Model job description

# CISO (Chief Information Security Officer)

## Scope, purpose and nature of role

More than merely a figurehead, the CISO is the thought-leader for information risk and security management and related activities throughout the organization. That this is a C-level position reporting directly to the CEO clearly indicates senior management’s appreciation of its relevance and importance to the business. The CISO is responsible for developing and implementing strategies concerning the protection and legitimate exploitation of our information assets, ensuring our compliance with relevant laws and regulations, governing and (at a high level) managing the information risk and security management function, and most of all supporting/enabling achievement of business objectives. The CISO has interests in, collaborates with and seeks alignment of the *entire* organization since information is a valuable yet vulnerable resource throughout. Where appropriate, the CISO also liaises with external stakeholders such as auditors, service suppliers, customers and authorities such as industry regulators on significant matters.

## Distinguishing characteristics of the ideal candidate

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

* Visionary, a big-picture thinker with a broad perspective on information risk and security, governance, compliance *etc*., and a solid appreciation of how information security protects, supports *and* enables the business over a strategic scope and timescale;
* A natural leader with demonstrably strong leadership capabilities *e.g*. highly influential and motivational, a good bidirectional communicator both in writing and face-to-face;
* Combining strong personal integrity (grit) with pragmatism, willing to stand up for what’s right for the organization, yet open to alternative means of achieving it.

## Qualifications, skills and experience

The following are relevant and desirable for this role:

* **Information risk and security management:** CISM, master’s degree or similar; at least 20 years work experience including at least 10 years in the field; genuine hands-on experience with relevant approaches, standards, methods, frameworks *etc*.;
* **Business management:** MBA or equivalent, plus *extensive* real-world management experience involving contact with senior management, departmental/corporate management, budgeting, strategic planning, management reporting and metrics, legal and regulatory compliance, formulation and management of information security policies, forensics, fraud *etc*.

Candidates must be willing to undergo extensive background checks to verify their identity, character, qualifications, skills and experience, and suitability for the role.