Database Logging And Auditing Framework

Integrigy offers a comprehensive suite of security and vulnerability services that include audit and risk assessments, strategic consulting, and design.

In Integrigy's experience, the implementation of database and application logging seldom exceeds meeting the needs of basic debugging. Most organizations do not know where to start or how to leverage the built-in auditing and logging features to satisfy their compliance and security requirements.

The Framework for database logging and auditing is a direct result of Integrigy's consulting experience and is equally useful to both those wanting to improve their capabilities as well as those just starting to implement logging and auditing. Our goal is to provide a clear explanation of the native auditing and logging features available, present an approach and strategy for using these features and a straight-forward configuration steps to implement the approach.

Integrigy's Framework is also specifically designed to help clients meet compliance and security standards such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), FISMA, and HIPAA. The foundation of the Framework is PCI DSS requirement 10.2.

To make it easy for clients to implement, the Framework has three maturity levels – which level a client starts at depends on the infrastructure and policies already in place.

The three levels are -

Level 1 – Enable baseline auditing and logging for application/ database and implement security monitoring and auditing alerts

Level 2 – Send audit and log data to a centralized logging solution outside the database such the Oracle Audit vault

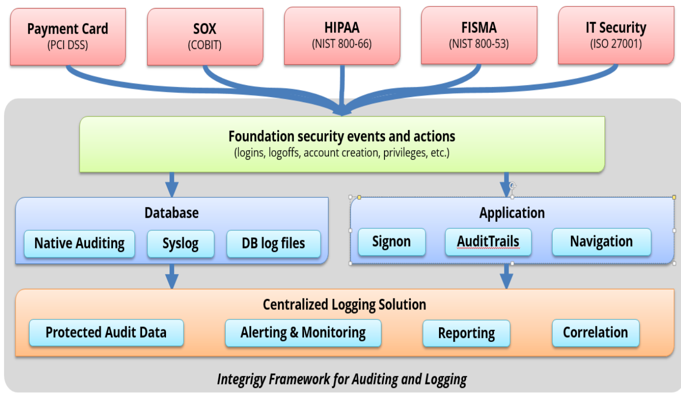
Level 3 – Extend logging to include functional logging and more complex alerting and monitoring

The foundation of the Framework is a set of fourteen (14) key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations. These events have been mapped to:

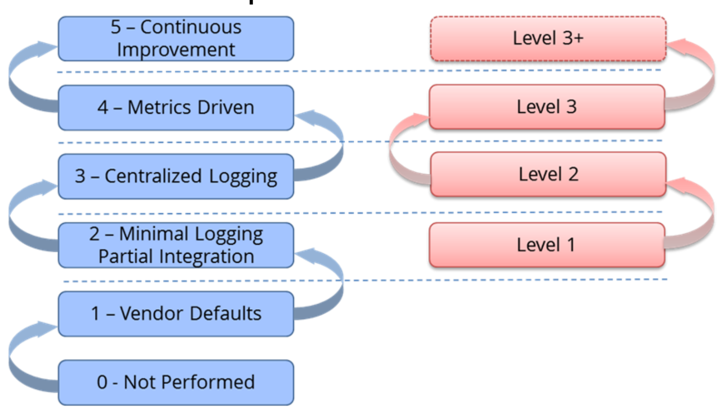
- PCI DSS
- SOX/COBIT
- HIPAA (NIST 800-066)
- IT Security (ISO 27001)
- FISMA (NIST 800-53)
- 21 CFR 11

The Integrigy Database Log and Audit Framework can be obtained from Integrigy's website at http://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

Framework



Implement in Three Phases



Common Maturity Model (CMM) ***Integrigy Framework***

14 Key Security Events	
E1 - Login	E8 - Modify role
E2 - Logoff	E9 - Grant/revoke user privileges
E3 - Unsuccessful login	E10 - Grant/revoke role privileges
E4 - Modify auth mechanisms	E11 - Privileged commands
E5 - Create user account	E12 - Modify audit and logging
E6 - Modify user account	E13 - Create, Modify or Delete object
E7 - Create role	E14 - Modify configuration settings

Integrigy Framework with the Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall

Oracle Audit Vault is aptly named; the Oracle Audit Vault and Database Firewall (AVDF) is a vault in which data about audit logs is placed. Oracle AVDF by itself does not generate audit data but utilizes the native database auditing. Before Oracle Audit Vault can be used, standard database auditing needs to be first enabled in the source databases. Once auditing is enabled in the source databases, AVDF collects the log and audit data using agents deployed on the source systems.

