Security Architect Certification

Why the certification is relevant

Malicious criminals continue to plague the business world with constant, and all too often successful, attacks on IT infrastructure. So, in a regulatory and compliance environment where failing to protect sensitive or private data can result in costly fines and penalties, it is time for businesses to take a much more proactive approach to their data security protocols, policies, and procedures.

Focus of the Security Architect

For most modern business enterprises, the collection, processing and storage of data is the driving force behind every transaction, decision and strategy. In a business era where everyone and everything is networked and connected, data is the most valuable commodity. Therefore, it is extremely vital that every business take necessary precautions to protect their data from unauthorised access, particularly if such access is made by individuals with malicious intent. The Security Architect's role is uniquely designed to take control of your enterprise's IT security strategy and implementation. This entails identifying security gaps and weaknesses from an architectural perspective. The Security Architect 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 and owners
- Benchmark security maturity levels
- Security Business Model design
- Security Model development
- Develop security guidelines

Modelling capabilities Practitioners will gain

- Develop Security Stakeholder Map
- Develop Security Requirement Map
- Develop Security Strategy Maps
- Define Security Capability Maps
- Define the Security Landscape Canvas
- Create Security Models
- Develop Security Service Models
- Construct Security Operating Models

Enterprise Standards used

OMG (software standards):
- BPMN – Business Process Modelling Notations
- CMMN – Case Management Modelling Notation
- DMN – Decision Modelling Notation

LEADing Practice (Enterprise Standards):
- Emerging & Disruptive Security Trends & Forces
- Security Classification & Categorisation
- Security Artefacts
- Security Architecture Modelling
- Security Lifecycle
- Security Meta Model

ISO27001 Information Security
NIST Cybersecurity Framework
Open Group Business Architecture
ISO/IEC 27033 IT Network Security Standard
Zachman Framework (Interrogatives)
ITIL 3 (IT delivery concept)
COBIT (Governance)