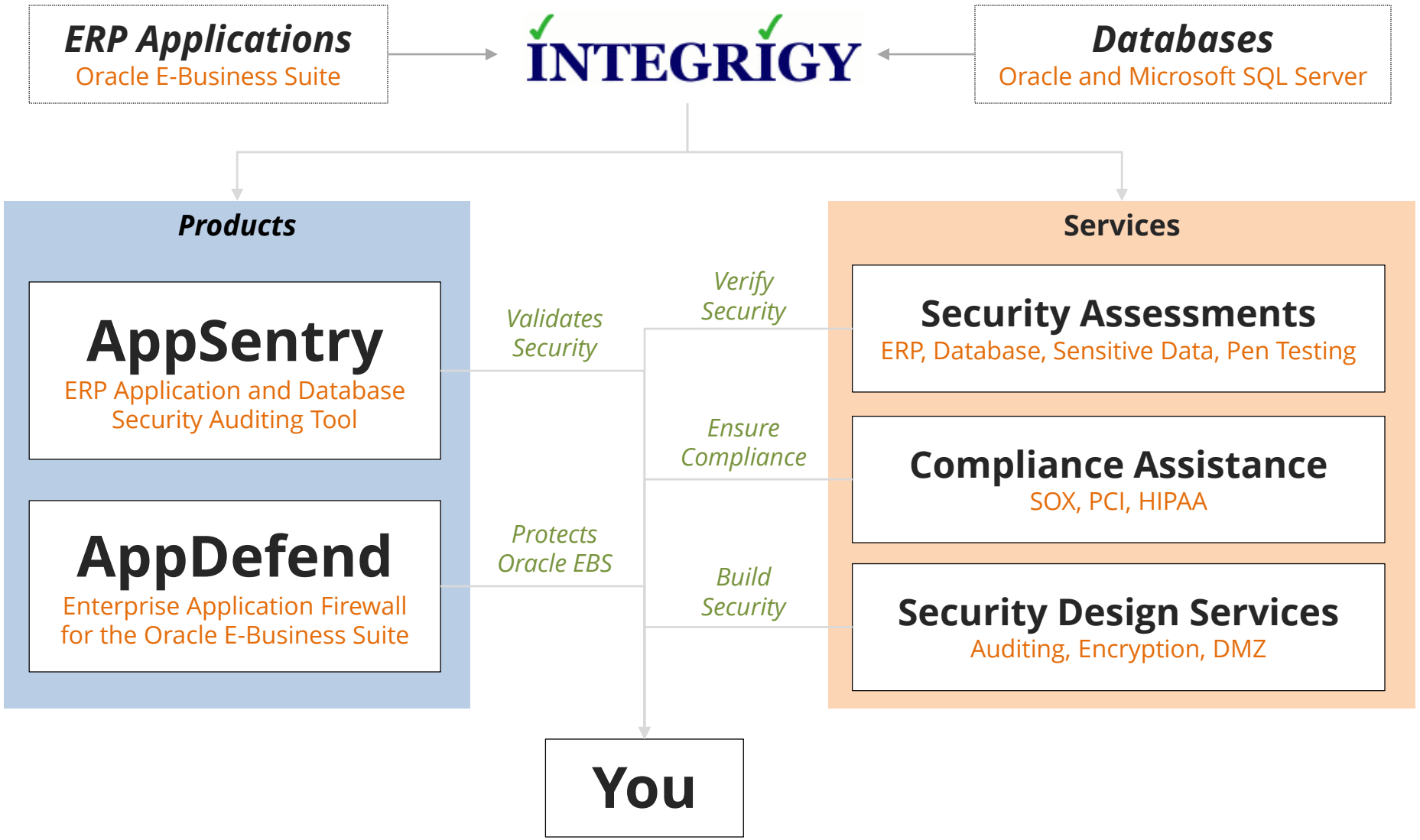
Integrigy Consulting Overview

Database and Application Security
Assessment, Compliance, and Design Services

March 2016

mission critical applications …
… mission critical security

About Integrigy



Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
Critical Patch Update July 2012	11.5.10 – 12.1.x	▪ Oracle E-Business Suite XSS
Critical Patch Update July 2011	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security configuration issue
Critical Patch Update October 2010	11.5.10 – 12.1.x	▪ 2 Oracle E-Business Suite security weaknesses
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	▪ 2 Issues in Oracle RDBMS Authentication ▪ 2 Oracle E-Business Suite vulnerabilities
Critical Patch Update April 2008	12.0.x 11.5.7 – 11.5.10	▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.0.x, 11.5.1 – 11.5.10	▪ Default configuration issues
Critical Patch Update July 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update April 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update Jan 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	11.0.x, 11.5.1 – 11.5.8	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.0.x, 11.5.1 – 11.5.8	▪ Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	▪ Multiple vulnerabilities in AOL/J Setup Test ▪ Obtain sensitive information (valid session)
Oracle Security Alert #53	10.7, 11.0.x 11.5.1 – 11.5.8	▪ No authentication in FNDFS program ▪ Retrieve any file from O/S

