Security Analyst Certification

Why the certification is relevant

This rise in the widespread use of technology brought with it a rise in security problems and cybercrime. For hackers, the possibilities increased exponentially, along with the potential rewards. Cybercrime now permeates every facet of society and is for most organisations critically important. Independent of size or industry every business starts to take necessary precautions to protect their information systems and technology from unauthorised access, particularly if such access is made by individuals with malicious intent.

Focus of the Security Analyst

Advancing your career as a Security Analyst to take control of your enterprise's security strategy, implementation, and testing is a good place to start. In general, Security Analysts are tasked with identifying weaknesses in current security systems and developing solutions to close security vulnerabilities. To perform this task well, ideal candidates will have highly advanced technical skills, a proven ability to communicate with all levels of an organisation and experience applying both skillsets to solve real problems. The Security Analyst certification program covers technology, systems and business analysis. It covers an analytical and modelling framework for integrating IT, technology platforms and infrastructure with strategy, innovation, value, requirements and complexity management. The Security Analyst Program can be integrated into any relevant organisation. It does so by adding the following theory, practice and modelling capabilities.

Theories Practitioners will learn

- Capture security forces and disruptive trends
- Identify security gaps and pain points
- Understand security strategies
- Identify security requirements
- Security performance management

What Practitioners will work with in Practice

- Work with stakeholders, business and security owners
- Security Model definitions
- Security Model analysis
- Setup security measurements and monitoring
- Apply continuous security improvement

Modelling capabilities Practitioners will gain

- Develop Security Stakeholder Map
- Develop Security Requirement Map
- Develop Security Strategy Maps
- Define Security Capability Maps

Enterprise Standards used

OMG (software standards):
- UML - Unified Modelling Language
- CMMN – Case Management Modelling Notations

LEADing Practice (Enterprise Standards):
- Security Strategy (Physical & Cyber)
- Security Roadmap (Physical & Cyber)
- Security Categorisation & Classification
- Security Decomposition & Composition
- Security Modelling
- Security Lifecycle
- Security Meta Model

ISO27001 Information Security
NIST Cybersecurity Framework
IEEE Process Engineering standards
ISO 42010 Systems & Software Engineering
ITIL 3 (IT delivery concept)
COBIT (Governance)