Model job description

# Information Risk and Security Manager

## Scope, purpose and nature of role

The primary functions of the Information Risk and Security Manager are to (1) inspire and coordinate the wide variety of activities associated with identifying, evaluating and treating information risks throughout the organization, and (2) lead the information risk and security team. The role includes but stretches well beyond IT risk and security, touching on aspects such as compliance, physical security, personnel security, incident management, business continuity and more. A further objective is to liaise with and provide relevant, timely, credible information and sound professional advice to senior management concerning the organization’s information risk profile and the status of information risk treatments, with the aim of preventing ‘nasty surprises’.

## Distinguishing characteristics of the ideal candidate

The following personal traits are high on our wish-list:

* Passionate about information risk and security - a font of knowledge and energy, with a strong almost evangelical drive and enthusiasm for the subject;
* An inspirational leader – keen to motivate and get the most out of the organization’s information risks and security experts, aligning colleagues towards the achievement of business objectives;
* Good at forming productive working relationships - liaising with various specialists, advisors, managers and influencers throughout the organization, plus third parties such as business partners, suppliers, customers, authorities *etc*., on information risk and security matters;
* A strategic thinker – able to step back from the short- and medium-term issues to see the longer-term changes and threats relating to information, and to both engineer and seize valuable opportunities for improvement;
* Personal integrity and credibility – high ideals, tempered by a pragmatic, realistic approach.

## Qualifications, skills and experience

The following are relevant and desirable for this role:

* **Information risk and security management:** CISSP, CISM, CRISC, or similar; at least 10 years’ work experience in the field; familiarity with applicable standards, methods, models and approaches;
* **General business management:** MBA or business degree; at least 5 years as a team leader or manager responsible for dealing with information risk, security, privacy, incidents, business continuity, compliance *etc*.

Candidates must be willing to undergo background checks to verify their identity, character, qualifications, skills and experience.