Turbocharge Your Database Auditing with Oracle Unified Auditing

February 25, 2021

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications

Oracle E-Business Suite
and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database
Security Auditing Tool

Validates and Audits Security

AppDefend

Enterprise Application Firewall
for Oracle E-Business Suite
and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

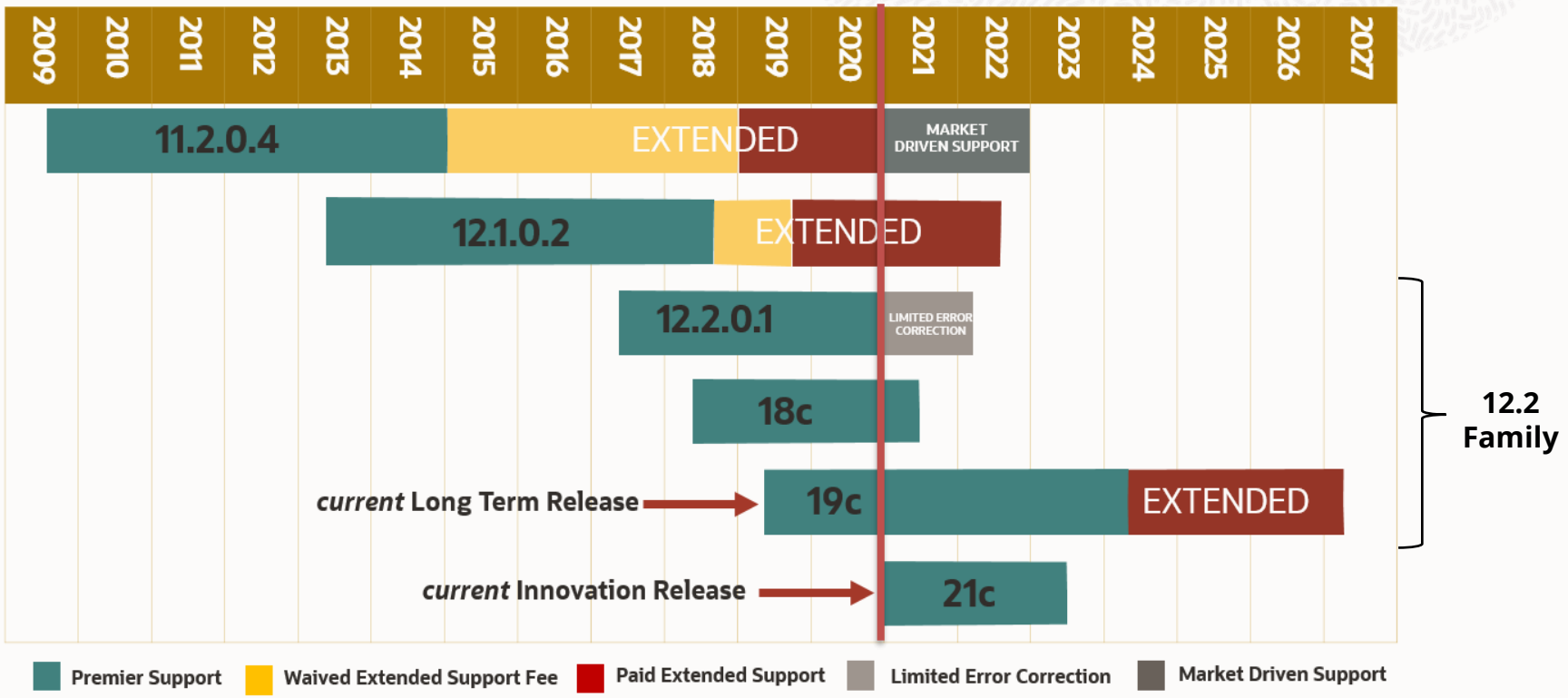
Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Oracle Database Releases

Database Releases and Support Timelines



Source – Oracle Database (RDBMS) Releases Support Status Summary (Doc ID 161818.1) – January 15, 2021

Auditing Design – Layered Design Example

All Databases

Common Events

Database Events
- Database logins
- Database logoffs
- Failed database logins
- Privileges commands

Security/Auth Events
- Create/Alter/Drop User
- Create/Drop Role
- Grant/Revoke Privileges system, role, object
- Database profile changes
- Sensitive packages

