INTEGRIGY

WHITE PAPER

How to Control and Secure Oracle E-Business Suite DBAs and Developers

FEBRUARY 2017

How to Control Oracle E-Business Suite DBAs and Developers

Version 1.0 – February 2017

Authors: Mike Miller, CISSP, CISSP-ISSMP, CCSP, CCSK

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

Table of Contents

OVERVIEW

A common compliance challenge for most Oracle E-Business Suite environments is how to control and secure direct database access by DBAs and developers, especially with regards to highly privileged, generic at the database, application, and operating system layers. Often, there is little control or active management of generic accounts like APPS and SYSADMIN with passwords being loosely controlled and frequently shared. This paper will describe the risks associated with these accounts and ways to effective manage and control them to meet security and compliance mandates.

Audience and How to Read This Paper

The intended audience are Oracle E-Business Suite DBAs, application administrators, IT security staff, and internal audit staff. A working technical knowledge of the Oracle E-Business Suite and Oracle Databases is recommended.

Oracle E-Business Suite Versions

The information in this guide is intended for and based on the Oracle E-Business Suite R12 (12.2). All the information and guidance should also be applicable to and be relevant for previous and future versions of the Oracle E-Business Suite, including but not limited to 11.5.x (11i) and 12.1.

GENERIC PRIVILEGED ACCOUNTS

> *A generic account is an application, database, or operating system account used for administration by **multiple people** and has **significant privileges***

The Oracle E-Business Suite is defined by generic accounts in each layer of the technology stack. These accounts are created by the installation of the Suite and are used to manage and maintain it and there are three primary types: Application, Database, and Operating System. The Application accounts are those accounts defined within the E-Business Suite such as SYSADMIN. The Database accounts are those accounts such as SYS and SYSTEM, and the Operating System accounts are accounts such as root, oracle, and applmgr.

Oracle E-Business Suite Generic Accounts	
Oracle E-Business Suite	**SYSADMIN**
	seeded application accounts
Oracle Database	**APPS, APPLSYS**
	SYS, SYSTEM
	Oracle EBS schemas (GL, AP, …)
Operating System ***(Unix and Linux)***	root
	Oracle, applmgr

The risks presented generic privileged accounts used by DBAs and developers are not inconsequential. The majority of data breaches are committed by insiders, either directly or indirectly due to compromised credentials[1]. Some of these breaches are intentional acts by rogue insiders, but unfortunately far too many are accidental acts. The graphic below deconstructs an easy exploit whereby those with access to operating system access (oracle/applmgr), database (SYS, APPS) or application (SYSADMIN) can escalate their privileges and/or gain access to sensitive information.

