



Your journey of aspirations begins here!

CDB believes in elevating the lives of all Sri Lankans. Our focus is to employ and engage individuals who aspire to grow their careers within a renowned financial entity, working with a dynamic team of industry professionals who are dedicated to raising the bar and setting benchmarks in Sri Lanka's financial industry.

## Manager - IT Governance Risk & Compliance (GRC)

We seek a highly motivated, enthusiastic, dynamic individual to lead our Risk and Compliance Department as Manager – IT Governance.

### Key Responsibilities

- In collaboration with IT and business units, develop and manage information security policies, standards and guidelines
- Manage, maintain, and continually improve all elements of the ISMS (ISO 27001) and the BCMS (ISO 22301), including policies, standards, controls, and associated registers
- Ensure that information technology governance and information security requirements are addressed during the procurement and implementation of all new information systems and service providers
- Identify relevant industry trends and potential evolving risks confronting IT/Business initiatives on an ongoing basis, and assess their impact on the organization's scope and strategy in terms of information security and business resilience
- Ensure that risk acceptance and mitigation plans in place are appropriate, with business sign-off and proactive management of risk governance. Monitor remediation plan execution through the risk treatment process
- Monitor and report on compliance with security policies, as well as the enforcement of policies, standards, and guidelines
- Provide leadership in achieving the Company's information security goals
- Identify security control gaps and providing recommendations, implement solutions and track progress
- Measure and execute a comprehensive security compliance programme, including appropriate reporting and remediation/recommendations
- Promote and monitor enterprise information security awareness programs; ensure organizational compliance

### Qualifications and Experience

- A Bachelor's Degree in Computer Science, Information Security or Technology or a Professional qualification in IT recognized by the University Grants Commission
- Full-time IT Governance, Risk, and Compliance experience in a reputable firm or organization for seven years
- Excellent knowledge of all aspects of technology, infrastructure, operations, security, development, change/transformation, support, innovation, and vendor management
- Professional certification in CISA, CISM, CGEIT, ISO, ITIL, or an equivalent combination in the IT/IS security discipline is preferred
- Previous experience in developing, implementing and maintaining an Information Security Management System (ISMS) and Business Continuity Management System (BCMS), certification/re-certification to ISO 27001 and ISO 22301 would be an advantage

### Special Skills and Attributes Required

- Verbal and written communication skills, including the ability to articulate complex concepts to various technical and non-technical audiences
- Experience and thorough understanding of overall Governance, Risk & Compliance (GRC) concepts
- Deeper understanding of information security technologies, regulatory and compliance needs, particularly in the financial sector
- Good understanding of relevant industry standards and frameworks (e.g. ISO 27001, ISO 22301, COBIT, NIST)
- Solid comprehension of cloud infrastructure, project management, development, and DevOps within a fast-moving implementation environment

Rewards and remuneration commensurate with qualifications, competencies and abilities, with a well-defined career path awaits those with ambition, motivation and a willingness to perform.

Please e-mail your CV together with contact details of two non-related referees indicating the position applied for in the "Subject" line of the e-mail to

 [careers@cdb.lk](mailto:careers@cdb.lk)

**CDB**   
Your Friend