



**Learning
Centre**

**Registered Partner Provider
(SWIFT Learning Center)
Partner ID Code: PTSANGFF**

Head Office

Suite D002, Garki Mall, Kabo Crescent,
Off Ahmadu Bello Way, Garki 2, FCT Abuja, Nigeria
☎ 0803 311 6245, 0812 314 2808
✉ hello@lemoninfotechser.com

Table of content

Pages

1. LEMON INFOTECH SERVICES PROFILE.....	1
1.1 About lemon Infotech.....	1
1.2 Vision.....	1
1.3 Mission.....	1
1.4 Our Values.....	1
1.5 Our Team	1
1.6 Our Clients	1
2. Training Overview.....	2
2.1 What we Offer	2
3. Course Information	3
3.1 Course Schedules.....	4
3.2 Course Description/Overview.....	5
3.2.1 Sanctions Screening Service over SWIFT	5
3.2.2 Capacity Building Bootcamp for Cyber Security.....	6
3.2.3 ISO 20022 Message Standards for Banks.....	8
3.2.4 SWIFT Audit Guidelines.....	9
3.2.5 Manage SWIFT Alliance Access/Entry.....	9
3.2.6 SWIFT System Housekeeping and Trouble Shooting Guidelines.....	10
3.2.7 Certification Programme.....	11
3.2.7.1 Certification Courses Offered.....	12
3.2.8 Registration Information.....	13
3.2.9 Mode of Payments.....	14
3.2.10 Course Certificates.....	14
4. Detachable Form.....	15

1. LEMON INFOTECH SERVICES PROFILE.

1.1 About Lemon Infotech.

Lemon Infotech is an emerging ICT Service Provider in Africa focusing to assist its customers to meet ever changing training service and ICT needs.

With growing changes in demand for faster, reliable, effective ICT System and training services, Lemon Infotech in collaboration with its first class global training and ICT partners is poised to provide its clients with excellent ICT solutions and training services, process optimization, control and compliance in order to enhance customer service delivery and achieve maximized returns on investments.

1.2 VISION:

To pioneer innovative ICT Solution and Training Services to aid national and global enterprises manage, control and secure their financial transaction and maximize profit.

1.3. MISSION:

To tailor portfolio of Technology Solutions to eliminate financial back- office transaction operations pain and security nightmares.

1.4. OUR VALUES:

- Respectfulness
- Passion for Technology that works
- Responsibility and Accountability
- Continuous Self development

1.5. OUR TEAM:

A team of passionate young people carefully recruited to create synergies and great relationships with our customers. Our technical team undergoes rigorous screening for technical and creative problem-solving to ensure a high quality of service delivery. They are continually trained on leading technology and skills to best serve our customers.

1.6 OUR CLIENTS:



2. TRAINING OVERVIEW.

Operational excellence is definitely a must-have in today's financial industry. Lemon Infotech, the Accredited SWIFT Partner Provider, (SWIFT Learning Center) in collaboration with SWIFT sc and its other Global Partner Training Providers are well positioned and committed to offer a best-in-class SWIFT and other financial industry training courses to help you perform more effectively and efficiently.

2.1. WHAT WE OFFER.

Lemon Infotech with its global training partners offer a range of learning solutions to suit your needs, delivery preference and knowledge level. Inspired by a strong focus on improving operational efficiency and cost effectiveness, we can respond to every evolving industry learning and solution challenges.

We draw on the 40 years' experience and the best pool of experts of the SWIFT Learning Center and other global Partners to design, develop, package and deliver training, and Certification programs that cover the latest and most comprehensive information on all SWIFT and other Partner products and services to meet your needs.

On quarterly basis, we add new courses to enhance our training portfolio. If you did not find what you are looking for in this quarter, please reach out to us to ensure that your training interest is catered for in the next quarter.

Are you interested in a particular topic? Do you want to mix one of our training with another topic? Do you want to tailor a specific topic to your specific training needs? Do you need a focused practice for your operations? Then, contact us at Lemon Infotech Services, and we shall be happy to plan your own training and solution destinations.