[1] https://digitalguardian.com/blog/insider-outsider-data-security-threats

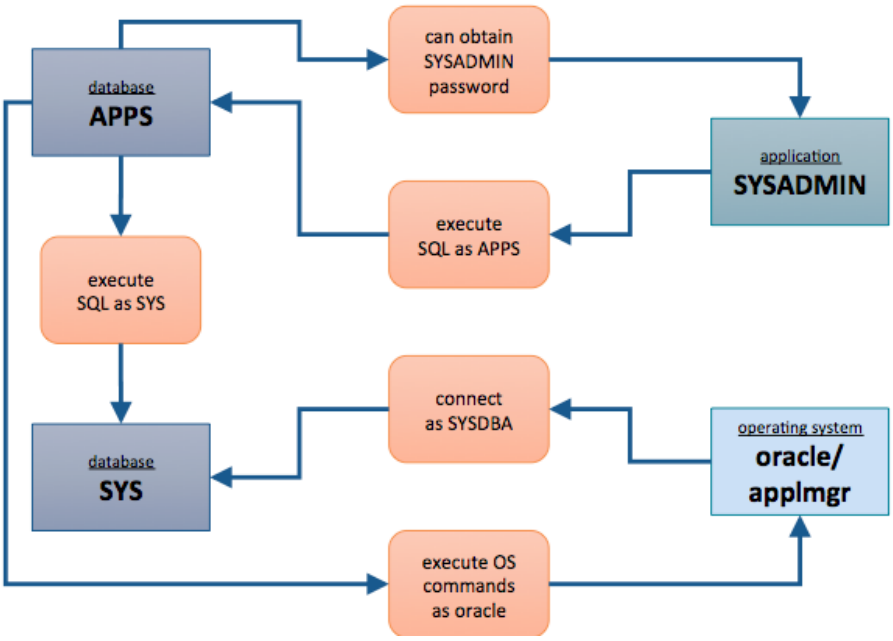


Figure 1 - Privileged User Trust Issues

Strategically five (5) guiding principles can be applied to protect against the risks presented by generic privileged Oracle E-Business Suite accounts:

1. Restrict access
2. Least privilege
3. Password governance
4. Trust-but-verify

Restrict Access

The number one recommendation for database security is to physically reduce direct access to the database. It is rare for a database security vulnerability NOT require a database session. Therefore, by physically limiting direct access to a database, a large measure of security can be provided. Limiting physical access is achieved through network segmentation and/or air gaps as well as requiring privileged users such a DBAs who require direct database access to use a Bastion host or Jump box[2].

Least Privilege

Least privilege is a universal security principle. Whether it is the combination to a bank safe or knowing the passwords to privileged Oracle E-Business Suite generic accounts, this universal principle dictates that everyone should not have access. Access to generic privileged accounts should be given only to personnel whose job function requires access on a regular basis – not ad-hoc and/or because the person believes it makes their job easier. For example, Oracle DBAs should not have the operating system root account for the server running the database. Likewise, the system administrators should not know the SYSTEM and/or APPS passwords.

[2] https://en.wikipedia.org/wiki/Jump_server

Password Governance

The privileged generic accounts created through the installation of the database and/or the Oracle E-Business Suite need their passwords changed (not left as default), need to use complex passwords (not easy to guess) and need to be unique passwords (not shared or all the same). To effectively govern passwords in this manner, privileged generic accounts need to be secured by a password vault. Ideally, the password vault is tightly coupled to a ticket system whereby each password pull can be linked to a ticket.

Trust-But-Verify

Privileged generic accounts for the Oracle E-Business Suite cannot be dropped and/or permanently end-dated. To maintain and support day-to-day operations of the Oracle E-Business Suite, generic privileged accounts must be used. Those personnel whose job functions require them to use the accounts however should not be trusted blindly. An effective logging, auditing, and monitoring strategy needs to be in place to verify the trust and actions of those using privileged generic accounts.

How should you apply the five guiding principles? This paper will review the Oracle E-Business Suite privileged generic accounts by answering three (3) tactical questions:

1. What and how to control the password
2. What to log & monitor for
3. What to audit for

Application Generic Accounts

The installation of the Oracle E-Business Suite creates about 35+ application accounts. These generic privileged accounts are used by administrators to log into the end-user interface to define security structures (e.g. menus and responsibilities) and/or users. DBAs also at times are required to enter a few of the passwords into utilities for patching and other tasks – e.g. SYSADMIN.

The generic privileged application accounts can be broken into two (2) sets the SYSADMIN account and all other seeded generic local accounts - created by the install of the Suite and defined in the table APPLSYS.FND_USER.

The SYSADMIN Account

The SYSADMIN account is the "God" user of the Oracle E-Business Suite. It must be kept open and cannot be disabled or end-dated. It must be used for certain functions and has access to all data within the Oracle E-Business Suite.

