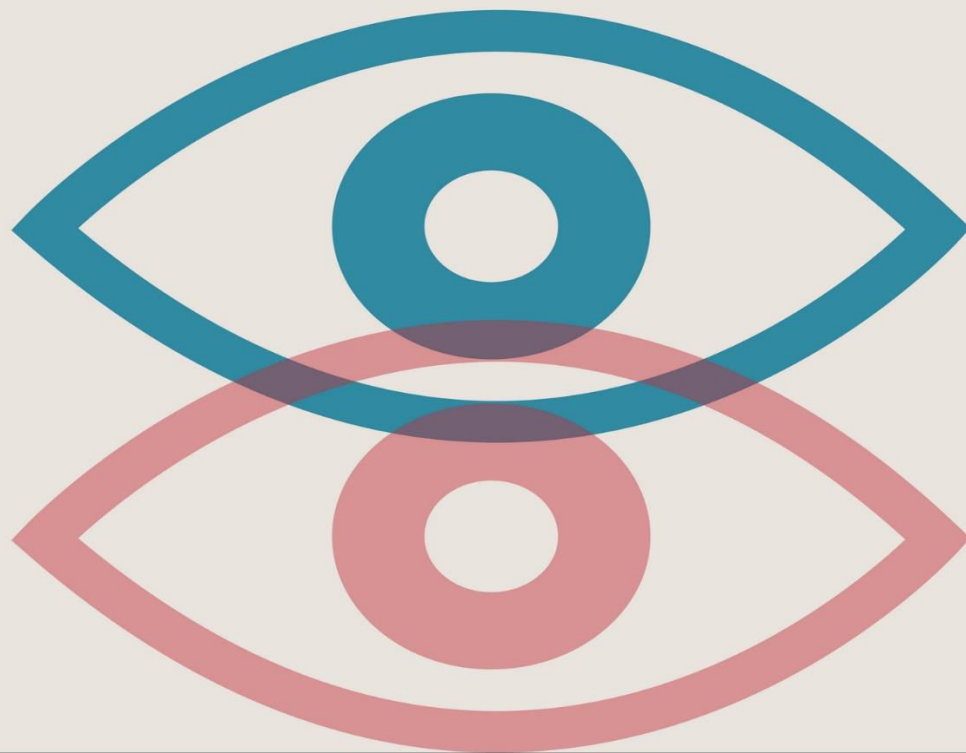


Auditing Your Information Systems and IT Infrastructure

BY NWABUEZE OHIA



Practical Audit Programs/Checklists for Internal Auditors

This page intentionally left blank

Auditing Your Information Systems and IT Infrastructure

Practical Audit Programs/Checklists for Internal Auditors

By

Nwabueze Ohia

Discover Other Titles by Nwabueze Ohia

1. Auditing your Payment Cards Processes, Systems and Applications: A Step by Step PCIDSS Compliant Audit Program
2. Auditing Your Windows Infrastructure, Intranet and Internet Security: A Practical Audit Program for IT Assurance Professionals
3. IT Infrastructure Risk & Vulnerability Library: A Consolidated Register of Operational and Technology Infrastructure Vulnerabilities for IT Assurance Professionals

Editor: Nwabueze Ohia
Designer: Nwabueze Ohia

Copyright © 2017 Nwabueze Ohia. All rights reserved

This Book is licensed for your personal enjoyment only. This Book may not be re-sold or given away to other people. If you would like to share this book with another person, please purchase an additional copy for each recipient. If you're reading this book and did not purchase it, or it was not purchased for your use only, then please return to your favourite Book retailer and purchase your own copy. Thank you for respecting the hard work of this author.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the copyright owner.

Permissions may be sought directly from the author on Phone number: +234(0)803 757 4700; email: info@oxleyconsults.com.ng. Alternatively, you may 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 owe 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/>**

This page intentionally left blank

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/>

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 amazon (or 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.

How does it work?

To post a review on Amazon, just log into your account and click on the Create Your Own Review button (under Customer Reviews) of the relevant product page. You can find examples of product reviews in Amazon. If you purchased from another outlets/online store, simply follow their procedures.

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.