To stay on top of our latest Training News, please visit our website on:

www.lemoninfotechserv.com

Follows us:

Twitter: @lemoninfotech

Facebook: Lemon Infotech

We look forward to receiving your training request and other solutions needs.



3 Course Information

SWIFT TRAINING COURSES 2020.
COURSE PRICES AND REGISTRATION INFORMATION

3.1 COURSE SHEDULES

DATE	COURSE	LOCATION	PRICE
23 - 24 March, 2020	<ul style="list-style-type: none"> Sanctions Screening Service Over SWIFT 	Lagos	N470, 000.00
25 - 26 March, 2020	<ul style="list-style-type: none"> Capacity Building for Cyber Security 	Lagos	N470, 000.00
SECOND QUARTER TRAINING PROGRAM			
15 – 16 June, 2020	<ul style="list-style-type: none"> ISO 20022 Message Standards for Banks 	Lagos	N470, 000.00
17– 18 June, 2020	<ul style="list-style-type: none"> SWIFT Audit Guide Lines. 	Lagos	N470, 000.00
THIRD QUARTER TRAINING PROGRAM			
21 – 22 Sept, 2020	<ul style="list-style-type: none"> Manage Alliance Access/Entry 	Lagos	N470, 000.00
23 rd Sept, 2020	<ul style="list-style-type: none"> Certification Programme (On Request) 	Lagos	
23 - 24 Nov, 2020	<ul style="list-style-type: none"> SWIFT System Housekeeping and Troubleshooting Guidelines 	Lagos	N470, 000.00

3.2 COURSE DESCRIPTION/OVERVIEW

3.2.1 SANCTIONS SCREENING SERVICE OVER SWIFT

NON – COMPLIANCE CAN LEAD TO COSTLY FINES AND REPUTATIONAL DAMAGES

Sanctions are important tools of governance in the global financial industry. Most countries have used sanctions or had sanction placed against them or their citizens.

States increasingly use sanctions to fight economically, rather than physically, and as such, sanctions have become common tools in foreign relations, peacekeeping and conflict resolutions. Given their prevalence, everybody in the financial industry should have a good understanding of what sanctions are, how they work, why they are used, key components of Sanctions Screening, what is needed to access the service, how the Screening engine interact financial messages, and the price of non-compliance.

COURSE CONTENT:

- Fundamentals of Sanctions Screening
- Screening Capabilities
- Technical Administrative Tasks
 - o Activate Tokens
 - o Access the Portal
 - o Create Sanctions Screening Users (with sanctions screening Administrators).
- Routing Rules of MT019
- Sanctions Screening User Interface
- Alert Investigations
- Sanction Screening Administration
 - o Message Scope
 - o List Management (Public and Private)
 - o False Positive Reduction (Hit Reducing rules and Exceptions)
- Reporting
- Good Practices of using Sanctions Screening

COURSE AIM AND OBJECTIVE:

- Describe the Sanctions Screening Service
- Discover how the Compliance Officer manages filter configurations such as Sanction Lists, Message Types and Hit Rate from the Sanction Screening Admin Menu.
- Describe how to configure Sanction Screening according to your organization's compliance policy.
- Provides suggestions on how develop Sanction Screening Workflow for your organization.
- Explain how to effectively reduce your Hit Rate for faster payments receipt and delivery to and from your correspondents banks.
- Avoid Fines and Reputational Damages.

3.2.2 CAPACITY BUILDING BOOTCAMP FOR CYBER SECURITY (2 DAYS)

“A well-Prepared Staff on the nuisances of Cybersecurity Threats and best practices is often your bank's first line of defense”

There has been a significant evolution in the cyber threat facing the global financial industry over the last 5 years as adversaries have advanced their knowledge. They deploy increasingly sophisticated means of circumventing individual controls within the users' local environments, and probe further into their systems to execute well-planned and finally orchestrated attacks.