SYSADMIN Account Governance Recommendation	
Control	▪ SYSADMIN should only be used for a few specific functions – named accounts for all other administration activities ▪ Change ticket required for all use in production ▪ Use custom generic, less privileged account for scheduled concurrent programs and proxy user ▪ Change password when cloning ▪ Frequently rotate password (90 days)

SYSADMIN Account Governance Recommendation	
	▪ **Manage password** in password vault *[Vault]*
Log & Monitor	▪ Implement auditing for all usage *[Framework]* ▪ Alert on login and monitor all usage
Audit	▪ Check last password change date ▪ Verify password complexity and length settings ▪ Interview to determine how password is controlled

Seeded Generic Accounts

The seeded generic application accounts are designed to own and define various modules of the Oracle E-Business Suite. Some may be kept open, and others are recommended to be end-dated. One particular risk is that these accounts have well-known default passwords.

Seeded Account Listing	
User Name	**Module**
AME_INVALID_APPROVER	AME
APPSMGR	AOL/FND
ASADMIN	AOL/FND
ASGADM	ASG
ASGUEST	AS
AUTOINSTALL	AOL/FND
CONCURRENT MANAGER	AOL/FND
FEEDER SYSTEM	AOL/FND
GUEST	AOL/FND
IBE_ADMIN	IBE, ONT
IBE_GUEST	IBE
IBEGUEST	IBE, IBU
IEXADMIN	IEX
INDUSTRY DATA	AOL/FND
INITIAL SETUP	AOL/FND
IRC_EMP_GUEST	IRC
IRC_EXT_GUEST	IRC
MOBADM	ASG
MOBDEV	ASG
MOBILEADM	ASG
OP_CUST_CARE_ADMIN	XDP
OP_SYSADMIN	XDP
ORACLE12.0.0 – ORACLE12.9.0	AOL/FND
PORTAL30	AOL/FND
PORTAL30_SSO	AOL/FND
STANDALONE BATCH PROCESS	AOL/FND
SYSADMIN	AOL/FND

Seeded Account Listing	
User Name	**Module**
WIZARD	AOL/FND
XML_USER	AOL/FND

Application Generic Account Governance Recommendation	
Control	▪ **End-date** per best practices ▪ Change password to random string
Log & Monitor	▪ Implement auditing for all usage or access *[Framework]* ▪ Alert on any attempt to access
Audit	▪ Review usage of accounts for external access (DMZ) ▪ Check end-date and last use ▪ Check last password change date ▪ Check for newly seeded accounts after any major patches or upgrades

DATABASE PRIVILEGED GENERIC ACCOUNTS

The structure and design of the Oracle E-Business Suite make extensive use of the Oracle RDBMS. The install of the Suite creates 250+ generic database accounts. These may be split into two groups, the accounts directly supporting the database itself and those supporting the Suite. Of these 250+ accounts, the table below classifies the privileged generic accounts -

Privileged Generic Oracle E-Business Suite Database Accounts		
Oracle Database	**SYS**	▪ Owner of the database ▪ Must be used for some operations
	SYSTEM	▪ Generic DBA account ▪ Must be used for EBS adpatch & adadmin
Oracle E-Business Suite	**APPS**	▪ Application account for all access – users, concurrent manager, and maintenance ▪ Must be used for maintenance ▪ APPS can access all data, including encrypted sensitive data
	APPLSYS	▪ Same password as APPS ▪ Should not be directly accessed
	Schema Owners (GL, AP, etc.)	▪ 250+ schema accounts ▪ All active and have default passwords ▪ Significant privileges

Integrigy Corporation's assessment services routinely analyze privileged Oracle generic accounts. The table below depicts a recent summary of assessment results. By far, the risk of not changing default passwords is an on-going issue for many clients. First and foremost for clients concerned with securing privileged Oracle generic accounts, is the need to ensure the default passwords are not used.

