INTEGRIGY

Security Assessment Services

Integrigy Consulting

October 2023

mission critical applications ...
... mission critical security

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 Security

AppDefend

Enterprise Application Protection
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, GDPR, PCI, HIPAA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE
Gold Partner

Integrigy Background

- Extensive experience with Oracle
  - Founded by former Big-6 consultants with significant experience on Oracle implementations in Fortune 500 companies
  - Founders recognized a major gap in all implementations – little or no security auditing done on projects
  - Integrigy has found more security bugs in the Oracle E-Business Suite than anyone else inside or outside of Oracle

- Both an ERP company and a security company
  - Products developed to support and enhance an ERP implementation – Integrigy understands the issues and risks challenging large ERP implementations
  - Integrigy bridges the gap between applications, databases, and security

Agenda

1. Integrigy Background
2. Oracle E-Business Suite Security
3. Assessment Services
4. Proposal
5. Q & A

Oracle ERP Example Security Risks and Threats

Risks and Threats ▪ examples	1 DB Pass	2 App Pass	3 Direct Access	4 App Sec Design	5 Extern App	6 Patch Policy	7 SQL Forms	8 Change Control	9 Audit	10 Pass Control
1. Sensitive data loss (data theft) ▪ Bulk download via direct access ▪ Bulk download via indirect access	●		●		●	◐		◐		
2. Direct entering of transactions (fraud) ▪ Update a bank account number ▪ Change an application password	●		●	●	◐		●	●	◐	●
3. Misuse of application privileges (fraud) ▪ Bypass intended app controls ▪ Access another user's privileges		●		●	◐	●			◐	●
4. Impact availability of the application ▪ Wipe out the database ▪ Denial of service (DoS)	●	◐	●		◐	●	◐	◐		

Oracle EBS Top 10 Security Vulnerabilities

1. Default Database Passwords
2. Default Application Passwords
3. Direct Database Access
4. Poor Application Security Design
5. External Application Access Configuration
6. Poor Patching Policies and Procedures
7. Access to SQL Forms in Application
8. Weak Change Control Procedures
9. No Database or Application Auditing
10. Weak Application Password Controls

