Security Bootcamp Scope

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.

Security Bootcamp
What do you learn?

Participate to this open enrolment course to build up your SWIFT security management skills.

- How to approach Cyber Security on SWIFT & learn the latest Cyber threats
- Gain deep dive understanding on the CSCF Framework (Customer Security Control Framework)
- Learn the latest info and best practices around the KYC Self Attestation tool and its processes
- Get to know about the latest Cyber Security Counterparty Risk guidelines
- Gain insights on CSCF 2019, lessons learned and future CSP roadmap on 2020
- Understand the effectiveness of your SWIFT Organisation Security Roles and Responsibilities
- Learn from the experts from SWIFT on CSI (Customer Security Intelligence)
- Gain insights on the Modus Operandi and experience an actual Cyber Attack and how to prevent future attacks and Cyber resilience
- With continued improvements, learn How to better secure your SWIFT Products & Environment with latest Security Features
- As threats continue to exist, learn How to better define Scenario Risk Assessment & mitigate Risk Drivers
- Gain insights to the latest Security best practice guidelines from our consulting field experience, and engage further with SWIFT experts on CSP best practices
- Learn and participate from our case studies

Security Bootcamp 2020
Agenda

The SWIFT Security Bootcamp has a duration of 3 days split in x modules.

The session is articulated around a combination of practical best practice advice, theoretical sessions, group brainstorms and practical activities.

On request, the session can be delivered at your premises with an agenda customised to your needs.

SWIFT's Security Bootcamp

Day 1	Day 2	Day 3
Customer Security Programme - What is the concern? - Landscape Risks and Threats - Architecture types - The Security Controls Framework and Evolution - The KYC-SA attestation process - Cyber Risks and Counterparty Risk Management	**Managing PKI** - 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	**Hardware security Module** - Important to know - Risk scenarios and security controls **Managing the swift.com portal** - Introduction to swift.com - swift.com Administrators - Risk scenarios and security controls **Secure Channel application on swift.com** - Introduction - Alliance Security Officers - SWIFTNet Security Officers - Risk scenarios and security controls
Alliance Security Management: Alliance Access - Introduction - Administer your Alliance Access - Secure your back-office applications - Risk scenarios and security controls	**Cyber Intelligence** - SWIFT Network and the local customer managed environment - CSP and Customer Security Intelligence - Customer Security Intelligence at SWIFT - Cyber Attacks, how can you detect and defend yourself (Practical Demo)	**Security best practices** - Introduction to Alliance security guidance - Case study -- Risk Management -- Cyber Incident Response -- Conclusion

Content updated to reflect the latest SWIFTNet release and include more CSP information