Integrigy Survey Result			
Database Account	**Default Password**	**Exists in Database %**	**Default Password %**
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%

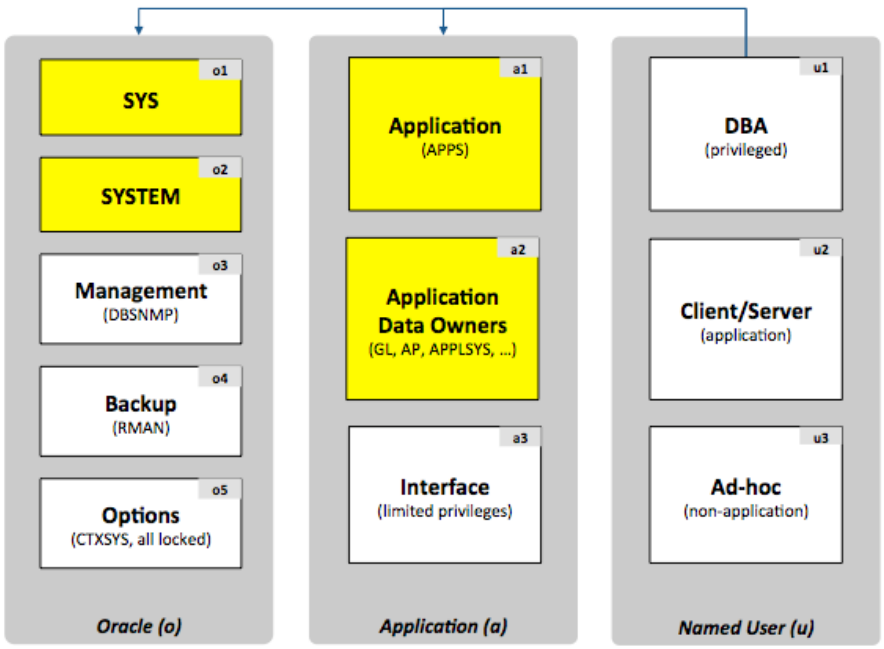
Recommended Tactical Approach

Integrigy's recommended tactical approach for generic database accounts is to classify them into three broad categories. The three (3) categories are: oracle database, application and named. Each category is then broken into components to address specific governance recommendations.

Oracle accounts are those accounts created by the installation of the Oracle RDBMS. Approximately 25 accounts are created with the installation of any Oracle database. Two accounts in particular warrant extra attention: SYS and SYSTEM. The SYS account owns the majority of the code that provides the RDBMS' basic functionality, and the SYSTEM account is the default "God" account created for the administration, support, and configuration of the database.

The application accounts are those database accounts created by the installation of the Oracle E-Business Suite. Well over 250 of these database accounts are created. The most important accounts are the APPS and APPLSYS accounts. These two accounts control how end-users connect to the database and have access to ALL data and transactions. The balance of the accounts are the persistent data stores for each module (e.g. the tables storing General Ledger (GL) data).

The named user accounts are those database accounts created by clients for their staff and personnel to support the Oracle E-Business Suite. Ideally, all DBAs first authenticate to the database using a named account and then connect to APPS such that an audit trail can be followed. As well, ideally all named accounts are GLOBALLY authenticated (e.g. Active Directory).



The tables below address the control, logging & monitoring and audit recommendations for five of the most important privileged generic database accounts (highlighted in yellow in the graphic above) -

SYS Account Governance Recommendation	
Control	▪ **Control password** with password vault *[Vault]* ▪ SYS should only be used for a few specific functions – named DBA accounts for all other database management activities ▪ Change ticket required for use in production ▪ Change password when cloning
Log & Monitor	▪ Implement auditing for logins, key security and change management events *[Framework]* ▪ AUDIT_SYS_OPERATIONS = TRUE ▪ Reconcile usage to change tickets
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

SYSTEM Account Governance Recommendation	
Control	▪ **Control password** with password vault *[Vault]* ▪ SYS should only be used for a few specific functions – named DBA accounts for all other database management activities ▪ Change ticket required for use in production ▪ Change password when cloning
Log & Monitor	▪ Implement auditing for logins, key security and change management events *[Framework]* ▪ AUDIT_SYS_OPERATIONS = TRUE ▪ Reconcile usage to change tickets
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

