Model job description

# Security Awareness Officer

## Scope, purpose and nature of role

Reporting to and under the guidance of the Security Awareness Manager, the Security Awareness Officer (SAO) is primarily responsible for delivering information security awareness and training throughout the organization for examples: maintaining and delivering the information security element of new employee orientation/induction training; assisting with the maintenance and dissemination of information security policies, procedures and guidelines; assisting with the gathering and analysis of information security metrics, particularly those relating to security awareness and culture (*e.g*. employee surveys); assisting with the planning, organization and delivery of various other security awareness activities from time to time (*e.g*. workshops, case studies and seminars). The job will involve liaison with various internal and external suppliers of awareness and training materials and services, and building a strong social network of contacts throughout the organization to help guide and deliver the awareness program.

## Distinguishing characteristics of the ideal candidate

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

* A patient teacher/trainer, good at putting points across in an engaging and enthusiastic manner, inspiring and motivating colleagues to take a genuine interest in information security;
* A “people person” who gets on well with others;
* Able to prepare as well as deliver awareness/training materials;
* Ideally more than just a basic understanding of information risk, security and related issues such as governance and compliance.

## Relevant qualifications, skills and experience

The following are considered relevant and desirable for the SAO role:

* **Information security:** CSSP, CISSP, CISM or similar qualifications (either certified or working towards them) plus at least 3 years work experience in this area;
* **Awareness and training:** some experience developing and/or delivering awareness/training activities (not necessarily information security but probably equally technical in nature);
* **Other aspects**: general familiarity with information security, risk, governance and control concepts.

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