Database Changes
- Database configuration changes
- Auditing changes
- Database links
- Core object changes

Anomaly Detection
- SQL Errors (defined list)
- Defined anomalous events
- Defined intrusion events
- Known security vulnerabilities

Compliance DBs

Compliance Events

SOX
- Database object changes
- Privileged account access by global list of accounts

PCI
- Requirement 10.2
- Access to card data in global list of tables
- Privileged account access by global list of accounts

GDPR
- Privileged account access by global list of accounts

HIPAA
- Privileged account access by global list of accounts
- Access to HIPAA data based on global list of tables

Per Database

Per Database Events (defined during database on-boarding)

Access to PII/Confidential Data
- Tables and columns containing PII and confidential data
- Select, Insert, Update, and/or Delete based on requirements

Privileged Account Access
- Definition of accounts per application or database
- Exceptions to monitoring based on location or type of access

Auditing Design – Oracle E-Business Suite Example

Common Events

Security Events
- All database sessions
- All failed database logins
- All application sessions
- All failed application logins

Database Events
- SQL errors
- SQL errors by EBS end-user
- Sensitive packages

SOX Events and Reports
- Database user changes
- Database user password changes
- System privileges and roles changes

Anomaly Detection
- SQL Errors (defined list)
- Defined anomalous events
- Defined intrusion events
- Known security vulnerabilities

	EBS End-User	EBS Batch	Deployment	APPS DBA	All Other
Overview	All end-user application SQL is ignored, except specific statements/objects for select users.	All concurrent requests SQL is ignored.	Deployment will tag all DDL/DML with change ticket number.	All APPS DDL/DML performed by DBAs for manual changes, patching, and maintenance.	All DDL/DML for all other database users, including standard Oracle DB, Oracle EBS, and individual database accounts.
Capture/Filter	DB User: APPS Source: App Servers App User: Set and (not GUEST or SYSADMIN) App: FRMWEB, …	DB User: APPS Source: CM Servers App: STANDARD, …	DB User: APPS Source: Deployment Server Additional Capture Package # Package Deployer	DB User: APPS Source: Not filtered prior Operating System ID	DB User: All other ▪ Oracle – SYS, SYSTEM, … ▪ Oracle EBS – APPLSYS, APPLSYSUB, 300+ module ▪ Other – SSO, … Operating System ID
Alerts/Reporting	SYSADMIN Logins SYSADMIN Activity Summary SYSADMIN Activity Detail GUEST Errors/SQL Injection GUEST Large Queries	None	All-Deployment-No Ticket All-Deployment-With Ticket	DBA APPS Logins DBA APPS Usage Summary DBA APPS Usage Detail DBA-Changes Window DBA-Changes Ad-hoc Unauth APPS Use Summary Unauth APPS Use Details	All-DB Logins All-DB Usage Summary All-DB Usage Detail Unath APPLSYSPUB Use Non-App/Non-DBA DDL/DML

99.5% of all SQL statements

Integrigy Auditing Framework – Security Events and Actions

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

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 Auditing Framework – Security Events Mapping

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	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects Create/Modify/Delete	10.2.7	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2

Oracle Unified Auditing

- **Unified Auditing introduced in Oracle 12.1**
- **Consolidates multiple audit trails into a single location (“unified”)**
  - AUD$, FGA_LOG$, DVSYS.AUDIT_TRAIL$ … now saved in UNIFIED_AUDIT_TRAIL
- **Performance improvements in writing and reading (12.2+) audit data**
  - Uses an internal relational table
- **Improved security of the audit trail**
  - New roles to manage and view audit trail
  - No ability to delete audit trail except through audit trail management package
- **Unified Auditing is always enabled**
- **Database initialization parameter no longer used for auditing**
  - audit_trail, audit_file_dest, audit_sys_operations are deprecated