APPS Account Governance Recommendation	
Control	▪ **Manage password** with password vault *[Vault]* ▪ **APPS should only be used for EBS administration and patching** – named DBA accounts for all other database management functions ▪ Use custom database profile with no lockout but strong password controls ▪ Change password when cloning
Log & Monitor	▪ Implement auditing for logins, key security and change management events *[Framework]* ▪ Monitor closely for failed logins *[Framework]* ▪ **Attempt to reconcile** DBA usage to change tickets
Audit	▪ Check last password change date ▪ Review logins to see who else is using ▪ Interview to determine how password is controlled

EBS Schema (Application) Account Governance Recommendation	
Control	▪ **Change all passwords using FNDCPASS and throw the password away** ▪ Control the APPLSYS account same as APPS ▪ R12 = lock all the schema accounts using the utility AFPASSWD –L ▪ Change passwords when cloning
Log & Monitor	▪ Implement auditing for all logins, key security and change management events *[Framework]* ▪ Alert on any logins to the schema accounts ▪ Alert on any logins to APPLSYS
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

General IT controls for database passwords

Besides the recommendations above, Integrigy recommends that database password profiles[3] be created and assigned for each of the three categories of database accounts. Ensure that all accounts are assigned an appropriate profile. Never use the DEFAULT ("unlimited") profile and routinely check for accounts assigned to the DEFAULT profile. Ideally, either use a custom password verify function or the complex Department of Defense DISA STIG password verify function that Oracle now provides.

Also, routinely check for default database passwords, especially after major database upgrades and Oracle E-Business Suite patches. Use a tool like Integrigy AppSentry[4] rather than the Oracle view DBA_USER_WITH_DEFPWD that checks all accounts for many passwords.

Integrigy believes that database profiles should be used as a method for categorizing the database accounts based on purpose and usage. No account should ever have the DEFAULT profile, and periodic checks should be enabled to identify any such accounts, as this could be an indication of a rogue account or deviation from standard DBA procedures. One such example is often during application installation, database accounts may

[3] https://docs.oracle.com/database/121/DBSEG/users.htm#DBSEG002

[4] https://www.integrigy.com/products/appsentry

be created without the DBAs knowledge as part of installation scripts. These accounts almost always have default passwords, usually where password equals username. This categorization can also be used to generate reports for periodic review of database accounts by managers.

A suggested set of database password profiles involves having four profiles. The profiles are defined as follows –

Profile Name	Accounts	Description
DEFAULT	None	No accounts should be assigned this profile, and a periodic review should be made for accounts using this profile. This would indicate the account was created using an automated process or script and was not identified at execution time. The password controls for this profile should be relaxed, as strict password controls often will cause installation scripts to fail.
XXXX_PROFILE	All Client XXXX named accounts	All Client XXXX individual user accounts should be assigned this profile, and the password parameters should match the Client XXXX password guidelines for user accounts.
DB_PROFILE	All standard Oracle Database accounts and all non-interactive application accounts	All standard Oracle database accounts (SYS, SYSTEM, DBSNMP, CTXSYS, etc.) and all non-interactive application accounts (those if locked would not cause a denial of service) should be assigned this profile. The password parameters should be for an application/service account with a password verify function, account lockout, and periodic password change.
APP_PROFILE	All interactive application databases including web application and interface accounts	All application accounts that require interactive access to the database from either client/server programs, web applications, or interfaces. For maximum compatibility, no password parameters should be enforced, especially account lockout.

