Model job description

# Information Security and Privacy Compliance Manager

## Scope, purpose and nature of role

The primary duty of the Information Security and Privacy Compliance Manager (ISPCM) is to ensure that the organization achieves a sufficient level of compliance with relevant information security and privacy-related obligations imposed by laws, regulations, standards, contracts, policies *etc*. This involves proactively identifying and assessing the obligations, developing suitable responses and, in conjunction with various other parties, adopting suitable controls, policies, procedures, compliance metrics, awareness/training, monitoring, reinforcement and enforcement activities. The ISPCM also: acts as a specialist professional advisor on information security and privacy compliance matters; liaises closely with other governance, risk management, information security, privacy and compliance experts, plus external authorities and contacts; assists with the drafting, review and implementation of the compliance elements of information security and privacy policies; prepares reports concerning compliance failures, breaches or incidents; owns the information security and privacy parts of the compliance database; and has a leadership/advisory role in the identification, management and eventual resolution of exceptions and exemptions.

## Distinguishing characteristics of the ideal candidate

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

* Decisive – able to make difficult decisions, prioritize along strategic lines, and take appropriate action without prevaricating or unduly delaying, yet willing to be held to account for those decisions and actions, and willing to seek and accept advice from experts where necessary;
* Persuasive: overcoming inertia, reluctance *etc*. and convincing people to fulfil their obligations;
* Self-contained *i.e*. self-motivated and sufficiently confident and assertive to take actions that may be unpopular with those who risk or are contravening laws, policies, contract terms *etc*.;
* Diplomatic, rational and reasonable – able to handle difficult situations sensibly and fairly, engendering trust and respect in themselves despite the often-delicate nature of the role (*e.g*. dealing professionally with noncompliant managers or business partners).

## Qualifications, skills and experience

The following are relevant and desirable for this role:

* **Information security risk management:** at least 2 years work experience in this area, ideally holding relevant qualifications such as CISSP, CISM or degree;
* **Compliance and enforcement:** at least 3 years work experience in this area;
* **General:** at least 15 years employment post school/college.

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