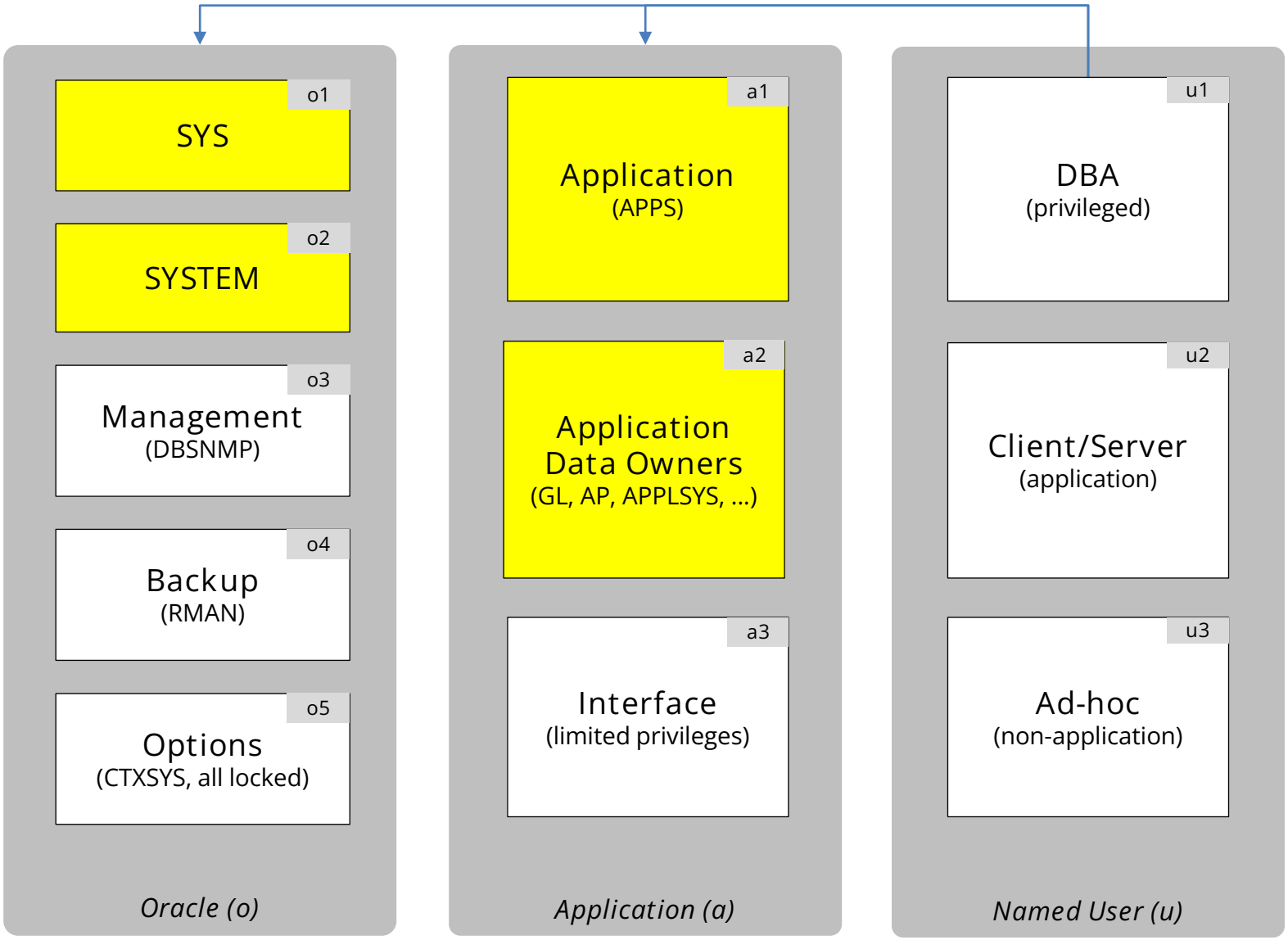
Oracle EBS Generic Privileged Accounts

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

30+ Seeded Generic Application Accounts

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	▪ SYSTEM_ADMINISTRATOR ▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	▪ MOBILE_ADMIN ▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	▪ ASG_MOBILE_ADMINISTRAOTR ▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	▪ OP_CUST_CARE_ADMIN
OP_SYSADMIN	OP_SYSADMIN	▪ OP_SYSADMIN
WIZARD	WELCOME	▪ AZ_ISETUP ▪ APPLICATIONS FINANCIALS ▪ APPLICATION IMPLEMENTATION

Integrigy Database Account Classification (Oracle)



What is Sensitive Data?

Payment Card Industry Data Security Standard (PCI-DSS 3.0)	▪ Credit Card Number
	  ▪ *Primary Account Number (PAN)*
	▪ CVV/CV2/CID (should not be stored)
	  ▪ *3 digits on the back for Visa/MC*
	  ▪ *4 digits on the front for AMEX*
	▪ Magnetic Stripe Data (should not be stored)

Privacy Regulations (employees, customers, vendors)	▪ First and last name
	▪ Plus most identifying numbers such as:
	  ▪ Social security number (SSN, Tax ID, 1099)
	  ▪ Credit card number
	  ▪ Bank account number
	  ▪ Financial account number
	  ▪ Driver license or state ID number

HIPAA (Privacy Standard and Security Rule)	▪ First and last name
	▪ Plus one of the following (Protected Health Information):
	  ▪ "the past, present, or future physical or mental health, or condition of an individual"
	  ▪ "provision of health care to an individual"
	  ▪ "payment for the provision of health care to an individual"

Where else might be Sensitive Data?

