to result in a sufficiently coherent and professional approach information security policies and awareness. Having a suitable individual in charge of all three activities will improve compliance and reduce information security risks, both of which will lead to tangible savings and other benefits to the organization.

### **Key responsibilities of this position**

The Information Security Policy, Awareness and Compliance Manager is responsible for:

- Managing and leading activities associated with the ISPM. This involves liaising with relevant employees from various parts of the organization and, in some cases, external/third party organizations in order to specify, commission, develop, review, approve, implement, maintain and obtain compliance with the ISPM;
- Managing and leading training and awareness activities to ensure that relevant employees and third parties understand, acknowledge and ultimately fulfill their obligations defined in the ISPM, plus applicable laws, regulations and contractual commitments, and ethics;
- Managing and leading information security compliance activities designed to achieve and maintain a high degree of compliance with both internally and externally-defined security requirements.

### **Personal characteristics of suitable candidates**

The Information Security Policy, Awareness and Compliance Manager must:

- Have an information security qualification such as CISSP or CISM, with a thorough understanding of information security principles and practices and ideally suitable experience of an ISMS;
- Be familiar with current good security practices gleaned from sources such as the ISO/IEC 27000 and NIST SP800 standards plus applicable laws and regulations;
- Be an experienced manager or team leader, ideally with a management qualification such as an MBA;
- Be a capable professional writer;
- Be “a people person” with experience of delivering information security awareness and training activities, ideally with experience of developing the creative materials used;
- Be proactive and self-motivated, capable of appreciating and acting in the organization’s best interests;
- Exude confidence and professionalism in relation to information security policies, awareness and compliance;
- Be inspirational, an enthusiastic or even evangelical promoter of information security.



### Important note from IsecT Ltd.

This is a generic example or template document. **It is unlikely to be entirely sufficient or suitable for you without customization.** Because it is generic, it cannot fully reflect every user's requirements. We are not familiar with your organization's specific circumstances or information security needs. It is certainly *not* legal advice.



This work is copyright © 2009, IsecT Ltd., some rights reserved. It is licensed under the [Creative Commons Attribution-NonCommercial-Share Alike 3.0 License](#). You are welcome to reproduce, circulate, use and create derivative works from this provided that:

- (a) it is not published in any public forum other than those explicitly authorized for this purpose by IsecT Ltd.;
- (b) it is not sold or incorporated into a commercial product; and
- (c) it is properly attributed to IsecT Ltd.