This page intentionally left blank

SWIFT Infrastructure Audit Checklist/Program

By

Nwabueze Ohia

Editor: Nwabueze Ohia
Designer: Nwabueze Ohia

Notices

Knowledge and best practices in the field of information and technology security are constantly evolving. As new risk and vulnerabilities emerge, changes in research methods and broader experiences are required to contain the threats to system and human security. It is therefore expedient for professional practices to rise to the challenges and threats pose by information security risk and vulnerabilities.

Practitioners and researchers in this industry must always rely on strong personal judgment and experience in evaluating and applying information and methods being acquired from this book while also exercising professional due care and caution to ensure their safety and those of others, as well as parties for whom their own professional responsibility.

To the fullest extent of the law, neither the Publisher nor the author(s), contributors, or editors, assume any responsibility for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, procedures, products, instructions, or ideas contained in the material herein.

For information on all Oxley Technologies Inc. publications and materials, visit our web site at http://oxleyconsults.com.ng/

Your feedback is invaluable to us

If you recently bought this book, we would love to hear from you! You can write a review on the online store where you purchased this book) about your last order! If you bought this book from our website at http://oxleyconsults.com.ng/, we will appreciate if you leave a review on our website! We will love to hear real client experiences and feedback as part of our continual service improvement process.

Once you have submitted your review, send us an email at info@oxleyconsults.com.ng with the link to your review so we can properly thank you/appreciate your feedback.

Table of Content

About the Author

A Certified Information Systems Auditor (CISA), PECB certified Lead Auditor in ISO 27001 (Information Security Management System), ISO 22301 (Business Continuity Management System), ISO 20000 (IT Service Management System) and Lead Cyber Security Manager (ISO 27032), Nwabueze Ohia is a seasoned Information Assurance and Cyber Security professional/expert with over 12 years working experience in consulting and full time employment. He has worked in the banking sector in Nigeria as IT auditor and information security practitioner with experience spanning information systems audit and assurance, information/cyber security, technical infrastructure security/assurance, system controls analyst, IT risk analyst, data analyst and consultant. He is an expert in the development of audit work programs, checklists and risk assessment template that conform to Institute of Internal Auditors (IIA) standard, which practitioners has found useful in the discharge of their assurance functions. With his rich knowledge of the financial services sector and underlining security/controls required of systems and IT infrastructure in the sector, his eBooks, educational and professional materials, which are result oriented and tailored towards addressing information security issues have assisted practitioners within Nigeria, Sub-Sahara Africa and beyond in addressing risk in the ever changing and dynamic control environment. Beyond the financial services sector, practitioners in other industries such as insurance, telecommunication, web hosting, Internet service providers, SaaS, cloud service provider, distribution & supply chain management, shipping, oil & gas, etc., have leveraged on materials produced by Nwabueze to excel in their endeavors.

Nwabueze Ohia has written several educational and professional materials in the field of information assurance, information/cyber security and technical infrastructures, which are published on his website (http://oxleyconsults.com.ng). In addition, he has four books to his credit, which he self-published on Amazon Kindle Book store as well as other ebook platforms across the globe. His wealth of experience in information assurance and cyber security consulting as well as working in financial service sector are brought to bear on all his published materials/eBooks as an experience professional with practical/hands-on perspective. He holds a Higher National Diploma (HND) in Electrical/Electronics Engineering (Telecommunications) from Federal Polytechnic Nekede Owerri, a Bachelor of Technology (B. Tech) degree in Information Management Technology (IMT) and recently completed Master of Science Degree (MSc) in Information Management Technology (IMT) from Federal University of Technology Owerri, Imo State. This is in addition to series of professional/technical training courses he has attended in the course of his career, which endorsing him as a subject matter expert in his chosen profession.

Nwabueze Ohia is passionate about giving back to the internet and the knowledgebase of his chosen profession, having greatly been enriched by same, which he has demonstrated through several writeups, articles and professional papers published on his website for other to read and be enriched including guest posting on other professional web platforms. He finds joy and fulfillment in extending helping hands to the needy and the downtrodden of our society. His hobbies are traveling around the world, soccer, lawn tennis and above all, web application development/programming. Born in 1983 to Nigerian parents from the Eastern part of the country, he is happily married with a daughter.

This page intentionally left blank

Preface

By Nwabueze Ohia

The SWIFT network provides a platform for participating financial institutions to exchange financial transaction information/messages that enables international payment in a reliable, secure and standardized manner. To do this, each participating financial institution can be identified on the SWIFT platform with Business Identifier Codes (BICs) also known as "SWIFT code".

Given the volume of transactions that go through SWIFT network on daily basis, which has been estimated to be about 15 million with value in hundreds of billions of dollars (USD), the need to ensure end-to-end transaction and data exchange security on SWIFT platform cannot be overemphasized. With growing and worrisome cyber attacks that were recorded on SWIFT network in the past, particularly in 2016, SWIFT issued a new Customer Security Control Framework (CSCF) program that provided control frameworks for securing SWIFT local infrastructure and operating environment by identifying 22 mandatory and 9 advisory/optional controls (CSCF Version 2021), which participating customers worldwide put at over 11,000 need to comply with and attest to for continued participation in the SWIFT global transaction messaging network.

The control framework was built around 3 objectives, which are; Secure Operating Environment; Know and Limit Access; and Detect and Respond to incidents with 8 core principle that gave rise to 31 security controls (22 mandatory and 9 optional/advisory) as highlighted below.

1. Restrict Internet Access & Protect Critical Systems from General IT Environment

1.1 SWIFT Environment Protection (Mandatory)

1.2 Operating System Privileged Account Control (Mandatory)

1.3 Virtualization Platform Protection (Mandatory)

1.4A Restrict Internet Access (Advisory)

2. Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security (Mandatory)

2.2 Security Updates (Mandatory)

2.3 System Hardening (Mandatory)

2.4A Back-Office Data Flow Security (Advisory)

2.5A External Transmission Data Protection Security (Advisory)

While the new Customer Security Program (CSP) provided elaborate details on how to implement the 16 mandatory and 11 advisory controls to ensure security compliance to the expectation of SWIFT, risk assurance practitioners (IT Auditors, Cyber/Information Security Analysts, System Control Analysts, IT Risk Analysts) are still finding it difficult to provide assurance on the effectiveness and adequacy of stipulated controls implemented by the business based our interactions and engagements with industry leaders and stakeholders. In other words, there are still control testing knowledge gaps amongst those with security assurance responsibilities on SWIFT infrastructure and operating environment. Hence, the need for this practical and result oriented audit program/checklist put together to help practitioners in bridging those skill gaps.

The SWIFT infrastructure audit program/checklist provided practical steps of auditing the SWIFT infrastructures and operating environment along the lines of the newly issues Customer Security Program with the sole objective of complying with the requirements of the framework by testing the effectiveness and adequacy of the 16 mandatory and 11 optional controls. The book provided risk assurance practitioners with practical test procedures to follow, things to look out for, evidence/artifacts required to validate control effectiveness and security of the SWIFT local infrastructure and operating environment.

If you are an Auditor, Information Security Analyst, Risk Officer, Security Manager or System Control Analyst looking to carry out self-assessment, audit or security review of your SWIFT local infrastructure and operating environment in readiness for an external assessment or audit, this book is your best guide through what needs to be done to beyond passing your assessment, ensure security of your SWIFT infrastructure. With the guide provided in this book, you can comfortably/independently conduct self-assessment or audit of your SWIFT Infrastructure and operating environment with little or no external assistance.