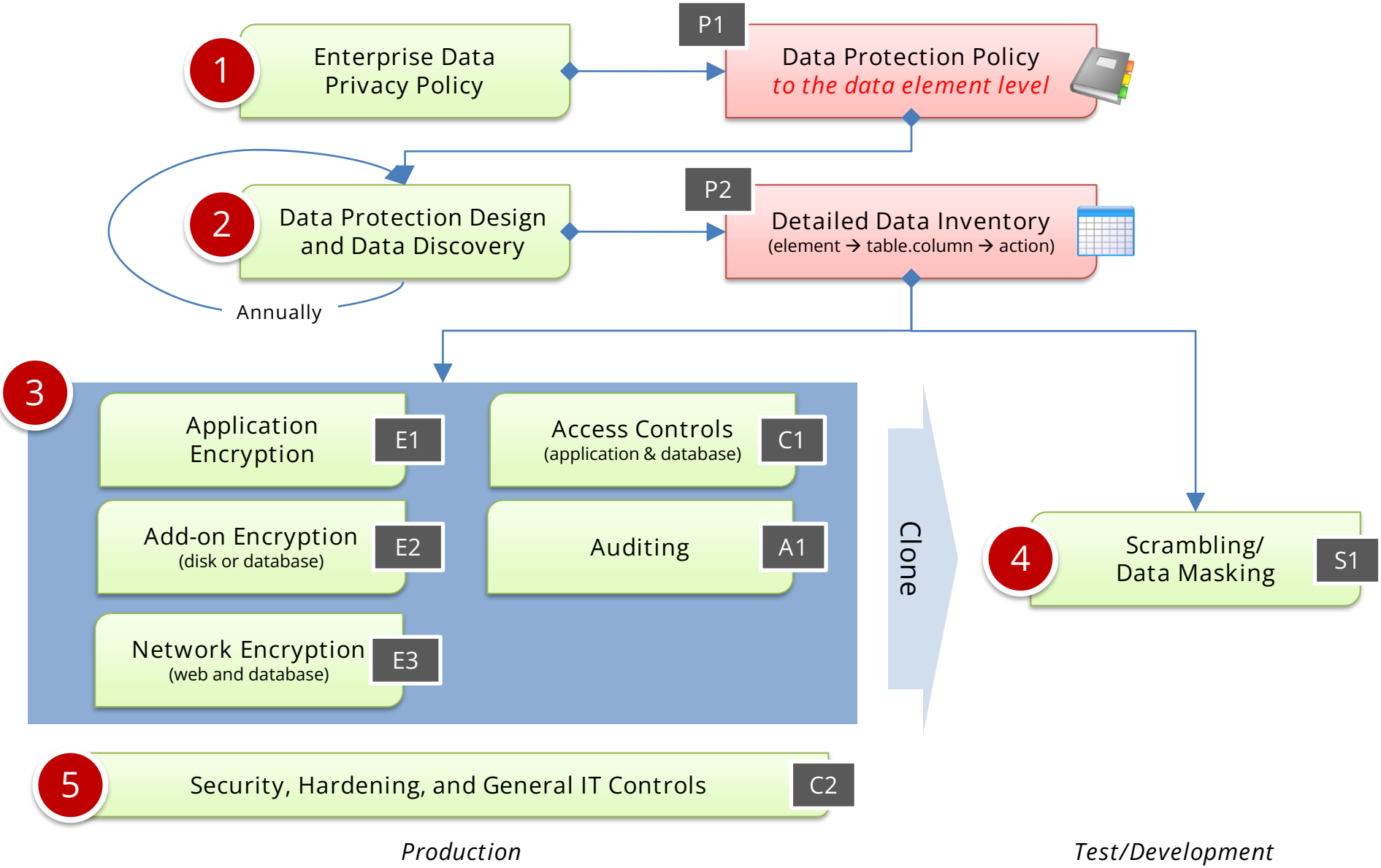
- Custom tables
  - Customizations to package applications may be used to store or process sensitive data
- "Maintenance tables"
  - DBA copies tables to make backup prior to direct SQL update
  - Names often like hr.per_all_people_f_011510
- Interface tables
  - Sensitive data is often transmitted between application and temporarily stored in interface tables – often gets stuck or archived

