This page intentionally left blank

Risk Assessment Program/Checklist for Information Security Management System (ISMS)

(ISO/IEC 27001:2013)

By

Nwabueze Ohia

Editor: Nwabueze Ohia
Designer: Nwabueze Ohia

Permissions may be sought directly from Oxley Technologies Inc.
Phone number: +234(0)803 757 4700; email: info@oxleyconsults.com.ng.
Alternatively, you can submit your request online by visiting the Oxley Technologies Inc. website at http://oxleyconsults.com.ng/contact-us/, and we will get back to you.

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.

Booking

For trainings and capacity building sessions, conferences/seminars and public speaking opportunities as well as consulting engagements on subjects/topics/areas covered in this book or others books by the author, you can contact Nwabueze Ohia directly on phone number +234-8037574700 or email address nwabueze.ohia@oxleyconsults.com.ng for further discussions.

For full list of trainings offered by the author, visiting http://oxleyconsults.com.ng/training/

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 14 years working experience in consulting and full-time employment. He has worked in the banking sector in Nigeria as IT Security 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 round 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 ISO/IEC 27001 is an international standard that was put in place to provide minimum requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system (ISMS). Every organization wishing to comply and be certified to the ISO/IEC 27001 standard adopt an implementation strategy for its ISMS based on its needs and objectives, organizational processes, structure and security requirements. The primary objectives of establishing, implementing, maintaining and continually improving the ISMS within an organization is to preserve the confidentiality integrity and availability of its information assets through the application of risk management process and providing assurance to stakeholders on risk management adequacy.

To be effective, organization seeking to comply with ISO/IEC 27001 standard must integrate its information security management system with the organization's processes and overall management structures by ensuring that information security is considered and embedded in processes, information systems and control design. Regulatory agencies across several industries including financial services, telecommunications, insurance, energy, manufacturing, business services and consulting have mandated the implementation and compliance of ISO/IEC 27001 standard for practitioners within its IT Standards Blueprint. The objective is to ensure continual improvement within an organization by determining whether processes within the scope of the its ISMS conforms to the organization's own requirements for ISMS as well as the control requirements of the ISO 27001 standard.

This book is a do-it-yourself risk assessment guide for the IT audit & risk assurance professionals who perform risk assessment review of ISO/IEC 27001 information security management system. It provides a detailed step by step guide on how to perform risk assessment of the ISO/IEC 27001 management system to ensure compliance with the ISO/IEC 27001 standard as well as organization's own requirement for ISMS.

It serves as a risk assessment program/checklist for IT Assurance practitioners (including IT auditors and IT risk analyst) and ISMS Managers with details of procedures to be performed to confirm adequacy of risk management and compliance with the requirements of the ISO 27001 management and annexure control clauses. It provides the reader with control objectives, description of the ISO/IEC 27001 management and annexure control clauses, reasons for selection of controls, evidence to be used for decision on control adequacy, responsible persons, ampong others. The risk assessment program/checklist can easily be

integrated with popular audit management software such as teammatessolutions or MKinsight field audit.

Intended for organizations desirous of building its information security management system to conform to ISO/IEC 27001 standard. ISO/IEC 27001 Lead Auditors (LA) and Lead Implementer (LI) will find this book very useful the continuous review of their ISMS and ensuring that they pass the certification and surveillance audits by external auditors. Below is a sample page of the database security audit checklist/program. For full access to the document, you can subscribe to our membership plan or purchase the book by click the Buy Now or Add to Cart button below.