Unified Auditing Enhancements by Version

12.2	▪ **Audit policy conditionally based on database roles** ▪ Redesign of based Unified Auditing base table ▪ Integration with Transparent Sensitive Data Protection (TSDP) ▪ New audit events for Database Real Application Security (AUDIT_GRANT/REVOKE_PRIVILEGE) ▪ Ability to capture Virtual Private Database (VPD) predicates in the audit trail (rls_info) ▪ Performance and stability improvements
18c	▪ **Write audit records to SYSLOG (see MOS ID 2623138.1)** ▪ Unified Audit trail is automatically included in the Data Pump dump files
19c	▪ **Ability to audit only Top-Level SQL statements – exclude statements run from within PL/SQL procedures or functions** ▪ AUDSYS.AUD$UNIFIED system table has been redesigned to use partition pruning to improve read performance ▪ SYSLOG audit records now include PDB_GUID to identify pluggable database where the audit records originated ▪ **EVENT_TIMESTAMP changes from TIMESTAMP(6) WITH LOCAL TZ to TIMESTAMP(6)**
21c	▪ **Unified Auditing policy configuration changes effective immediately for current session and all active sessions** ▪ Unified Audit policies enforced on the current user (triggers, definer rights) ▪ Auditing for connections and requests to XML DB HTTP and FTP Services ▪ Unified Auditing on an editioned object now applies to all its editions ▪ SYSLOG destination for common Unified Audit policies (UNIFIED_AUDIT_COMMON_SYSTEMLOG) ▪ **Deprecation of Traditional Auditing**

Unified Auditing Issues

12.1.0.2	PSU or Bundle Patches queue write mode changes to immediate write mode	Unified Auditing changes mode of writing in 12.1, see MOS ID 2530035.1
12.1.0.x	object_schema and object_name contain incorrect values	Patch 23624488
12.1.0.1	Standard Edition unable to enable Unified Auditing	Patch 17466854
12.1.0.x	Poor performance	Patch 28186466, see MOS ID 2212196.1
12.1.0.2+	AUDIT Commands Executed With CONTAINER = ALL Inside The CDB Are Not Synchronized Into PDB	See MOS ID 2312141.1
12.1.0.1	Audit ACTIONS ALL does not audit all actions	Fixed in 12.1.0.2, See MOS ID 16714031.8
12.2.0.1+	CREATE ANY JOB system privilege is not audited	Fixed in 19.1.0, see MOS ID 27000076.8
12.1.0.2+	Failed SYS logins may not be audited	Fixed in 19.1.0, see MOS ID 27378208
12.1.0.2+	Newly created users are not audited by policies with EXCEPT clauses	See MOS ID 2400613.1

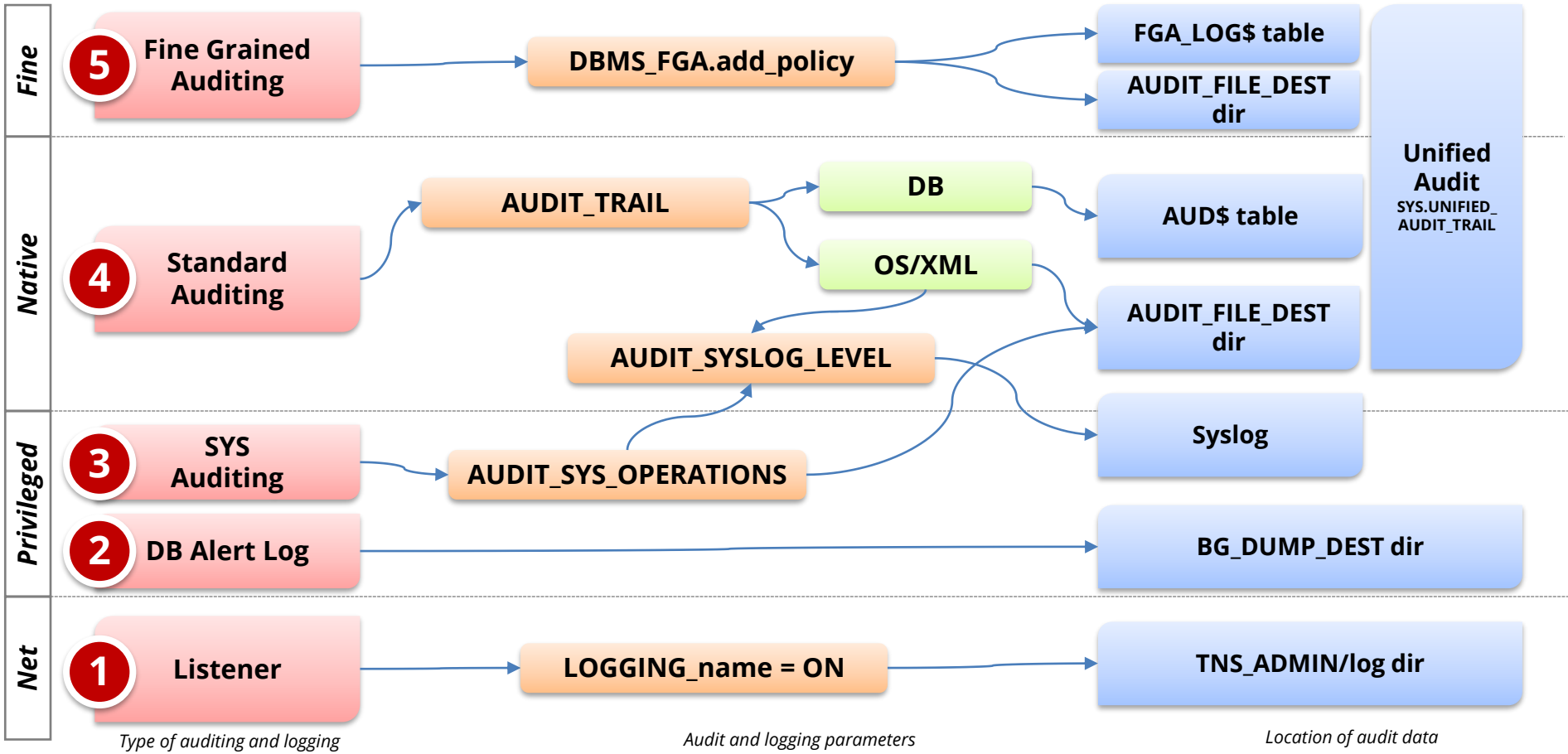
Oracle Database Auditing Types and Modes