Database

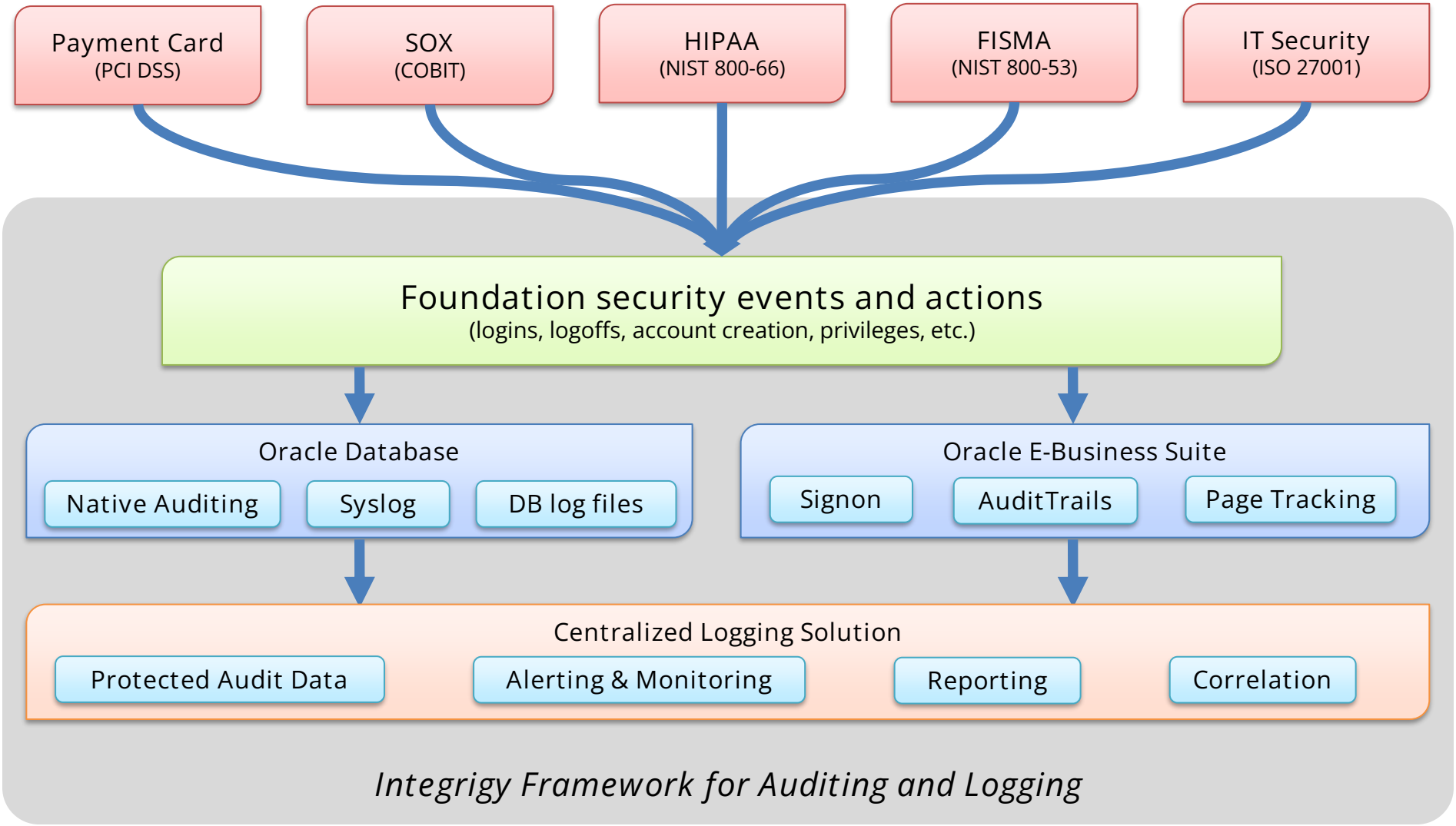
- Interface files
  - Flat files used for interfaces or batch processing
- Log files
  - Log files generated by the application (debug log of credit cards)

