IT AUDIT
PROGRAM SERIES

DATABASE SECURITY AUDITING

How To Perform Security Audit of Your Oracle & Microssoft SQL Server Database Infrastructures

BY
NWABUEZE OHIA

This page intentionally left blank

Database Security Auditing

(How to Perform Security Audit of Oracle & Microsoft SQL Server Database)

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.

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
Preface by Nwabueze Ohia

Main Section Database Security Auditing (Oracle, Microsoft SQL Server & MySQL)

Section 1: Audit Program for Oracle Database Security (All versions)

Section 2: Audit Program for Microsoft SQL Server Security (All versions)

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 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 database is an integral part of every organization's information system and IT infrastructure. As a matter of fact, it is one of the major components of every application solution. Given its critical function of storing and retaining organizational data and business information, the security of the database cannot be overemphasized. To ensure security of business information and confidential customer data, an end-to-end security approach to application security are essential and same include security of the database. Where adequate controls are not put in place at the database level, organizational data and business information could be exposed to the risk of confidentiality, integrity and availability (CIA). Thus, it is important that investment is made in database security implementations, administration and monitoring.

To ensure that good security practices are put in place for the security of enterprise database systems, Information Risk Assurance and Cybersecurity practitioners who are saddle with the responsibility of database security should understand their roles in the process toward ensuring that the best security practices for enterprise database systems are adopted and enforced. While there are different database management systems/software in the marketplace to choose from, it is important that decisions on which database technology to use is made on the basis of business and security requirements of the organization. In doing this, the organization must adopt a security baseline for its database systems pivoted on its security requirements and operational standards. Thus, it behooves on the information security and IT risk assurance functions to provide assurance on the security of the database system. However, this cannot be achieved without granular understanding of the configurable security parameters of the database management system technologies in the marketplace.

This book is a do-it-yourself security assessment guide for the widely used database management system such as, Oracle and Microsoft SQL Server database systems. It provides a details explanation of all configurable security parameters in the mentioned database systems, their security implications and how they could be exploited to perform malicious attacks on the database when activated. This book will help Information Risk Assurance and Cybersecurity practitioners as well as Database Administrators to perform security assessment

review of their database infrastructure and to adopt the best security baseline that is most suitable for their organization. It provides a practical approach to reviewing database systems and outline test procedures to be performed that will validate the security or otherwise of the database.

It serves as a security audit program and risk assessment checklist for IT Assurance practitioners (e.g. IT Risk Analyst/Manager, Cyber/Information Security Analysts, Information Systems Auditors and Systems Control Analysts, CISO, etc.) and enable them understand as well as identify some security configurations that are built to the database infrastructure some of which are installed by default when setting up the database except exclusively turned off. Audit program/checklist can easily be integrated with popular audit management software such as teammatessolutions or MKinsight field audit.

Intended for organizations desirous of build a security baseline for their enterprise database management systems from the ground up or strengthen an existing one. 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.

This page intentionally left blank

Introduction

The database management system serves as a warehouse for organizational/business information, such as customer data, employee information, transaction data, health/medical information, public records, etc. The database system provides a structured approach to storing and retrieval of business data. To ensure confidentiality, integrity and availability of business data stored in the database, rules are defined in the database to control how data are accessed, used for business processing and archived for future use as well as retention. The rules configured in the database are for the security of organizational data and to ensure optimal usage, access and availability.

There are different types of architecture that can be used to deploy a database for optimal usage, which largely depends on business requirements, security considerations and availability requirements of concerned business data. Applications that run is a distributed network environment are basically designed to function in a 3-tier architecture consisting of the client-side (web or mobile client), the server-side (backend application) and the database (datastore). Application users that consume application services through the client-side (web or mobile interface) in most cases do not interact directly with the application database but do so through the server-side of the application (a.k.a. application server). This architecture ensures security of the database and information stored on it. However, for smaller applications where the client and server application sit within the same container, direct connection could be made to the database, which may not be recommended given the heightened risk of security breach. Although this architecture is dependent on the specifics of the systems being used and business requirements and are prevalent in desktop and workgroup applications.

Database configurations are what drive the functionality of the database. Every database management system has inbuilt configuration settings that is used to control data availability, accessibility, confidentiality, integrity, retainability and security of the database. These configurations can be categorized into the following functionalities.

1. Security

2. Availability
3. Performance
4. Scalability
5. Retention

The database management infrastructure when acquired come inbuilt with these configurations. However, their usage depends on the business and security requirements of the organization in question. Thus, it is not a good practice to install a database with all inbuilt configurations put to production at once. This could spell doom for the organization given its security implication. As such, it is best security practice to adopt configurations that best suit the organization's needs and requirements. To do this, organizations must define and adopt a minimum security baseline for its database, which is an operational guideline that outline configurations that will be turned on in production and those that will be turned off. As the name implies "baseline", it is only the minimum standard and not the maximum, as such, there is room to put in place additional parameters that best secures the database and ensure optimal performance of the database. Configurations should not be enabled arbitrarily. Only configurations that are required should be turned on while unused ones should be turned off until when required.

In determine the baseline for the database, organizations most consider the OEM's security documentations for the database system, the requirement of the application to run on the database as well as performance. In most case, the application running on top of the database determine or drive what the configurations of the database will be in terms of security and performance. As such, it is important to engage robustly with the application vendor to provide upfront all information and requirement for the database as well as other underlining infrastructures such as operation system platform the application and database will run on. These considerations are essential in building a functional and feasible security architecture for applications and their databases.

----------End of Sample Pages of This Book----------

For full access to all pages of this book, click "Add to Cart" button on top of this web page to purchase the book. A link will be provided and sent to you to download the book after successful payment.