Traditional Auditing	▪ Enabled based on database initialization parameter (audit_trail) ▪ Audits based on audit statement ▪ Audit trail stored in AUD$
Unified Auditing	▪ Enabled by default ▪ Audits based on audit policies ▪ Audit trail stored in UNIFIED_AUDIT_TRAIL

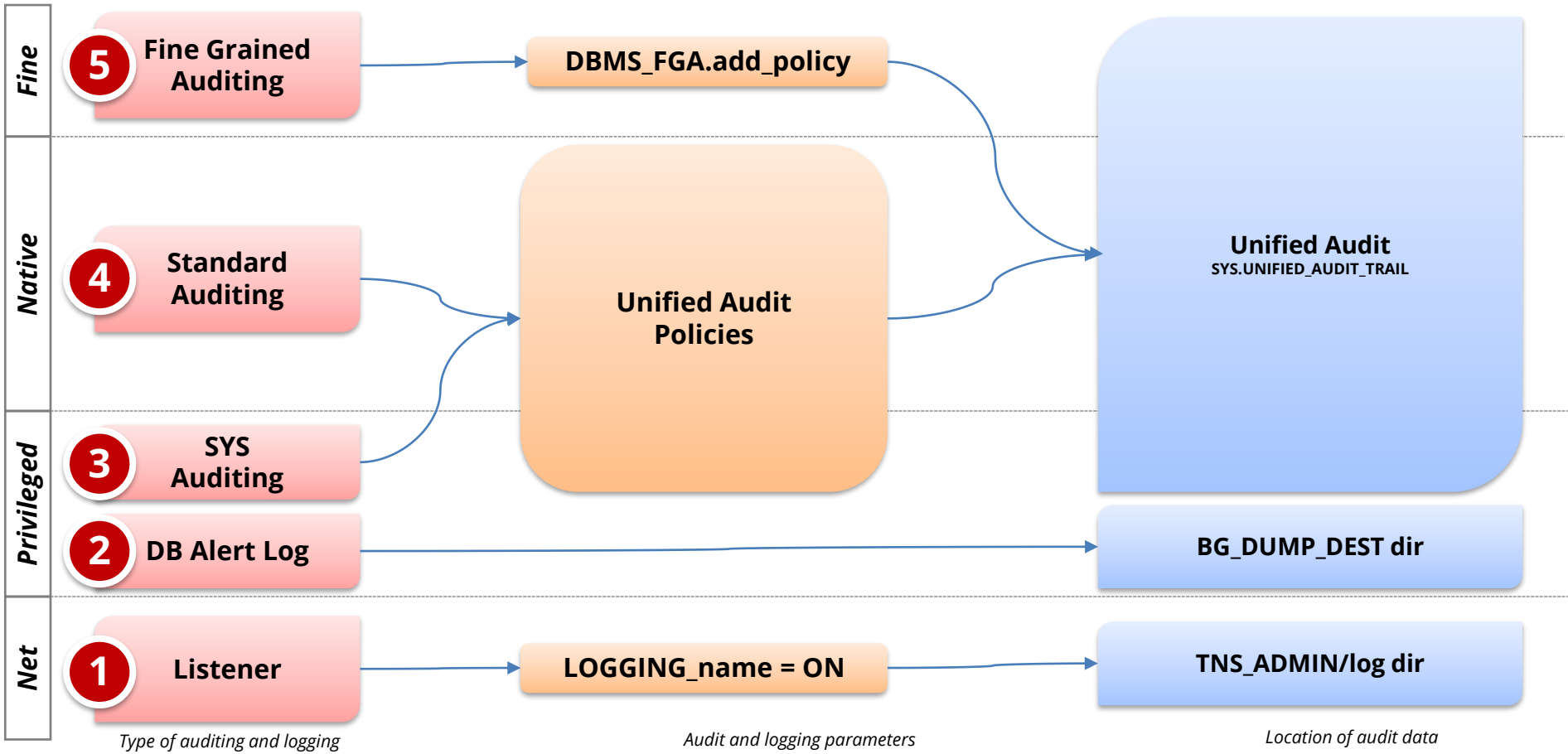
Mixed Mode	▪ Traditional and Unified Auditing are both enabled simultaneously ▪ Audit data written based on Traditional Auditing audit statements and Unified Auditing audit policies