File System

How – Integrigy Data Protection Process



Integrigy Framework for Auditing and Logging



Foundation 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

Agenda

1 Integrigy Background

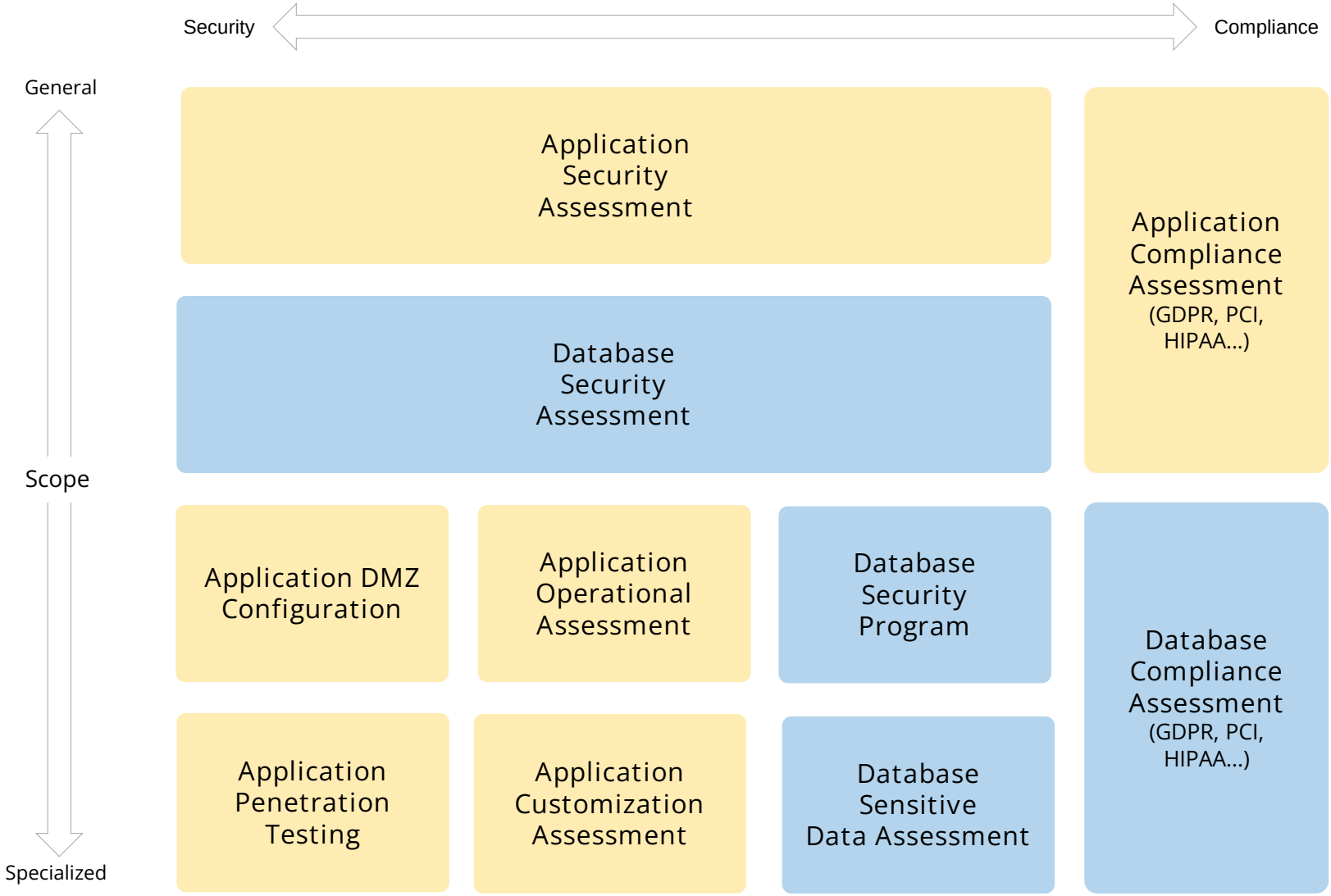
2 Oracle E-Business Suite Security

3 Assessment Services

4 Proposal

5 Q & A

Integrigy Assessment Services



Oracle EBS Security Assessment Scope

Oracle E-Business Suite	▪ user and system profile options ▪ application security patches (CPUs) ▪ application patches ▪ default application accounts and passwords	▪ application auditing ▪ application logging ▪ application user account analysis ▪ sensitive data discovery and privileges
Oracle Database	▪ database initialization parameters ▪ database security patches (CPUs) ▪ database patches ▪ database system/object/role privileges ▪ default database accounts and passwords ▪ database password management ▪ database access manager	▪ custom database accounts and schemas ▪ database links ▪ database auditing ▪ database logging ▪ listener configuration ▪ sensitive data protection
Oracle Application Server	▪ application server/Apache/J2EE configuration ▪ forms and report server ▪ application server configuration	▪ application server security patches (CPUs) ▪ application server patches ▪ application server logging
Operating System *(Unix and Linux)*	*Oracle EBS operating system specific* ▪ file permissions for application/database/application server files ▪ OS user accounts (oracle/applmgr)	▪ OS access ▪ OS patches ▪ OS configuration
Network	*Oracle EBS network specific* ▪ firewall configuration (open ports) ▪ load balancer	▪ reverse proxy ▪ web application firewall ▪ SSL configuration and termination

Oracle Database Security Assessment Scope

Oracle Database	▪ database initialization parameters ▪ database security patches (CPUs) ▪ database patches ▪ database system/object/role privileges ▪ default database accounts and passwords ▪ database password management ▪ database access manager	▪ custom database accounts and schemas ▪ database links ▪ database auditing ▪ database logging ▪ listener configuration ▪ sensitive data protection
Operating System *(Unix and Linux)*	*Oracle Database operating system specific* ▪ file permissions for application/database/application server files ▪ OS user accounts (oracle)	▪ OS access ▪ OS patches ▪ OS configuration
Network	*Oracle Database network specific* ▪ firewall configuration (open ports) ▪ network segmentation	