Resource Name	Suggested Default	XXXX PROFILE	DB_PROFILE	APP PROFILE
FAILED_LOGIN_ATTEMPTS	10	5	10	UNLIMITED
PASSWORD_GRACE_TIME (Days)	7	10	10	UNLIMITED
PASSWORD_LIFE_TIME (Days)	180	90	365	UNLIMITED
PASSWORD_LOCK_TIME (Days)	1	30	DEFAULT	DEFAULT
PASSWORD_REUSE_MAX (Passwords)	UNLIMITED[4]	2	DEFAULT	DEFAULT
PASSWORD_REUSE_TIME (Days)	UNLIMITED[4]	180	DEFAULT	DEFAULT
PASSWORD_VERIFY_FUNCTION		ORA12C_S	ORA12C_STRON	ORA12C_STRONG_V

Resource Name	Suggested Default	XXXX PROFILE	DB_PROFILE	APP PROFILE
		TRONG_VERIFY_FUNCTION	G_VERIFY_FUNCTION	ERIFY_FUNCTION[1]
Database Accounts	None	All individual accounts	All standard Oracle DB accounts	All interactive application accounts

[1] All interactive application database accounts should be set to strong passwords with a minimum length of 10 characters and be complex passwords as a matter of procedure. Since these accounts are all controlled by the DBAs and the passwords are changed simultaneously, there should be minimal risk that the passwords are set with weak passwords.

[2] The SYS account is exempt from the FAILED_LOGIN_ATTEMPTS settings, therefore, cannot be locked due to an excessive number of failed logins. Oracle 12 delivers a new hidden parameter '_sys_logon_delay.' This parameter introduces a one-second delay before the same client can attempt subsequent SYS logons. The parameter applies not to just SYS, but all Oracle 12c password file users such as SYS, SYSKM, SYSDG and SYSBACKUP. The default is one (1) second. A value of zero (0) means the feature is disabled.

For more information on query and set this parameter see: How To Query And Change The Oracle Hidden Parameters In Oracle 10g,11g and 12c (Doc ID 315631.1)

To query the parameter use this SQL:

```
SELECT A.KSPPINM "PARAMETER",
       B.KSPPSTVL "SESSION VALUE",
       C.KSPPSTVL "INSTANCE VALUE"
FROM   X$KSPPI A,
       X$KSPPCV B,
       X$KSPPSV C
WHERE  A.INDX = B.INDX
AND    A.INDX = C.INDX
AND    A.KSPPINM  = '_sys_logon_delay';
```

[3] No PASSWORD_VERIFY_FUNCTION is used since the creation of accounts under this profile would be the account is being created by an automated process or script and will fail when a default password is set rather than a user supplied password. A mitigating control to periodically search for accounts with the DEFAULT profile will identify any such accounts.

[4] PASSWORD_REUSE_MAX and PASSWORD_REUSE_TIME work in conjunction. Thus setting PASSWORD_REUSE_MAX to 5 and PASSWORD_REUSE_TIME to 450 days will not allow a user to reuse the same password for at least five passwords and in a 450 day period (90 days x 5). Setting either value to UNLIMITED never permits a user to reuse the same password.

Operating System Privileged Generic Accounts

The Oracle E-Business Suite has two (2) primary privileged generic operating system accounts that need to be carefully governed. They are the accounts that own the database and the application code, respectfully known as oracle and applmgr.

EBS Operating System Account Governance Recommendation	
Control	▪ **Control password** with password vault *[Vault]* ▪ **Prevent direct logins to oracle and applmgr** ▪ DBAs should have named OS accounts ▪ Require DBAs to use to su, sudo, or PowerBroker to access oracle and applmgr accounts ▪ Enforce a chain-of-trust – named user → generic user ▪ No developer access to production server OS
Log & Monitor	▪ Implement auditing at the OS level for all user logins ▪ Use keystroke or command logging if required ▪ Alert on direct logins to oracle or applmgr
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

Overall Best Practice Recommendations for Privileged Generic Accounts

Governing generic privileged accounts is not an isolated security requirement and should be part of an overall database security program. This program should define an overall access management policy based on IT security policies and compliance requirements (e.g. SOX, PCI, HIPAA).