Pure Unified Auditing	▪ Enable in database kernel, disables Traditional Auditing
	▪ No database initialization parameters (audit_trail)
	
	`$ cd $ORACLE_HOME/rdbms/lib`
	`$ make -f ins_rdbms.mk uniaud_on ioracle`

Mixed Mode – Traditional Auditing + Unified Auditing



Pure Unified Auditing



Is Unified Auditing Enabled?

- Yes, enabled by default in Mixed Mode
- Only `ORA_SECURECONFIG` and `ORA_LOGON_FAILURES` policies enabled by default

	V$OPTION Parameter 'Unified Auditing'	
	= TRUE	**= FALSE**
V$PARAMETER audit_trail = none	↑ **Pure** Unified Auditing (`UNIFIED_AUDIT_TRAIL`)	↑ **No** ← Unified Auditing (`no auditing`)
V$PARAMETER audit_trail = DB,OS,…	↑ **Pure** Unified Auditing (`UNIFIED_AUDIT_TRAIL`)	↑ ← **Mixed Mode** (`AUD$ + UNIFIED_AUDIT_TRIAL`)

Traditional Auditing Audit

AUDIT **<statement | system_privileges | roles>**

BY **<ALL | user, user, ...>**

WHENEVER [NOT] SUCCESSFUL

- **Auditing limited to a list of users or ALL users**
  - No granularity
- **No conditions allowed by on the "context" of the database session**
- **Filtering and removing of noise done after the fact in alerting and reporting**
- **Unable to granularly capture audit trail of high volume users (e.g., APPS)**

Unified Auditing – CREATE AUDIT POLICY Statement

CREATE AUDIT POLICY <name>

<standard_actions | **component_actions** | system_privileges | roles>

WHEN **<audit_condition_expression>**

EVALUATE PER <STATEMENT | SESSION | INSTANCE>

[ONLY TOPLEVEL]

- **Audit policies expanded to actions in –**
  - Oracle Data Pump, Oracle SQL*Loader Direct Path Load, Oracle Label Security, Oracle Database Real Application Security, and Oracle Database Vault
- **Conditions based on SYS_CONTEXT allow to base audit on the context of the database session**
- **TOPLEVEL limits auditing to only SQL statements issued directly by a user rather than all statements include those in procedures, functions, and triggers**

Unified Auditing – AUDIT statement

AUDIT POLICY <name>

[BY <**user, user, …>**]

[EXCEPT <**user, user, …>**]

[BY USERS WITH GRANTED ROLES **<roles, roles, …>**]