Oracle PeopleSoft Security Assessment Scope

PeopleSoft	▪ user and system profile options ▪ application security patches (CPUs) ▪ application patches ▪ default application accounts and passwords	▪ application auditing ▪ application logging ▪ application user account analysis ▪ sensitive data discovery and privileges
Oracle Database	▪ database initialization parameters ▪ database security patches (CPUs) ▪ database patches ▪ database system/object/role privileges ▪ default database accounts and passwords ▪ database password management ▪ database access manager	▪ custom database accounts and schemas ▪ database links ▪ database auditing ▪ database logging ▪ listener configuration ▪ sensitive data protection
Oracle WebLogic	▪ application server/Apache/J2EE configuration ▪ forms and report server ▪ application server configuration	▪ application server security patches (CPUs) ▪ application server patches ▪ application server logging
Operating System *(Unix and Linux)*	*PeopleSoft operating system specific* ▪ file permissions for application/database/application server files ▪ OS user accounts (oracle)	▪ OS access ▪ OS patches ▪ OS configuration
Network	*PeopleSoft network specific* ▪ firewall configuration (open ports) ▪ load balancer	▪ reverse proxy ▪ web application firewall ▪ SSL configuration and termination

Oracle EBS Security Assessment

Scope/Activities	▪ A detailed assessment to identify security issues and weaknesses in the Oracle EBS production technical environment (application, database, application server, operating system, and network) as it is installed, configured, maintained, and used. ▪ The three phase Security Assessment is a quantifiable, consistent, and thorough review of the state of the application and infrastructure security at a point in time. ▪ Reviews configurations, profiles, passwords, patches, default accounts & passwords, file permissions, privileges, database access, database auditing, sensitive data, etc.
Deliverables	▪ Detailed documented analysis of the environment providing an in-depth understanding of the security risks and weaknesses associated with the application and database. ▪ Actionable list of recommendations that will provide a foundation for a secure environment is included. ▪ Includes a detailed analysis of the current state of Oracle Critical Patch Updates (security patches) for the database, application server, and application along with a client based action plan for applying the missing security patches.

