SWIFT Security Bootcamp 2.0

A unique experience to build solid security management skills

In an era of persistent cyber threats, security management is high on everyone's agenda. The security of your SWIFT infrastructure plays a critical role in the running of your business.

To control these SWIFT security aspects, a number of functions have been established, including SWIFTNet Security Officer, Alliance Security Officer, and swift.com Administrator.

In addition, SWIFT introduced its Customer Security Programme (CSP) and its accompanying CSP Controls in further protection of customer businesses.

Today, many institutions struggle to setup the right organisational structure to man the required functions and often run suboptimal processes and procedures, which may lead to exposure and certain vulnerabilities or risks.
The SWIFT Security Bootcamp aims to shed light on cyber threat scenarios, security-related roles & responsibilities, risk driver mitigation, CSP awareness and help institutions to trigger the right questions internally to ensure security is managed in the best way possible, and provide the necessary know-how to manage all activities in line with best practice.

Audience

This course is an open enrolment course, designed for SWIFT Security Officers, Chief Information Security Officers, IT Security Auditors and Risk Managers, as well as members of SWIFT operations & Cyber Security teams who are interested to build on their expertise. By being open to several organisations, this course promotes interactivity and sharing of experience between participants.

Course Content

The program covers following topics:

- Cyber security concepts & latest threats
- Customer Security Controls **Framework** (part of CSP)
- SWIFT Product & Environment **Security Features**
- Scenario **Risk Assessment & Risk Drivers**
- Security best practice **guidelines** in line with **the latest interface releases and CSP requirements & CSP**
- **Cyber Intelligence**
- Security Roles and Responsibilities
  - Role of SWIFTNet Security Officers for PKI
  - Role of Hardware Security Module (HSM) administrators
  - Role of Alliance Security Officers (LSO/RSO)
  - Role of Alliance Gateway administrators
  - Role of swift.com administrators
  - Cyber risk management responsibilities
  - Cyber incident recovery function

The training is delivered by professional trainers and subject matter experts.

To ensure **multi-channel learning,** a combination of **practical best practice** advice, **theoretical** modules and **group facilitation** is used.

Practical Information

On industry request, the SWIFT Security Bootcamp was condensed over a duration of 3 days. The training will take place in various countries around the world.

For more information visit the tailored learning page of **our website**

Are you looking to train a group of employees at your premises? Would you like to combine topics? Thanks to its modular structure, the SWIFT Security Bootcamp can be customised to your needs.
Please contact your account manager for more information.

AGENDA
SWIFT SECURITY BOOTCAMP 2.0

DAY 1

Customer Security Controls Framework

- What is the concern?
- Landscape risk and threats
- Architecture types
- The Security Controls Framework and its evolution
- The KYC-SA attestation process
- Cyber risks and counterparty risk management

Alliance Security Management: Alliance Access

- Introduction
- Administer your Alliance Access
- Secure your back-office applications
- Risk scenarios and security controls

Alliance Security Management: Alliance Web Platform

- Introduction
- Administer your Alliance Web Platform
- Secure your connections

DAY 2

SWIFTNet Security Management: The Public Key Infrastructure

- SWIFT, security and the PKI
- PKI administration through O2M
- Reporting and administration
- Risk scenarios and security controls

Alliance Security Management: Alliance Gateway

- Introduction
- Administer your Alliance Gateway
- Prepare PKI for messaging
- Secure your remote applications
- Risk scenarios and security controls

Cyber-attacks on customers' systems (CSI)

- CSP and Customer Security Intelligence
- SWIFT ISAC portal
- SWIFT network and the local customer managed environment
- Modus Operandi in practice
- Recovery roadmap

DAY 3

SWIFTNet Security Management: The Hardware Security Module

- What is an HSM?
- Management of an HSM
- HSM behaviours
- Risk scenarios and security controls

swift.com Security Management

- Introduction
- swift.com Administrators
- Alliance Security Officers
- SWIFTNet Security Officers
- Risk scenarios and security controls

Security best practices

- Introduction to Alliance security guidance
- Case study:
  - Risk management
  - Cyber incident response
  - Conclusion

Learning objectives

Once you complete this workshop you should be able to:

- Understand the latest cyber threats and their potential impact on your infrastructure
- Identify the functions involved in the management of a SWIFT environment, and how to implement segregation of duties
- List the tools available to help you securing your SWIFT applications
- Explain the SWIFT Customer Security Programme, and translate the Security Controls into concrete actions