WHENEVER [NOT] SUCCESSFUL

- **Able to make audit policy granular to specific users or roles**
  - Simple to change without recreating all audits as in Traditional Auditing
- **BY USERS WITH GRANTED ROLES enables audit if users is in a role**
  - Not the actions of the role, which is done in the audit policy
- **EXCEPT important to audit all users, except high volume users (e.g., APPS)**

Unified Audit Policies Installed by Default

Policy Name	Enabled By Default	# of Audits
ORA_SECURECONFIG	Yes	49
ORA_RAS_POLICY_MGMT	No	35
ORA_RAS_SESSION_MGMT	No	14
ORA_ACCOUNT_MGMT	No	9
ORA_DATABASE_PARAMETER	No	3
ORA_LOGON_FAILURES	No	1
ORA_DV_AUDPOL2	No	19
ORA_CIS_RECOMMENDATIONS	No	35
ORA_DV_AUDPOL	No	2,180

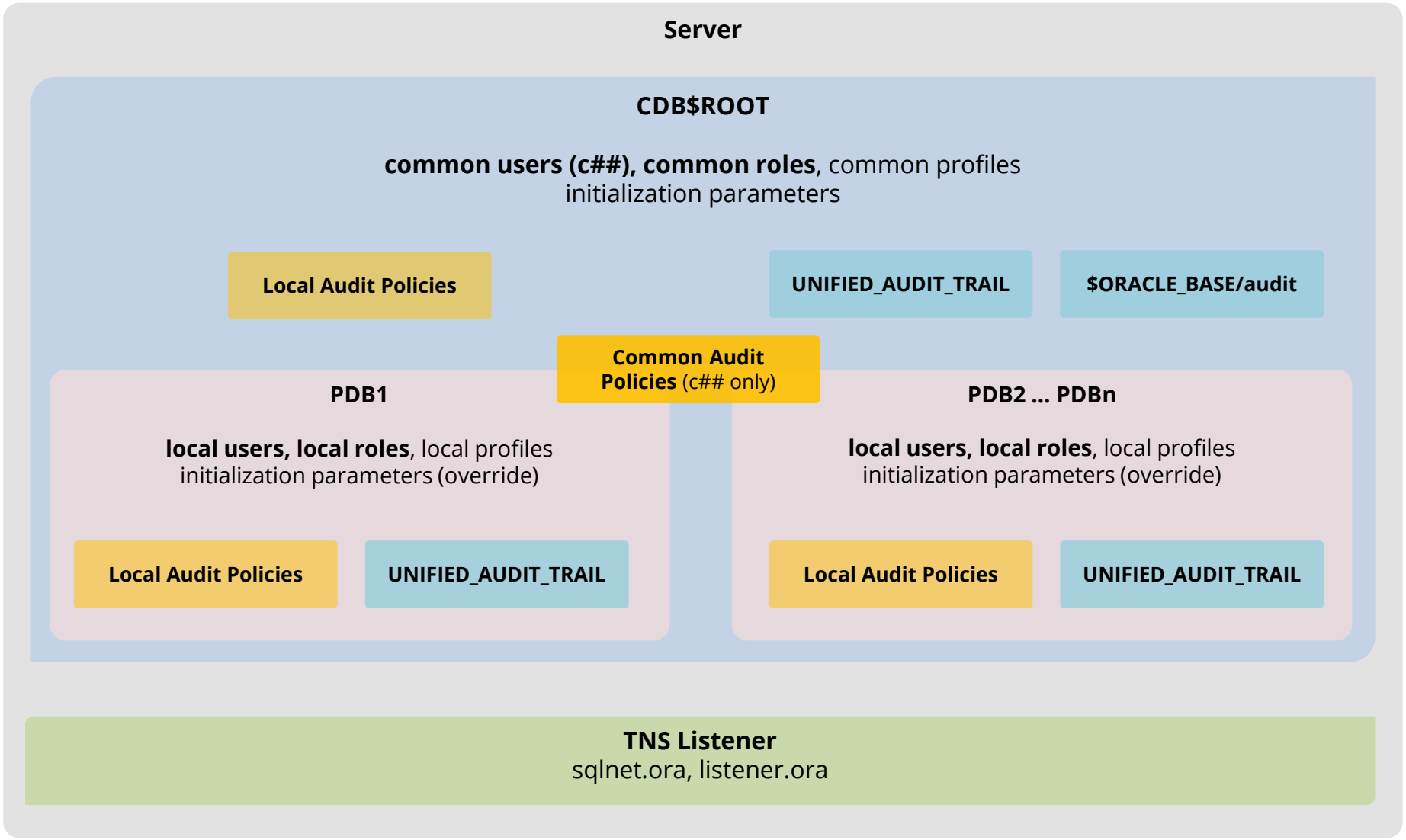
Audit Policies are Objects

```
SELECT owner, object_name, object_type, created, last_ddl_time, timestamp,
oracle_maintained
FROM dba_objects
WHERE object_type = 'UNIFIED AUDIT POLICY'
ORDER BY object_name;
```