Operational Security Domains

		ERP Technical Components			
		Application	Database	Application Server	Operating System
Operational Processes	1. Application Security	1.1 User Management 1.2 System Admin SOD	1.3 Database Security 1.4 DBA SOD	1.5 Network and Web	1.6 OS Security
	2. Data Security	2.1 Data Management & Privacy	2.2 Database Access and Privileges	2.3 Web Access	2.4 File Permissions
	3. Auditing	3.1 Application Auditing	3.2 Database Auditing	3.3 Web Logging	3.4 OS Auditing
	4. Monitoring & Troubleshooting	4.1 Application	4.2 Database	4.3 Web and Forms	4.4 Operating System
	5. Change Management	5.1 Object Migrations 5.2 Application Configuration	5.3 Change Control 5.4 Database Configuration	5.5 Change Control	5.6 Change Control
	6. Patching	6.1 Application Patches	6.2 Database Patches	6.3 Application Servers Patches	6.4 OS Patches
	7. Development	7.1 Application	7.2 Database	7.3 Web 7.4 Web Services/SOA	7.5 Shell and File Transfer

Operational Assessment

- Inspection
  - Written policies and procedures and other documentation are reviewed to ascertain what are the stated policies and procedures
  - “how should it work”
- Collaborative Inquiry
  - Key personnel are interviewed to confirm the stated policies and procedures and management’s representations and to identify any known gaps or weaknesses
  - “how do people think it works”
- Testing and Validation
  - For each operational domain, tests and validations are performed to determine
  - “how does it actually work”

Assessment Assumptions

- Goal is to improve security, can't make it perfect
- Security is a cost/benefit proposition
  - Balance security objectives with operational realities
- Internal threat is greater than external threat
  - Insider knowledge and understanding of Oracle Applications is far greater and more dangerous
- Perimeter network is secure
  - Internal network is insecure
- Undisclosed security holes exist in Oracle E-Business Suite
  - Both known and unknown security bugs must be addressed

Critical Success Factors

- Complete
  - The assessment must be broad and deep in order to review the entire technology stack and application
- Accurate
  - All the information and recommendations must be precise and correct to allow for a rapid and thorough implementation of those recommendations
- Applicable
  - With the multitude of versions, modules, and configurations of Oracle Applications, the assessment must focus not only on the current state of the application but also address future patches, upgrades, and configuration changes.
- Effective
  - Changes to the configuration and installation must be supported and work with minimal effort and change.
- Efficient
  - The recommendations must able to be implemented in a cost effective and timely manner.

Technical Scope

- Oracle EBS Production Environment
  - Web servers, forms servers, concurrent manager servers, and database servers
- Oracle EBS Development Environments
  - Assessed using automated tools
  - Minimal manual testing
- Modules included in the scope of the project is only reviewed and assessed from a technical perspective
  - Functional and business activities are not in scope.
- Segregation of duties is only analyzed for System Administrator functions and responsibilities
  - Not for other module responsibilities or functions (GL, AP, etc.).

Automated Assessment Tools

- Integrigy AppSentry™
  - Application security scanner designed for Oracle E-Business Suite, Oracle Peoplesoft, Oracle WebLogic, and Oracle Database
  - 300+ security checks
  - Does not require any changes to the environment or software to be installed on servers – query only
  - No performance impact - Single threaded
- Integrigy Scrutinize Suite
  - Scrutinize/Java - Java code scanner to detect SQL injection, parameter tampering, cross site scripting
  - Scrutinize/PLSQL – Oracle PL/SQL code scanner to detect SQL injection
- Integrigy Jintplus
  - Capture of database information for automated and manual analysis
- Integrigy NetScan and TNSSpy
  - Analyzes Oracle E-Business Suite at the network level
- Nessus (optional)
  - Vulnerability scanner to identify OS level issues
- OWASP ZAP/Burp Suite (optional)
  - Web application proxy to test for issues in customizations

PCI Security Assessment

Scope/Activities	▪ A detailed security assessment to determine compliance to PCI-DSS for all layers of the Oracle EBS technology stack including application, database, and application server. Operating system and network configuration directly associated with the Oracle EBS are assessed. ▪ Evaluate existing operational controls against best practices and appropriate PCI compliance requirements. ▪ External network scan for Oracle EBS servers and review of external Oracle EBS configuration. ▪ This assessment may be used as an input to an annual QSA compliance audit or to assist in remediation of PCI issues identified during an audit.
Deliverables	▪ Detailed report with findings and actionable recommendations. All findings are directly mapped to the 12 PCI DSS compliance requirements.