Consulting Services Overview

Oracle E-Business Suite

- **Application Security Assessment**
- **PCI Security Assessment**
- **Operational Assessment**
- **External/DMZ Security Assessment**

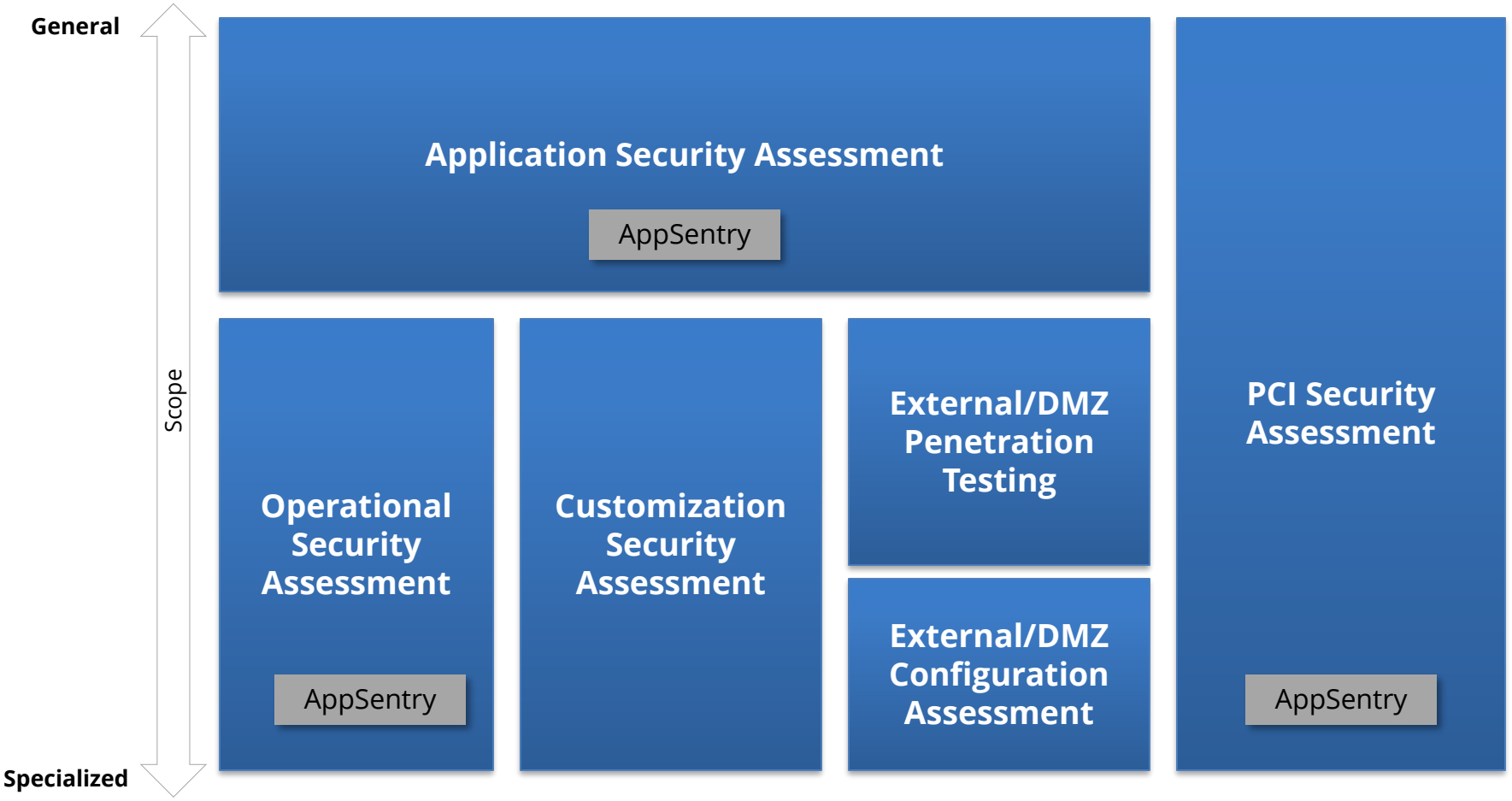
Oracle Database

- **Database Security Assessment**
- **PCI Security Assessment**
- **Database Security Strategy and Standards**
- **Database Auditing Strategy and Design**

Oracle E-Business Suite

Security Services

Oracle EBS Security Services



Application 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.

Application Security Assessment Overview

- **The goal of the application security assessment is to identify security issues and weaknesses in the Oracle Applications production technical environment as it is installed, configured, maintained, and used**

- **The assessment is a quantifiable, consistent, and thorough review of the state of the application and infrastructure security at a point in time**
  - Findings will be reflective of the current state of security

- **The deliverable is an actionable list of recommendations that will provide a foundation for a secure environment**

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 Applications**
  - Both known and unknown security bugs must be addressed

Assessment 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.