CONTENTS AT A GLANCE

Part I	Audit Overview
Chapter 1	Effectiveness of the Internal Audit Function
Chapter 2	The Audit Process
Part II	IT Systems, Processes and Infrastructure Audit
Chapter 3	Audit of Data Centers
Chapter 4	Audit of Business Continuity and Disaster Recovery
Chapter 5	Audit of Business Process Re-engineering (BPR) and Automation)
Chapter 6	Audit of Governance of Enterprise IT
Chapter 7	Audit of Physical and Environment Security
Chapter 8	Audit of Windows Infrastructure, Intranet and Internet Security
Chapter 9	Audit of Financial Technology Applications and Payment Applications (Online Banking and Payment Apps)
Chapter 10	Audit of Unix and Linux Operating System Infrastructure
Chapter 11	Audit of Core Banking Applications (Finacle, Flexcube and Phoenix)
Chapter 12	Audit of Payment Cards (Debit, Credit & Prepaid) Processes, Systems and Applications – PCI DSS Compliance
Chapter 13	Audit of Employee Information System
Chapter 14	Audit of Perimeter Network Security
Chapter 15	Audit of Database Security
Chapter 16	Audit of Virtualized Infrastructure

TABLE OF CONTENTS

About the Author

Preface by Nwabueze Ohia

Part I	Audit Overview -----	21
Chapter 1	The Internal Audit Function -----	23
	Effectiveness of the Internal Audit Function -----	25
	The Mandate -----	27
	Consulting and Pre-Audit Planning Engagements -----	28
	Information Gathering -----	27
	Risk Assessment -----	28
	Business Pain Points Identification -----	29
	Resource Budgeting -----	29
	The IT Audit Team -----	30
	Composition -----	30
	Competence of IT Audit Team -----	31
	Data Preparation and Analysis -----	31
	Onsite and Offsite Activities -----	31
	Partnering with the Audit Client -----	32
Chapter 2	The Audit Process -----	34
	Planning -----	35
	Execution -----	35
	Reporting -----	36
	Grading/Rating -----	37
	Corrective Actions and Remediation -----	38
	Follow Up/Issue Tracking -----	38
	Determining the Audit Universe -----	39
	Determining the Audit Type -----	39
	Full Audit -----	40
	Spot-checks -----	40
	Follow Up Audit -----	40
	Investigation and Special Audit -----	40
	Effective auditing through audit automation (audit management software) ----	41

Part II	IT Systems, Processes and Infrastructure Audit -----	42
Chapter 3	Audit of Data Centers -----	46
	Data Center Audit Program -----	47
	Data Center Checklist -----	47
	Organization and Administration of the Data Center -----	47
	Environmental Controls -----	53
	Monitoring and Surveillance Controls -----	55
	Physical and Logical Access Controls to the Data Center -----	58
	Data Backup and Restoration -----	60
Chapter 4	Audit of Business Continuity and Disaster Recovery -----	62
	Audit Program for Business Continuity and Disaster Recovery Management -----	63
	Audit Checklist for Business Continuity and Disaster Recovery -----	64
	Business Continuity Readiness -----	64
	Disaster Recovery (DR) Site -----	68
	DR Data Center Controls -----	72
Chapter 5	Audit of Business Process Re-engineering (BPR) and Automation -----	75
	Business Process Re-engineering (BPR) Audit Program -----	76
	Business Process Re-engineering (BPR) Audit Checklist -----	77
	Procedures and Standards -----	77
	System Development -----	77
	System Testing -----	78
	Change Management -----	78
	Access Controls -----	79
	Documentation -----	80
	Code Review and Vulnerability Assessment/Management -----	82
Chapter 6	Audit of Governance of Enterprise IT -----	83
	IT Governance Basics -----	84
	Information Technology Governance and Strategic Planning ---	85
	Information Systems Strategy -----	86
	Information Security Management -----	86
	Information Risk Management -----	87

	Performance Management -----	87
	IT Governance Audit Program -----	88
	IT Governance Audit Checklist -----	89
Chapter 7	Audit of Physical and Environment Security -----	90
	Physical and Environment Security Audit Program -----	91
	Physical and Environment Security Audit Checklist -----	92
	Physical Security Administration (Premises and Restricted Areas) Entry Control Systems (Biometric, Smartcard and Locks) Management -----	92
	Security Surveillance (CCTV System) -----	95
	Safety Procedures and Environmental Controls -----	96
	-----	103
Chapter 8	Audit of Windows Infrastructure, Intranet and Internet Security -----	109
	Audit Program of Windows Infrastructure, Intranet and Internet Security -----	110
	Audit Checklist of Windows Infrastructure, Intranet and Internet Security -----	112
	Policies, Procedures and Administration -----	112
	Change Management -----	113
	Security Administration -----	115
	Log Management -----	120
	Logical Access Controls -----	120
	Business Continuity, Disaster Recovery and Backups -----	124
	Vulnerability Management -----	126
	Active Directory/Domain Controller Server Controls -----	128
	Endpoint Management and Data Loss Prevention (DLP) -----	138
Chapter 9	Audit of Financial Technology and Electronic Payment Applications (Online Banking and Payment Apps) -----	144
	Audit Program for Audit of Financial Technology and Electronic Payment Applications -----	145
	Audit Checklist for Audit of Financial Technology and Electronic Payment Applications -----	147
	Policies and Procedures -----	147
	Review of Third Party Service Level Agreements (SLAs) -----	147