The groups behind these attacks are deploying ever more creative techniques to access users' critical assets. These include gaining Administrative rights for operating systems, manipulating software in memory, and tampering with legitimate functionality to bypass two-factor authentication.

It is now clear that the adversaries are prepared to invest considerable time in planning and preparing for attacks. The determination, patience and cunning the attackers are demonstrating make it more imperative than ever, that customers rapidly deploy and maintain all basic cyber hygiene tools and measures, comprehensively adhere to recommended security controls, and incorporate all the elements set out in SWIFT's Customer Security Programme.

There is no single solution, silver bullet or one-time implementation that will protect this complex threat-stream. It must be understood that cybersecurity is a continuous process rather than a static end state, no system can be assumed infallible, or immune to attack.

Less cyber-mature and smaller financial organizations deserve special attention but have been neglected so far. Many of the latter are particularly vulnerable, constrained by fewer resources, smaller staff, and often less experience. In 2018, 58% of the overall victims of cyberattacks were small businesses. Some reports suggest that credit unions and banks with less than \$35 million in assets account for the majority of hacking and malware breaches in the financial sector. Moreover, incidents dating back to 2016 suggest that some threat actors specifically, target financial organizations in the Global South and low-income countries.

It is against this background that in 2017, the G20 Finance Ministers and Central Bank Governors warned that the malicious use of Information and Communication Technologies could undermine security and confidence and endanger financial stability. These concerns have led to a flurry of regulatory and policy activity in recent years at both the international and national levels from the Financial Stability Board to the IMF, CPMI, and IOSCO as well as the EU, India, China, Singapore, and the US and from the industry side, from SWIFT's Customer Security Program to FS-ISAC and Sheltered Harbor.

COURSE CONTENT:

The content below is designed to correlate with the SWIFT Customer Security Framework and ISO/IEC 27002 and ISO 27035 to aid the fight against the global cyberattack

- Payment System Environment Protection
- Operating System Privileged Account Control
- Internal Data Flow Security
- Security updates
- System Hardening
- Operator Session Confidentiality and Integrity
- Vulnerability Scanning
- Physical Security
- Password Policy
- Multi-Factor Authentication
- Logical Access Control
- Token Management
- Physical and logical Password Storage
- Malware Protection
- Software Integrity
- Database Integrity
- Logging and Monitoring
- Cyber Incidence Response Planning
- Security Training and Awareness
- Virtualization Platform Protection
- Back-Office Data Flow Security
- External Transmission Data Protection
- Critical Activity Outsourcing
- Transaction Business Controls
- Application Hardening
- Intrusion Detection
- Penetration Testing
- Scenario Risk Assessment.

COURSE AIM AND OBJECTIVE:

The course aims to educate financial institutions on how to prevent or minimize undesirable and potentially fraudulent business consequences:

- Unauthorized sending or modification of financial messages.
- Processing of altered or unauthorized SWIFT inbound transactions messages
- Confidentiality breach (business data, computer systems, or operational details).

3.2. 3 : ISO 20022 MESSAGE STANDARDS FOR BANKS

Quality Data means Quality Payments.

The ISO 20022 is an increasingly established global language for payments messaging. It creates a common language and model for payments data. ISO 20022 significantly improves the quality of data across the payments eco-system.

ISO 20022, is single standard that covers all business domains and end-to-end business processes, facilitates the creation of new services and enhanced straight-through processing. It uses modern, mainstream XML technology which is well supported and which facilitates efficient integration.

The new ISO 20022 messages, compliant with agreed market practice, will be live on SWIFT in November 2021. After a period of four years of co-existence, the corresponding legacy SWIFT MT messages will be decommissioned on the SWIFT platform.

Almost 200 markets infrastructure driven initiatives are either already implementing ISO 20022 or are considering adopting the standard for payments and securities transformation projects.

COURSE CONTENT:

Focus:

- ISO 20022: Standards business modelling
- Representation syntax (MXL)
- SWIFT Messaging: Naming, Transportation, Extensions, Validation mechanism
- ISO 20022 in practice: Implementation and collaboration overview.
- Implementing ISO 20022: Project toolkit
- My Standards Demo (Standards, Base Libraries and Portal.
- Overview of integration solution for translation needs.

