



CYBER SECURITY (For ARMs)

IBF Standards - Private Banking and Wealth Management

4 IBF-STs TRAINING HOURS

For registration of public scheduled session, [click here](#).
To organize a tailored session for your organization, please contact us at email@salmonthrust.com

This 4-hour course provides a comprehensive understanding of the generic enterprise and cyber risk management practices and specific cyber risk concepts commonly deployed in the financial industry to enhance the overall cyber security and risk management. The complexity of today's connected digital environment is exposing organizations to numerous technology and cyber threats that could lead to substantial data and financial losses as well as reputational damages.

Designed for professionals responsible for business activities exposed to technology and cyber risks, this programme focuses on the practical considerations in the design, adoption and implementation of systems and processes for optimal cybersecurity and technology risk (TR) management, aligned to global cybersecurity best practices, including MAS TR and Cyber Hygiene guidelines, covering the key technology and cyber risk management concepts and best practice implementation approaches, including its management and applications to IT and cyber risks. It will also go beyond that and address the practical usage of that knowledge; with case studies and examples.

TARGET AUDIENCE

- Assistant Relationship Managers in Private Banking
- Operations functions in Private Banking
- Covered persons under Private Banking Code of Conduct who may be interested

LEARNING OUTCOMES

- Identify potential risks and threats associated with cybersecurity, such as viruses, hacking, and identity theft
- Protect personal and business information from cybersecurity threats
- Follow cybersecurity policies and procedures in own area of work
- Explain cybersecurity practices to customers and/or stakeholders
- Take appropriate actions as required during cybersecurity breaches
- Identify relevant channels in the organisation to report and initiate corrective actions

COURSE OUTLINE

Cybersecurity threats and risks

- Motivation and drivers of cybercrimes
- Cyber universe of Attack Surface and evolution
- Risk identification - common cyber threats like viruses, hacking and identity theft
- Emerging cyber threats and risks

Organisation's cybersecurity policies and procedures

- Foundational aspect – data governance, hierarchy, breach and loss data incidence management
- Cyber risk management framework and processes, implementation and compliance
- Understanding of causes of data leakage and losses
- Training and education

Areas prone to cybersecurity threats

- Cyber threat landscape
 - Mission critical assets
 - Data security
 - Application security
 - Endpoint security
 - Network security
 - Perimeter security

Best practices to safeguard against threats

- Establish cyber governance structure
- Produce cybersecurity policies and procedures
- Maintain board's and senior management's engagement with cyber risk
- Enhance user education and awareness incl. for clients
- Comply with cyber risk management framework and principles
- Forward looking scenario analysis with breach and simulation testing (ethical hacking and penetration)

Cybersecurity regulations and compliance requirements

- Adopt best practices from NIST guidelines and standards, MAS TRM, 3rd Party and Cyber Hygiene guidelines
- Periodic independent cyber risk model validation and review and assessment
- Scenario analysis and dry runs readiness and response testing

Relevant channels and responsible stakeholders for cybersecurity reporting procedures

- Conform to Cyber and Operational GRC / ERM framework organizational reporting hierarchy and process based on COSO, ISO 31000 standards for information and communication sharing and reporting
- Dynamic dashboard information access to key stakeholders, including Board, senior management, Divisional and BU Heads

Concluding Remarks, Q&A, Summary of Key Points, Course Feedback and MCQ Assessment

Assessment - MCQ

IBF STANDARDS

This course is designed to meet the following Technical Skills and Competencies (TSCs) in Skills Framework for Financial Services:



This programme has been accredited by The Institute of Banking and Finance (IBF) under the IBF Standards.

Industry Segment : Private Banking and Wealth Management

Job Role : Assistant Relationship Manager
Relationship Managers
Relationship Director / Team Leader

Technical Skills and Competencies (TSCs) and Proficiency Level

C1. Cybersecurity - Level 3

IBF-STTS

This programme has been accredited under the IBF Standards, and is eligible for funding under the IBF Standards Training Scheme (IBF-STTS), subject to all eligibility criteria being met. Candidates are advised to assess the suitability of the programme and its relevance to participants' business activities or job roles.

Find out more on www.ibf.org.sg

ABOUT IBF CERTIFICATION

Participants are encouraged to access the [IBF MySkills Portfolio](#) to track their training progress and skills acquisition against the Skills Framework for Financial Services. You can apply for IBF Certification after fulfilling the required number of Technical Skills and Competencies (TSCs) for the selected job role.

Find out more about IBF certification and the application process [here](#).

ABOUT THE IBF STANDARDS

The IBF Standards are a set of competency standards for financial skills. These Standards are developed in partnership with industry leaders and provide a professional development and skills roadmap for financial sector practitioners to excel in their respective job roles. They currently cover 12 industry segments in the financial sector.

ABOUT THE INSTITUTE OF BANKING AND FINANCE SINGAPORE

The Institute of Banking and Finance Singapore (IBF) is the national accreditation and certification agency for financial industry competency in Singapore under the IBF Standards. Find out more on www.ibf.org.sg

ABOUT SALMON THRUST

Founded in 2004, Salmon Thrust is committed to delivering real-world banking and financial training to professionals working in banks, corporates, government agencies, and other financial institutions.

Based in Singapore, we offer our clients in the region a broad range of up-to-date financial topics, delivered via classroom training and e-learning. Our courses range from foundational programmes for new entrants, right through to the most complex and current topics in the industry.

At Salmon Thrust, we are attentive to our clients' diverse learning needs. We identify relevant courses to bridge the learning and skill gaps, empowering our clients to make better decisions and bring real value to both their customers and organisations.

T (65) 6323 0768 **E** email@salmonthrust.com