This page intentionally left blank

Risk Assessment Checklist/Program for Email (Exchange Server) and Active Directory (AD) Infrastructure

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 Contents

About the Author ---------- 7
Preface by Nwabueze Ohia ---------- 9

Main Section Risk Assessment Checklist/Program for Email (Exchange Server) and Active Directory (AD) Infrastructure

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 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

Microsoft Active Directory infrastructure is a system that provides single sign on (SSO) functionality for Windows systems as well as other unrelated platforms. It uses Lightweight Directory Access Protocol (LDAP) for querying and modifying items in the directory service while the Active Directory (AD) is basically the directory database. Given the wide acceptance of Windows systems by most businesses and corporations around the world, the Active Directory infrastructure has become one of the most deployed and used LDAP solutions worldwide. From providing authentication service across diverse systems and applications to enforcing group policies across enterprise systems, the AD infrastructure is critical to enterprise systems security and service delivery.

As important as the Active Directory (Domain Controller) infrastructure is to the business, there are risks that are inherent in its usage, which if not identified and adequately remediated could lead to serious security issues within the organization. This is couple with the threat of abuse or misuse of the system by operators and users. Given that the active Directory infrastructure provides authentication service to Email systems such as Microsoft Exchange Server, it is important not to look at both systems in isolation. The risk associated with AD and Exchange infrastructure would vary with organizations and largely depends on how the infrastructures were deployed. As such, it is important that personnel with security oversight responsibilities on the AD and Exchange infrastructures put in context organization's uniqueness in terms of information security policies, procedures, security baselines, regulatory and legal requirements while conducting their security assessment or reviews of these infrastructure to know how best to protect them.

This book is therefore a documentation of risks and vulnerabilities associated with Active Directory and Microsoft Exchange infrastructures, threats and threat agents that could exploit those weaknesses, their impact on the organization and actions required to mitigate the risks. It serves as a risk assessment checklist/guide for risk assurance practitioners (IT Risk Manager, Cyber/Information Security Analysts, Information Systems Auditors and Systems Control Analysts) and enable them understand as well as identify some of the risks inherent in the AD and Exchange infrastructure, implications/impact of such risks/vulnerabilities and ways

to mitigate them. The book is a risk assessment checklist/program guide for risk assurance practitioners and provides unique/rich database of vulnerabilities/risk, control lapses, process failures and substandard practices associated with Active Directory (Domain Controller) and Exchange Server infrastructure. The book also covers the following.

- Active Directory infrastructure security review.
- Group policy object.
- Exchange server (On-premise) security.
- Microsoft Azure service (AD and Exchange cloud).

Intended for organizations desirous of build a risk management program around their Windows infrastructures from the ground up or strengthen an existing one.

Below is a sample page of the Active Directory (AD) and Exchange infrastructure risk assessment checklist/program. For full access to the document, you can subscribe to our membership plan or purchase the book by click the Buy Now button below.