COURSE AIM AND OBJECTIVE:

- Understand ISO 20022 and the solution SWIFT has designed to help implement it.
- Get an overview of the different mapping and possibilities.
- Demonstrate various tools and resources developed for ISO purposes
- Prepare you for adoption.

3.2.4. SWIFT AUDIT GUIDELINES:

The Course describes how to get familiar with the profiles of the people who manage the security at your local infrastructure connected to SWIFT and with the tools and interfaces they use. Explains the operational risks and how to analyze permissions and activity logs.

COURSE CONTENT:

Focus:

Will focus on various checklists and exercises on data analysis practice for guidance on the topics below:

- Overview of SWIFT
- SWIFT Customer Security Controls Frameworks
- PKI Certificates HSMs
- Risk analysis in SWIFTNet and the SWIFT interfaces
- Integrity, filtering and other security controls
- Audit trails
- Archive, backup and business continuity planning
- SWIFT.com

AIM AND OBJECTIVE:

- Explain how SWIFT operates within and outside the user local environment with its tools and interfaces.
- To get familiar with the roles and responsibilities of people that manage the security of the local infrastructure connected to SWIFT.
- Explain operational risks and how to analyze them.

3.2.5. MANAGE SWIFT ALLIANCE ACCESS/ENTRY.

The Course introduces high level overview of the server and its clients, and the “views” to manage the Alliance Access.

COURSE CONTENT:

Focus:

- Updates, installation of patches, message syntax tables and BIC files.
- User Management and Security Parameters-profiles, users, passwords and security parameters.
- Alliance Gateway Connectivity: configuring Alliance Gateway Connections, Configuring Local Terminal connections as well as emission and inception profiles.
- Message Partners: connectivity of Alliance with external applications and printers
- Routing: defining routing rules in Alliance Access
- Message Searching and Reporting: using advance searching functions and reporting
- Archive and back-up procedures
- Scheduling and Calendar
- System Parameters and Event Log: how to change parameters and how to activate or de-activate alarms
- Using the Monitoring GUI supervising the new monitoring elements which are only available through Alliance Web Platform as well as using the new multi-instance monitoring tool

AIM AND OBJECTIVE

- Get most out of the Alliance Access system using this hands-on course
- Learn how to use the features and functionalities of Alliance Access; monitoring tools for supervision and control of different Alliance Access elements
- Ensure a hitch free running messaging interface
- Performance of hands-on exercise on the Alliance Access

3.2.6. SWIFT SYSTEM HOUSEKEEPING AND TROUBLE SHOOTING GUIDELINES.

The Course is designed to introduce the System Administrators, being responsible for the day-to-day operations in the local infrastructure connected to SWIFT and providers of first line technical support, on how to avoid system failure and assess the associated risks with it, in order to ensure a healthy SWIFT infrastructure.

COURSE CONTENT.

- SWIFT infrastructure overview
- Components that fit together to connect to SWIFT
- Purpose of SWIFT infrastructure
- Reason for failure
- Risk behind incomplete housekeeping
- Recommended housekeeping activities for Alliance Web Platform, Alliance Access, Alliance Gateway, SNL, HSM, PKI and VPN (AVLL)

AIM AND OBJECTIVE:

- Learn how to keep system healthy
- Understand what happens if housekeeping tasks are not done periodically
- Learn the most important preventive housekeeping activities to be able to avoid failure
- Learn how to assess the associated risks with non- performance of housekeeping
- Ensure a healthy SWIFT infrastructure
- Independent diagnosis
- Improve resolution time
- Reduction of business impact
- Ensure business continuity

3.2.7 CERTIFICATION PROGRAMME

How do you ensure your team has the right SWIFT SKILLS?

Our Lemon Infotech Service Training Program ensures that the Certification Programme builds and validates SWIFT expertise in critical business areas, giving you confidence in your own competencies and that of your team.