PCI-DSS – Sample Mapping

#	Requirement	OS/Network	Oracle DB	Application
1	Use Firewall to protect data	1		
2	Do not use vendor-supplied defaults	3	3	2
3	Protect stored cardholder data			6
4	Encrypt across open, public networks	1		
5	Use Anti-virus software	1		
6	Develop and maintain secure applications	1	3	5
7	Restrict access to cardholder data		2	2
8	Assigned unique IDs for access	3	4	4
9	Restrict physical access to data			
10	Track and monitor access	7	6	6
11	Regularly test security	2	1	1
12	Maintain information security policy			

High Medium Low

External/DMZ Penetration Testing

Scope/Activities	▪ A white-box external penetration test of Oracle EBS external modules deployed in a DMZ environment, such as iSupplier, iStore, or iRecruitment, to identify weaknesses and security vulnerabilities in the deployment and configuration of the external Oracle EBS environment. The testing scope includes the network, firewalls, reverse proxy servers, application servers, and application. ▪ The penetration test fulfills compliance for PCI-DSS 1.2 requirement 11.3. ▪ A scan of external IP addresses will be performed to identify deployments of Oracle related servers and services.
Deliverables	▪ List of identified external hosts and ports ▪ Detailed report with all findings and recommendations, including detailed remediation steps for each finding and an action plan identifying immediate, short-term, and long-term remediation tasks.

External/DMZ Assessment

Scope/Activities	▪ A detailed assessment to identify security issues and weaknesses in the Oracle EBS when deployed externally in a DMZ environment. The assessment reviews the configuration of the network, firewalls, reverse proxy servers, application servers, and application to validate the configuration is per Oracle's configuration standard and Integrigy's best practices.
Deliverables	▪ Detailed report with all findings and recommendations, including detailed remediation steps for each finding and an action plan identifying immediate, short-term, and long-term remediation tasks.

Agenda

1 Integrigy Background

2 Oracle E-Business Suite Security

3 Assessment Services

4 Proposal

5 Q & A

Integrigy Assessment Proposal

- Oracle E-Business Suite Security Assessment
  - Production Oracle E-Business Suite environments
  - Application, database, application server, OS, network
  - Report deliverable per environment plus consolidated findings
  - Fixed bid assessment
    - 5 – 7 days per production environment
    - 2 – 3 month duration
    - One week on-site, following weeks remote

Integrigy Assessment Proposal Options

- Oracle EBS PCI Assessment
  - Detailed PCI assessment with mapping to PCI-DSS
  - Pre-work for QSA assessment or PCI Questionnaire
- Oracle EBS Custom Code Review
  - Review customizations including web pages, forms, and interfaces for security vulnerabilities such as SQL injection
- Oracle EBS External DMZ Detail Review
  - “White-box” penetration testing, code review of custom external web pages, and configuration review

PCI-DSS – Sample Mapping

#	Requirement	OS/Network	Oracle DB	Oracle EBS
1	Use Firewall to protect data	1		
2	Do not use vendor-supplied defaults	3	3	2
3	Protect stored cardholder data			6
4	Encrypt across open, public networks	1		
5	Use Anti-virus software	1		
6	Develop and maintain secure applications	1	3	5
7	Restrict access to cardholder data		2	2
8	Assigned unique IDs for access	3	4	4
9	Restrict physical access to data			
10	Track and monitor access	7	6	6
11	Regularly test security	2	1	1
12	Maintain information security policy			

High Medium Low

Integrigy Contact Information

Integrigy Corporation

web – www.integrigy.com

e-mail – info@integrigy.com

blog – integrigy.com/oracle-security-blog

youtube – youtube.com/integrigy