	Logical Access Controls -----	147
	Application Controls -----	151
	Database Controls -----	153
	Operating System Controls -----	156
	Redundancy and Data Backup -----	156
	Change Management -----	157
	Log Management -----	157
Chapter 10	Audit of Unix and Linux Operating System Infrastructure -----	158
	Audit Program for Unix and Linux Operating System Infrastructure -----	159
	Audit Checklist for Unix and Linux Operating System Infrastructure -----	160
	Organization and Administration -----	160
	Installation Audit -----	162
	Operating Policies and Procedures -----	162
	System and Security Administration -----	163
	Account Security (Logical Access Controls) -----	168
	Password Management Controls -----	169
	File Permission and Security Controls -----	171
	Network Security Controls -----	171
Chapter 11	Audit of Core Banking Applications (Finacle, Flexcube and Phoenix) -	173
	Audit Program for Core Banking Applications -----	174
	Audit Checklist for Core Banking Applications -----	175
	Policies and Standard Operating Procedure -----	175
	Segregation of Duties and Maker/Checker Controls -----	175
	Application Controls -----	176
	Change Management -----	181
	Business Continuity and Disaster Recovery -----	183
	Data Backup and Redundancy -----	184
	Security Administration -----	186
	User Access Management -----	189
	System Monitoring and Audit Trail -----	190
Chapter 12	Audit of Payment Cards (Debit, Credit & Prepaid) Processes, Systems and Applications – PCI DSS Compliance -----	192
	Audit Program for Payment Card Environment -----	193
	Audit Checklist for Payment Card Environment -----	195

	Organization and administration -----	195
	Application Controls -----	196
	Database Controls -----	199
	Redundancy and data backup -----	200
	Change Management -----	201
	Vendor Management -----	202
	Credit Card Portfolio Management -----	203
	Encryption Key Management -----	204
	Network Controls -----	209
	Vulnerability Assessment -----	212
	Operating System Controls -----	213
	Cards Operations, Personalization and Issuance (Debit and Credit) -----	215
Chapter 13	Audit of Employee/Human Resources Information Systems -----	220
	Audit Program for Employee/Human Resources Information System ---	221
	Audit Checklist for Employee/Human Resources Information System ---	222
	Onboarding and Exit Process -----	222
	Human Resources Organization and Administration -----	225
	Human Resources Application System (HR Software) -----	227
	Data Backup and Redundancy for HR Application -----	233
Chapter 14	Audit of Perimeter Network Security -----	234
	Audit Checklist for Perimeter Network Security -----	235
	Network Logical Access Controls -----	235
	Network Remote Access Controls -----	236
	Firewall Security Controls -----	238
Chapter 15	Audit of Database Security -----	244
	Oracle Database Audit Requirements -----	245
	Oracle Database Audit Checklist -----	246
	Microsoft SQL Server Database Audit Requirements -----	262
	Microsoft SQL Server Database Audit Checklist -----	263
Chapter 16	Audit of Virtualized Infrastructure -----	271
	Audit Checklist of Virtual Infrastructure -----	272
	Discover Other Titles By The Author -----	291

About the Author



A Certified Information Systems Auditor (CISA), Certified Lead Auditor for ISO 27001 (Information Security Management System), ISO 22301 (Business Continuity Management System), ISO 20000 (IT Service Management System) and ISO 27032 (Lead Cyber Security Manager), Nwabueze Ohia is a seasoned information risk assurance and cybersecurity expert with over 13 years' industry experience in IT consulting, IT audit, internal control/audit and information risk assurance. With bulk of his experience in the banking and financial institution space, Nwabueze have performed roles such as IS/IT Auditor, Information Security Analyst, IT Forensics/Fraud Investigator, IT Risk Analyst, System Control Analyst, among others, in the course of his professional life. His core strength/competences are in Information systems & technical Infrastructure auditing, IT risk assessment, cyber threat intelligence & analysis, security architecture & engineering (networks and operating systems), electronic fraud & forensic investigation, software engineering & web application development, data analytics and revenue assurance, among others.