OWNER	OBJECT_NAME	OBJECT_TYPE	CREATED	LAST_DDL_TIME	TIMESTAMP	ORACLE_MAINTAINED
SYS	INTEGRIGY_LOGON_SUCCESSES	UNIFIED AUDIT POLICY	24-OCT-19	24-OCT-19	2019-10-24:17:09:42	N
SYS	ORA_ACCOUNT_MGMT	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:14:31	Y
SYS	ORA_CIS_RECOMMENDATIONS	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:14:31	Y
SYS	ORA_DATABASE_PARAMETER	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:14:31	Y
SYS	ORA_DV_AUDPOL	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:02:02:59	Y
SYS	ORA_DV_AUDPOL2	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:02:03:02	Y
SYS	ORA_LOGON_FAILURES	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:14:31	Y
SYS	ORA_RAS_POLICY_MGMT	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:02:51	Y
SYS	ORA_RAS_SESSION_MGMT	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:02:51	Y
SYS	ORA_SECURECONFIG	UNIFIED AUDIT POLICY	17-APR-19	17-APR-19	2019-04-17:01:14:31	Y

10 rows selected.

Unified Auditing and Multitenant



Unified Auditing and Multitenant

- Common policies only audit Common Users (C##)
- All Oracle pre-defined policies are not common policies

	User	
	Common (C##)	**Local (PDB)**
Common Audit Policy root container = ALL visible in all PDB	**root** user audited	**PDB** no
	PDB user audited	
Local Audit Policy root or PDB container = CURRENT	**root** user audited	**PDB** user audited
	PDB user audited	

Mandatory Auditing

- **Unified Auditing always-on-auditing for SYSDBA**
  - SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, SYSKM

- **Mandatory Auditing Events (SYS.UNIFIED_AUDIT_TRIAL)**

  - CREATE AUDIT POLICY
  - ALTER AUDIT POLICY
  - DROP AUDIT POLICY
  - AUDIT
  - NOAUDIT
  - Database Vault configurations
  - DBMS_FGA PL/SQL package
  - DBMS_AUDIT_MGMT PL/SQL package
  - ALTER TABLE attempts on the AUDSYS audit trail