This is achieved through SWIFT experts and our team who are highly skilled, boosting reputation in the eyes of your management, overseers and customers.

How does it work?

In order to gain a certification, candidates must pass a formal proctored exam which include a product and service-specific questions as well as situational scenarios. Furthermore:

- Each track has clearly defined learning objectives
- Exams take place under controlled conditions
- Certifications are valid for a limited period to ensure skills remain current

How to become a SWIFT Certified Expert?

- Select your preferred certification track
- Review the certification scope to ensure you meet the required competencies
- Select your preferred delivery option:
 - ★ SWIFT-proctored certification combined with a tailored learning session.
 - Place an e-order on swift.com
 - ★ Customer-proctored exam that can be organized at your best convenience
 - Contact Lemon Infotech Services Ltd
 - ★ Mobile- 234 (0) 8033116245
 - ★ Email - gladan@lemoninfotechserv.com

3.2.7.1 CERTIFICATION COURSES OFFERED

a) ALLIANCE ACCESS ADMINISTRATOR CERTIFICATION EXAM.

Individuals who pass this certification exam have a deep knowledge of the administration of Alliance Access 7.2

Topics to be qualified on include:

- General knowledge of Alliance Access
- Upgrades and Updates
- Security
- Message Partners
- Routing
- Message Searching and Reporting
- Archive and Back up
- Scheduling and Calendar
- System Parameter and Event Log
- Monitoring

b). SWIFTNet SECURITY OFFICER CERTIFICATION EXAM.

Individuals who pass the certification exam understand the responsibilities and tasks required of a designated Security Officer in their organization.

Topics to be qualified on include:

- SWIFTNet Security Officer Environment
- Certificate Management
- Connectivity and Security
- Monitoring
- Online Operations Manager
- Routing Rules and Reporting
- RBAC Roles
- Secure Channel
- SWIFTNet Naming
- Security Officer Tasks
- SWIFTNet PKI

3.2.8 REGISTRATION INFORMATION

(a) COURSE REGISTRATION:

CONTACT:

Mr. G.M. Ladan

Email: gladan@lemoninfotechserv.com

Mobile: +234 (0) 8033116245

(b) TERMS AND CONDITIONS:

REGISTRATION POLICY:

- All participants attending the SWIFT Courses must obtain their own mySWIFT and SWIFTSmart Account before they can attend training and undertake a Certification Exam. A template to that effect will be sent to the prospective participants, four (4) weeks before the training dates.
- Cancellations- Must be received two (2) weeks before the commencement of the training.
- Cancellations received after two (2) weeks will attract 5% charges.
- Sign and detach the attached detachable Form and forward with your registered course / nominees to 3.2.9 (a) above.
- The Date and Location are subject to changes and you would be adequately notified in advance in advance by emails, text messages or calls in case of any changes

3.2.9 MODE OF PAYMENTS:

(a) Invoices:

To be issued immediately after registration

(b) Payments:

- ➔ Bank transfers (Accounts details will be indicated on invoice.
- ➔ Bank Draft.

Please Note: **Payments must be made before attendance.**

3.2.10 COURSE CERTIFICATES.

(a) ATTENDANCE CERTIFICATES:

To be issued by Lemon Infotech Services Ltd.

(b) CERTIFICATION EXAM:

To be issued by SWIFT.

4. Detachable Signature Form

For Institution:

Name: _____

Title: _____

Signature: _____

Date: _____

For Lemon Infotech Services Ltd

Name: _____

Title: _____

Signature: _____

Date: _____



INFOTECH SERVICES LIMITED



Learning
Centre

Registered Partner Provider
(SWIFT Learning Center)
Partner Code: PTSANGFF

Head Office

Suite D002, Garki Mall, Kabo Crescent,
Off Ahmadu Bello Way, Garki 2, FCT Abuja, Nigeria

☎ 0803 311 6245, 0812 314 2808

✉ hello@lemoninfotechser.com