Additional tactical steps to secure and govern privileged generic accounts should include the following -

- Use a Bastion host (virtual desktop) for direct O/S and/or database access
  - Restrict network access and/or database Access Control Lists (ACL)
  - Two-fact authentication to access
  - Use SSH Keys for appropriate O/S accounts
  - Install key logger
- Consider Oracle Database Vault
  - Additional license but comes with pack for Oracle E-Business Suite

Lastly, if nothing else is done other than to change default passwords, the use of a password vault is required. Regardless of whether or not you use a leading enterprise solution for a password vault or an open source alternative, password vaults shrink the trust perimeter and promote best practice behaviors. Ideally, a ticket system can be tightly coupled to the password vault such that when DBAs and developers pull passwords for privileged generic accounts that they first must prove that and/or reference a ticket assigned to them requiring the use of the account.

When designing a password vault take care to implement it as a "rules engine" and not to attempt to reproduce the organization's personnel directory and/or asset inventory (e.g. Configuration Items/CIs).

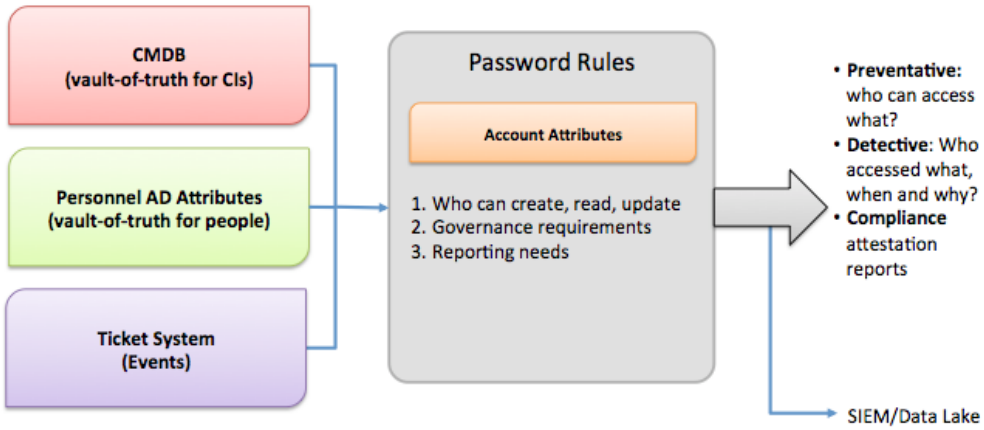


Figure 2 - Password Vault Rules Engine

PRIVILEGED GENERIC ACCOUNTS NEED TO BE LOGGED, AUDITED AND MONITORED

Using privileged generic accounts to support the Oracle E-Business Suite cannot be avoided. This means that some personnel, ideally a small group, need to be trusted. This trust as noted above should not be blind. The trust of those users using privileged generic accounts to support the Oracle E-Business Suite should be verified through logging, auditing, and monitoring.

Most Oracle E-Business Suite implementations do not fully take advantage of the auditing and logging features. These features are sophisticated and can satisfy most organization's compliance and security requirements.

The default Oracle E-Business Suite installation only provides a basic set of logging functionality. 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.

Even organizations already using centralized logging or Security Incident and Event Management (SIEM) solutions, while being more advanced in the Common Maturity Model (CMM), in Integrigy's experience are commonly challenged by the E-Business Suite's auditing and logging features and functionality.

