SMU
SINGAPORE MANAGEMENT UNIVERSITY

SMU Academy

SMU Certificate in IT Risk, Governance & Security (IBF Level 1)

Synopsis

Recent high-profile cyber crimes and IT breaches across the globe have made headline news. With digitilization rapidly transforming the financial services industry, managing technology risk is now a business priority.

It is critical for banking professionals to understand and manage IT risks, threats and vulnerabilities, to safeguard business continuity and reputation. Benchmarked to industry standards and best practices, this 2-day certification program provides the fundamental framework to identify risks and implement controls against potential security concerns.

Highlights

- Understand governance principles & risk management concept
- Know major risk exposures for Technology & Operations (T&O)
- Identify tools and controls to mitigate risks
- Be familiar with regulatory framework applicable to T&O
- Develop awareness of IT risks, threats & vulnerabilities
- Identify relevant network security controls to mitigate risks
- Assess new threats against established security controls
- Learn good security practices and standards
- Understand the intent and objectives of security reviews
- Perform security standards and compliance reviews

Program Date

16 Sep & 23 Sep

Classes from 9am to 5pm

Program Fee

S$1,500 (excluding GST)

IBF-STS Funding

IBF-STS provides 70% funding, subject to all eligibility criteria being met. For Singapore Citizens aged 40 years and above, IBF-STS provides 90% funding, subject to existing grant caps. For more information, refer to https://www.ibf.org.sg/programmes/Pages/IBF-STS.aspx.

For Enquiries

Jaclyn Mah | +65 6828 0254
Chiew Yee | +65 6828 0971

fti@smu.edu.sg
fti.smu.edu.sg/IT Risk L1

Who Should Attend

- New hires and entry level professionals in financial services or IT risk and security related disciplines
- Middle office staff such as product controllers, risk managers, auditors and compliance officers seeking to gain foundation knowledge in IT risk and security

Curriculum

Governance and Management Oversight

- Principles of governance & enterprise risk management
- IT governance & risk considerations
- Key governance operations, documents & risk management policies

Managing Contingency Risk

- Business continuity plan (BCP) vs Disaster recovery plan (DRP)
- Recovery time objectives (RTO) & recovery point objectives (RPO)
- Business impact & RTO

Internal Controls

- Preventive, detective & corrective controls
- Types of control & their limitations
- Technology risk management guidelines

Cyber Risk, Threats & Vulnerabilities

- Vulnerability element – operating system, application, database & network
- Threat source & categories
- CIA framework – confidentiality, integrity & availability

Cyber Security Components

- Technical safeguards
  - AAA concept
  - Encryption
  - Firewalls
  - Malware protection
  - Application design
- Data safeguards
  - Access control
  - Logging
  - Data loss prevention
  - Penetration testing
  - Security analyzers
- Human safeguards
  - account administration
  - password management

Cyber Security Frameworks & Standards

- CoBIT 5, ISO, ITIL, NIST, etc
- Key regulations – MAS Technology Risk Management (TRM) Guidelines
- Security standards baseline review

Cyber Security Attack & Defence Modelling

- Case study

Trainer's Biography

Leonard Ong has over 15 years of information and corporate security experiences gained in telecommunication, enterprise and banking industries. He held various roles within the security profession, with responsibilities in information security, corporate security, project management, consulting and business development. Currently Associate Director at Merck, Leonard also serves on the ISACA Board of Directors.