ISACA®

Database Audit Program

Audit

CONTENTS

4 Database Audit Program
4 / Audit Subject
4 / Audit Objectives
5 / Audit Scope
5 / Business Impact and Risk
5 / Minimum Audit Skills
5 / Testing Steps
6 Acknowledgments

ABSTRACT

Databases are a core component of the technology stack currently driving businesses, with MySQL, Microsoft® SQL and Oracle® databases taking center stage. Despite widespread adoption, databases remain a prime target for malicious actors due to the intrinsic value of the business and personal data they store, process and transmit. Due to the critical nature of enterprise databases, auditors and cybersecurity professionals must strive to understand the risk associated with their operations and the need for controls to provide adequate security.

Accordingly, ISACA introduced its *Database Audit Program* to help audit departments provide necessary assurance over database deployments through targeted, platform-specific audit testing, practical guidance and native database management tool usage. The *Database Audit Program* is an educational resource that can prepare and upskill IT auditors and cybersecurity professionals with the database knowledge required to assess this essential technology.

Database Audit Program

In preparation for audits conducted using this *Database Audit Program*, three key documents are recommended for additional reading:

- *MySQL 8.0 Reference Manual*, Oracle, 2022[1]
- *Securing SQL Server 2019*, Microsoft, 2022[2]
- *Oracle® Database Security Guide 19c*, Oracle 2022[3]

These documents contain valuable background information specific to each technology covered in the *Database Audit Program* to help readers understand the underlying principles of database security and the key points of audit focus. The *Database Audit Program* does not aim to provide complete assurance over all possible implementation variants of database security for the covered technologies, but instead targets a prioritized, highly focused set of audit subjects with the goal of greatly reducing the attack surface of the database technology deployed by the enterprise.

Audit Subject

Enterprise database products such as MySQL 8.0.27, Microsoft® SQL 2019 and Oracle® 19c primarily consist of physical or virtual database hosts that are fully enabled by database engine software. Enterprises typically leverage database products to serve as the backend of web applications that conduct Internet and/or intranet-based data transactions with users. These systems are employed for a wide range of purposes, such as e-commerce; employee management; financial transaction processing; and data analysis, storage and retrieval. The *Database Audit Program*, which is provided as a separate Excel® file, presents detailed guidance to audit and cybersecurity personnel on a strategic and sequential approach to auditing the various components of an enterprise database deployment.

Audit Objectives

The objective of this *Database Audit Program* is to provide auditors with an evaluation framework useful for assessing the adequacy and effectiveness of the implemented controls, enabling the enterprise to take additional actions as required to strengthen the confidentiality, integrity and availability of database deployments. The evaluations consider the security controls from the following perspectives:

- **General database controls**—Applicable to any database product. General database controls cover evaluations of the database host, secure default configuration, data classification policy and enforcement, change management processes for databases, and several other areas.
- **MySQL 8.0.27 controls**—Cover product-specific evaluations of secure default configuration, user access management, database logging, auditing, encryption, change tracking, backup and recovery.
- **Microsoft® SQL controls**—Cover product-specific evaluations of secure default configuration, user access management, database logging, auditing, encryption, change tracking, backup and recovery.
- **Oracle® Database 19c controls**—Cover product-specific evaluations of secure default configuration, user access management, database logging, auditing, encryption, change tracking, backup and recovery.

Evaluation outcomes provide management with an assessment of the database control environment, indicating whether it is adequately designed and operationally secure, and whether there are any governance challenges and data-specific risk factors that could result in reputational, legal and/or material financial impacts. The outcomes also provide management with a holistic perspective on database technology, considering

[1] Axmark, D.; M. Widenius; *MySQL 8.0 Reference Manual: Including MySQL NDB Cluster 8.0*, Oracle, 27 May 2022, https://docs.oracle.com/cd/E17952_01/mysql-8.0-en/mysql-8.0-en.pdf

[2] To, V., et al; *Securing SQL Server*, Microsoft, 17 May 2021, https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server?view=sql-server-ver16

[3] Huey, P.; S. Jeloka; *Oracle® Database Security Guide 19c*, Oracle, May 2022, https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/

people, processes and technologies as a complete ecosystem.

Audit Scope

The *Database Audit Program* is organized into the following categories:

- General database controls
- MySQL 8.0.27
- Microsoft® SQL Server 2019
- Oracle® Database 19c

Business Impact and Risk

Database technologies must be carefully evaluated, properly configured, and effectively deployed and managed throughout the database lifecycle. Management must ensure that the use of database technologies supports business objectives in a secure and ethical manner. The use of database technologies commonly entails both potential risk and consequences, including:

- Public access to sensitive data through database engine misconfiguration or open access to database configurations
- Storage and transmission of data in cleartext or using unsecure, unencrypted configurations
- Gaps in security through enablement of unnecessary network or database engine features and services
- Poorly managed access policies or excessive permissions, granting individuals more rights than necessary to perform job duties
- Inadequate monitoring, logging and notification mechanisms that alert management to avoidable or undesired security events
- Insertion of and acceptance of malicious data or database inputs that jeopardize data confidentiality and integrity

Minimum Audit Skills

The IT audit professional must have an understanding of security, controls and technology processes. The auditor should also possess adequate functional and business knowledge to determine alignment with business strategies. Individuals performing this audit should verify that they have performed the required research to comprehend the nature of database technology and its associated risk.

Testing Steps

Refer to the accompanying spreadsheet file.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Adam Kohnke
CISA, CISSP, GPEN
XL Security Consultancy LLC
USA

Expert Reviewers

Kanan Aliyev
CISA, CRISC, CDPSE
Azerbaijan

Igumbor Ehiedu Daniel
CISA, CGEIT, CRISC, ACCA, CBCI, CFE, CISSP, GCIH
Nigeria

Shamik Kacker
CISM, CRISC, CDPSE, CCSK, CCSP, CISSP, ITIL Expert, TOGAF 9
USA

Muhammad Tariq Ahmed Khan
CISA, CISM, CDPSE, CDFE, CEH, CISSP, ISO 27001, ISO 22301, PMP
Saudi Arabia

Sylvia Lim
CISA, CRISC, CCSK, CISSP
USA

Michael Malcolm
CISA, CIA, CISSP, CRMA
Canada

Monica Siddalls
USA

Ceren Tosun
CISA, AWS CP, CCSK, CIA, ISO 27001 LA Luxembourg

Marilize van Schalkwyk
CISA, CISM, CIA
Namibia

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Former Chief Information Security Officer and Privacy Officer, United Nations Office for Project Services (UNOPS), Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd., Israel

Tracey Dedrick
ISACA Board Chair, 2020-2021

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

DISCLAIMER

ISACA has designed and created the *Database Audit Program* (the "Work") primarily as an educational resource for IT audit professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, IT audit professionals should apply their own professional judgments to the specific circumstances presented by the systems or information technology environment.

Reservation of Rights

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/database-audit-program

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

Database Audit Program
ISBN 978-1-60420-949-5