Integrigy has developed a framework for auditing and logging in the Oracle E-Business Suite. This framework is a direct result of Integrigy's consulting experience and will be 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:

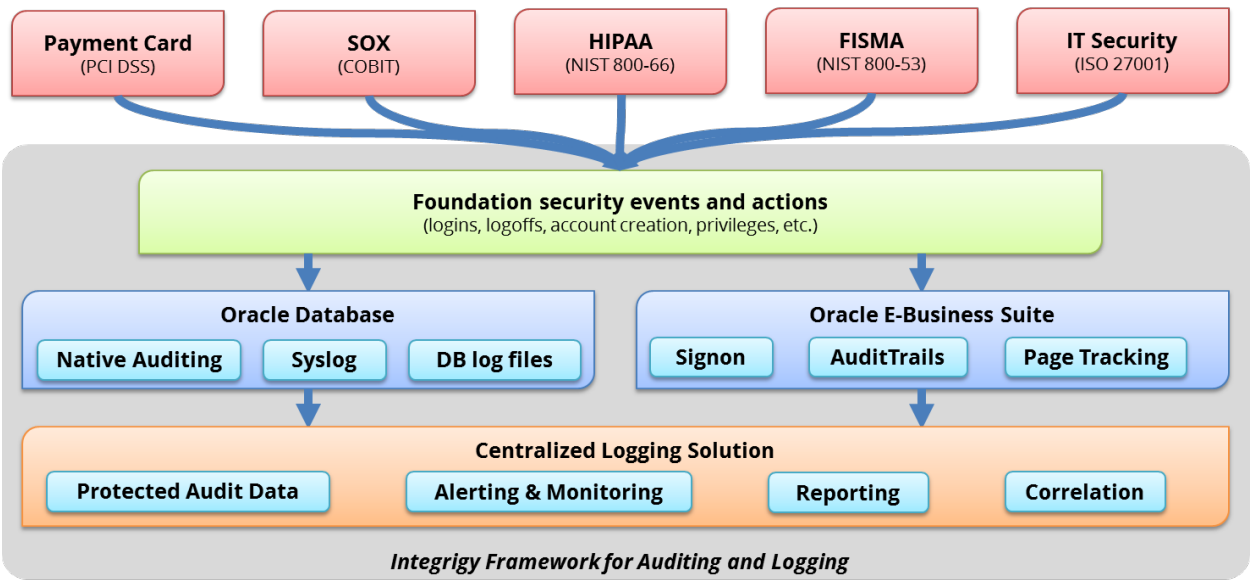
- **Level 1** – Enable baseline auditing and logging for application/database and implement security monitoring and auditing alerts
- **Level 2** – Send audit and log data to a centralized logging solution outside the Oracle Database and E-Business Suite
- **Level 3** – Extend logging to include functional logging and more complex alerting and monitoring

The framework is a result of Integrigy's consulting experience and is based on compliance and security standards such as Payment Card Industry (PCI-DSS), Sarbanes-Oxley (SOX), IT Security (ISO 27001), FISMA (NIST 800-53), and HIPAA.

The foundation of the framework is the set of security events and actions that should be audited and logged in all Oracle E-Business Suite implementations. These security events and actions are derived from and mapped back to key compliance and security standards most organizations have to comply with. We view these security events and actions as the core set, and most organizations will need to expand these events and actions to address specific compliance and security requirements, such as functional or change management requirements.

Table 1 presents the core set of audits that, if implemented, will serve as a foundation for more advanced security analytics. Implementing these audits will go a long way toward meeting logging and auditing requirements for most compliance and security standards like PCI requirement 10.2. The numbering scheme used in Table 1 will be referenced throughout the document.

Table 1 – Foundation Events for Logging and Security Framework					
Security Events and Actions	**PCI DSS 10.2**	**SOX (COBIT)**	**HIPAA (NIST 800-66)**	**IT Security (ISO 27001)**	**FISMA (NIST 800-53)**
E1 - Login	10.2.5	A12.3 DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects: Create object Modify object Delete object	10.2.7	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2



REFERENCES

- Integrigy Guide to Auditing and Logging in the Oracle E-Business Suite
  https://www.integrigy.com/security-resources/guide-auditing-oracle-applications
- Oracle 12.2 E-Business Security Guide https://docs.oracle.com/cd/E26401_01/doc.122/e22952/toc.htm

About Integrigy

Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

INTEGRIGY
Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com