With the log and audit information collected, the Audit Vault can generate alerts and offers dozens of comprehensive standard reports built by and for auditors. This includes standard reports for PCI, HIPAA, SOX and GLBA compliance reporting. Oracle BI Publisher can also be used to edit and create new reports.

For Oracle databases, standard Oracle auditing is supported along with Fine Grained Auditing (FGA), PL/SQL stored procedure, and Oracle 12c Unified Auditing.

Integration from Oracle AVDF to SIEMs is supported through Syslog, and standard functionality includes integration with ArcSight. Integration with the BMC Remedy ticket system is also supported.

For more information on Oracle AVDF refer to Integrigy's whitepaper, "Integrigy Guide to the Oracle Audit Vault", http://www.integrigy.com/security-resources/integrigy-guide-oracle-audit-vault

Integrigy Framework

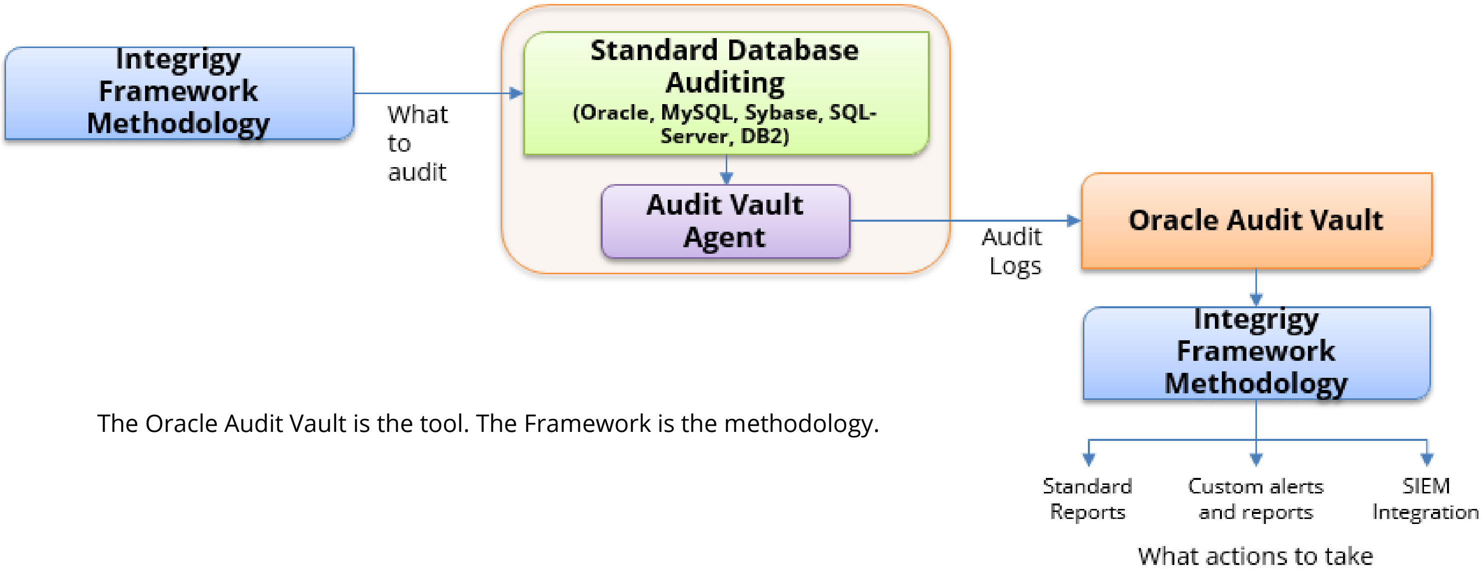
Integrigy's database Log and Audit Framework is ideally suited for use with the Oracle Audit Vault and Database Firewall (AVDF). The Oracle AVDF is a purpose built tool for database logging and auditing and the Integrigy Framework provides the methodology which can be equally applied to all databases supported by Oracle AVDF.

The Framework offers two basic benefits. First, it defines what logging and auditing should be enabled in the source database to provide the content for AVDF alerts and reports. Second, and more importantly, the Framework defines a set of critical events that should be alerted and reported on using AVDF.

The installation of the Oracle AVDF and implementation of the Framework can be completed within a few weeks, depending on the size and number of source databases. The key factor is the amount of logging and auditing currently enabled in the source databases.

High-level implementation plan -

- Review current auditing and requirements
- Install Oracle AVDF appliance and deploy collection agents
- Develop alerts and reports, training and knowledge transfer
- Integrate SIEM and ticket system



The Oracle Audit Vault is the tool. The Framework is the methodology.