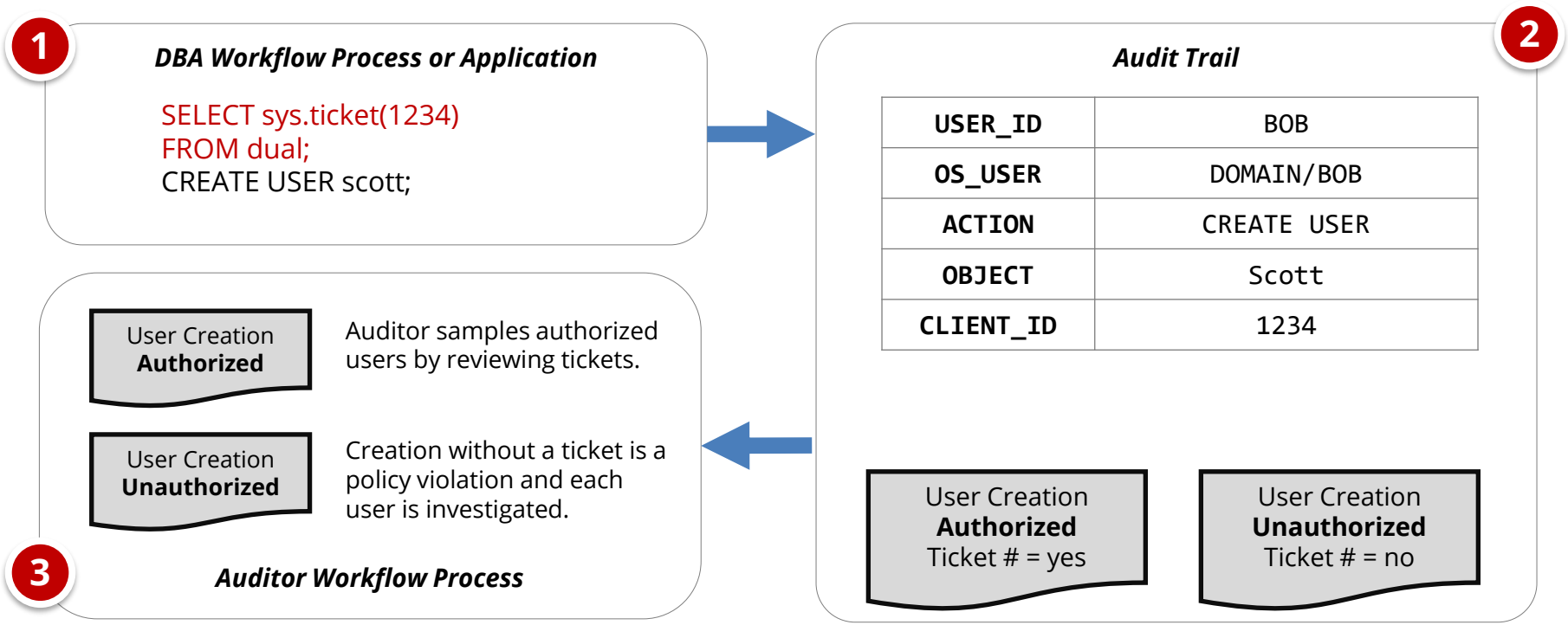
Recommended Database Logging – Security Events

Framework Event	Object	Oracle Audit Statement	Resulting Audited SQL Statements
E1, E2, E3	**Session**	session	Database logons and failed logons
E5, E6	**Users**	user	create/alter/drop user
E7, E8	**Roles**	role	create/alter/drop role
E13	**Database Links** **Public Database Links**	database link public database link	create/drop database link create/drop public database link drop public database link
E11	**System**	alter system	alter system
E14	**Database**	alter database	alter database
E9, E10	**Grants (system privileges and roles)**	system grant	grant revoke
E4	**Profiles**	profile	create/alter/drop profile
E11, E14	**SYSDBA and SYSOPER**	sysdba sysoper	All SQL executed with sysdba and sysoper privileges

See Integrigy Auditing and Logging Framework whitepaper for complete database auditing recommendations

Change Ticket Tracking – Create User Example

Capture ticket numbers and other information for a database session based on special SQL executed by database users or applications.



Oracle Database Security Changes

- **Database users**
  - Creation of users
  - Dropping of users
  - Alerting of users (password, profile, default tablespace, etc.)
- **Profiles (password and resource controls)**
- **Roles**
- **Role and system privileges**
  - Granting to users and roles
  - Revoking from users and roles
- **Table and object privileges**
  - Granting and revoking of select, insert, update, delete, execute, etc. privileges
- **Auditing**
  - Audit, noaudit
  - Fine-grained auditing (FGA) policies, Unified auditing policies, etc.
  - Purging of auditing tables
- **Oracle Database Vault configuration and policies**

Change Management Challenges

- Many changes are made by generic, privileged accounts and difficult to determine the named DBA
- Database and application patches may result in database security changes

Oracle Database Changes

- **Oracle Database patches**
- **Initialization parameters**
- **Packages, procedures and functions (PL/SQL code objects)**
- **Tables/Views/Indexes**
- **Triggers**
- **Materialized Views**
- **Database storage (tablespaces, data files, etc.)**
- **Other database objects (sequences, types, etc.)**

Change Management Challenges

- Some database changes are made by automated application processes as part of standard transaction processing
- Many changes are made by generic, privileged accounts and difficult to determine the named DBA
- Database and application patches may result in hundreds of database changes
- Initialization parameters may be changed in the database or operating system files

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**

linkedin – **linkedin.com/company/integrigy**

twitter – **twitter.com/integrigy**

Copyright © 2021 Integrigy Corporation