Given his strong auditing and information risk assurance background, he has developed series of audit work programs, checklists, risk assessment templates and information security programs, which professionals have recognized as valuable resources for information risk and security assurance. This is due to their conformance to standards/frameworks issued by professional bodies such as institute of Internal Auditors (IIA), Information Systems & Control Association (ISACA), International Information System Security Certification Consortium (ISC²), National Institute for Standards & Technology (NIST Risk Management & Cybersecurity framework) and Center for Internet Security (CIS). His Books, articles, best practice guides and web content are hands-on (do-it-yourself guide) and have assisted practitioners within Nigeria, Sub-Sahara Africa and beyond in addressing information risk and security concerns in the ever changing and dynamic IT environment. Beyond the financial services sector, practitioners in other sectors such as insurance, telecommunication, web hosting, Internet service providers, SaaS, cloud service provider, distribution & supply chain management, shipping, oil & gas, have leveraged content produced by Nwabueze to excel in their endeavors.

Nwabueze Ohia is a seasoned trainer and public speaker and operate the website (<http://oxleyconsults.com.ng>) where all his books and materials are published. He has published four books to his credit, which are available on Amazon Kindle Book store as well as other major eBook reading and distribution platforms worldwide. 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.

Nwabueze Ohia is passionate about giving back to the society and the knowledgebase of his chosen profession, having greatly been enriched by same. He has demonstrated this passion through several writeups, articles, best practice guides and professional papers published via his website and other outlets. 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, tennis and web application development/programming. Born in 1983 to Nigerian parents from the Eastern part of the country, he is happily married with two children.

This page intentionally left blank

Preface

By Nwabueze Ohia

Assuring the Security of Your Information Systems and IT Infrastructures (IT Audit and Internal Audit)

This edition has been updated to cover virtually all areas of information systems and IT infrastructure. "*Auditing Your Information Systems and IT Infrastructure: Practical Audit Programs/Checklists for Internal Auditors*", serves as a reference handbook for IT Auditors and other IT assurance professionals on how to use latest IT auditing techniques and programs to provide assurance on the security of enterprise information systems and IT infrastructure. New chapters on perimeter network security, database security and virtualized infrastructure are included. The book describes leading practices in internal audit and how the internal audit/IT audit function can effectively meet stakeholders' expectations and add value the business while maintaining its independence. Details on how to conduct specific audits of IT processes, services, systems or infrastructures were provided with hands-on checklists and audit test procedures. The following areas of information systems, processes and IT infrastructures are covered.

- Leading practices in internal audit function
- Data center
- Business continuity management and disaster recovery management
- Business process re-engineering (BPR) and automation function
- IT governance and strategic planning
- Physical and environmental security
- Windows infrastructure, intranet and internet security
- Financial Technology (Fintech) and Electronic Payment Applications
- UNIX operating system infrastructure (IBM AIX & Oracle UNIX)
- Core banking application (Finacle, Flexcube and Phoenix)
- Payment card (debit, credit & prepaid) processes, systems and applications – PCIDSS Compliance
- Employee (Human Resources) Information Systems
- Perimeter Network Security
- Database security (Oracle and Microsoft SQL Server Database)
- Virtualized infrastructure

Intended for IT Auditors and other Assurance professionals that are desirous of improving their auditing skills or organizations that are performing risk and control self-assessment (RCSA) exercise from the ground up.

What You Will Learn and Benefit:

- Build or improve your auditing and control testing techniques/skills by knowing what to look out for and how to verify the existence and adequacy of controls.
- Acquire hands-on audit programs/checklists to be used for auditing your core IT systems and infrastructure, which can easily be applied in your environment.
- Prepare for and pass management system certification audits such as PCI-DSS, ISO 27001, ISO 2230, ISO 20000 and ISO 90001.
- Audit programs/checklists from this book can easily be integrated into standard audit software such as Teammates or MKInsight as they share similar templates.
- Expand the scope of your audit testing to cover more areas of concerns or risk exposures.
- Strengthen your organization's internal audit process and control testing, a benefit from an expanded risk/vulnerability register.
- Rejuvenate the risk management effective and information security program of your organization, having an improved perspective of inherent risk/vulnerabilities of your IT infrastructure as well as a robust and realistic vulnerability/risk register.
- Risk mitigate and treatment plan.

Who This Book Is For:

IT professionals moving into auditing field; new IT Audit Managers, Directors, Vice Presidents, and would-be Chief Audit Executives (CAEs) and Chief Information Security Officers (CISOs); Security Specialists from other disciplines moving into information risk and security assurance (e.g., former military security professionals, law enforcement professionals, physical security professionals); and information risk and security specialists (e.g. IT Security Managers, IT Risk Managers, IT Control Analyst, Security Engineers/Directors, CIOs, CTOs, COO).

This page intentionally left blank

PART 1

AUDIT OVERVIEW

Chapter 1 The Internal Audit Function
Chapter 2 The Audit Process

-----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.