Assessment Phases

- **Phase 1 – Planning and Information Gathering**
  - Review of documentation
  - Interviews with key IT resources
- **Phase 2 – Testing**
  - Test/QA instance is analyzed first, then production
  - Automated scanning
  - Manually testing
  - Review of customizations
- **Phase 3 – Analysis and Reporting**
  - Review and correlation of data and findings
  - Development of report

Technical Scope

- **Oracle Applications Production Environment**
  - Web servers, forms servers, concurrent manager servers, and database servers
- **Oracle Applications 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.).

Technical Scope

- **Network infrastructure associated with Oracle Applications to determine appropriateness for the Oracle implementation**
- **Operating system (Unix, Linux, Windows) installation and configuration for each server to assess the security related to Oracle Applications**
- **All Oracle Applications Modules**
  - with the following exceptions –
    - CRM Interaction Center (Call Center, Telephony, Scripting, Email Center, etc.)
    - Mobile and Palm Solutions (Field Sales, Field Service, Gateway for Mobile Devices, etc.)
    - Credit Card Processing Integration (iPayment Integration with backend systems – Cybercash, First Data Corp., etc.)
    - Industry Solutions (Automotive, Clinical, i2, etc.)
    - Data Warehousing (Clickstream Intelligence, Warehouse Builder, Data Mart Suite, etc.)

Operational Security Assessment

Scope/Activities	▪ Operational activities (security management, auditing, monitoring and trouble-shooting, change management, patching, and development) as defined in 27 Security Domains, are assessed to determine any security or control weaknesses. ▪ Written security policies and procedures are reviewed to ascertain how they should work, follow by interviews to determine how people think it works, followed by actual testing to determine how it actually works.
Deliverables	▪ Detailed report with all findings and recommendations, including complete remediation steps for each finding and an action plan identifying immediate, short-term, and long-term remediation tasks. ▪ All findings and recommendations are mapped to security best practices such as ISO 27001 and COBIT.

Operational Security Assessment

- **Operational activities related to the Oracle Applications environment are assessed to determine if there are security or controls weaknesses**
  - Security management, auditing, monitoring and troubleshooting, change management, patching, and development are assessed for the Oracle Applications, database, application servers, and operating system
- **Operations specific to Oracle Applications are categorized into 27 domains**
  - Domains are individually assessed
  - Domains are mapped to ISO 17799/27002, COBIT, and NIST 800-53
  - Interview questions and tests/validations for each domain are defined in the assessment methodology

Operational Security Domains

Operational Processes	Oracle E-Business Suite Technical Components			
	Oracle E-Business Suite	**Database**	**Application Server**	**Operating System**
1. Application Security	1.1 User Management	1.3 Database Security	1.4 Network and Web	1.5 OS Security
	1.2 Segregation of Duties			
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	5.3 Change Control	5.5 Change Control	5.6 Change Control
	5.2 Application Configuration	5.4 Database Configuration		
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	7.5 Shell and File Transfer
			7.4 Web Services/SOA	

Operational Assessment

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

Customization Security Assessment

Scope/Activities	▪ All or a sample set of customizations are reviewed from a design and source code perspective to identify any potential security flaws, including SQL injection, cross-site scripting (XSS), and privilege escalation. ▪ The assessment scope will include all major customizations including but not limited to interfaces and integrations, custom web pages, custom forms, custom reports, and bolt-on's. ▪ A set of proprietary tools is used to initially scan customized source code to identify potential risk areas followed by a detailed manual source code review.
Deliverables	▪ Threat analysis for each type of customization. ▪ Listing of customizations identified during assessment and the customizations reviewed with a risk rating assigned to each customization. ▪ Detailed report with findings and recommended remediation per customization.

Customization Assessment

- **All customizations assessed from a design and source code perspective**
  - interfaces
  - web customizations
  - custom forms
  - reports
- **Customization design assessed to determine any security issues inherent in the design and implementation of the customization**
- **Customization source code is reviewed to identify any potential security flaws in the implementation of the customization, which may include SQL injection, cross-site scripting, parameter tampering, information disclosure, and improper or missing authentication**

Automated Assessment Tools

- **Integrigy AppSentry**
  - Application security scanner designed for Oracle Applications, Oracle Application Server, 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/Forms – Oracle Forms code scanner to detect SQL injection
  - Scrutinize/PLSQL – Oracle PL/SQL code scanner to detect SQL injection

- **Integrigy Intplus**
  - Capture of database information for automated and manual analysis

- **Integrigy NetScan and TNSSpy**
  - Analyzes Oracle Applications at the network level

- **Nessus**
  - Vulnerability scanner to identify OS level issues

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 Compliance 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

PCI-DSS Compliance Example

- **PCI 6.1 – *"Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release."***
- **Few Oracle customers install patches within 30 days**
- **Most customers are 1 to 2 quarters behind**
- **Business must prioritize applying security patches – effort to functionally test and apply, down-time**
- **Recommendations for patching and mitigating controls to satisfy requirement**
- **See Integrigy Whitepaper "Oracle E-Business Suite: Credit Cards and PCI Compliance Issues"**

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 Configuration 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.

Oracle Database Security Services

Database Security Assessment

Scope/Activities	▪ A detailed assessment to identify security issues and weaknesses in the Oracle Database 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 access, etc.
Deliverables	▪ Detailed documented analysis of the environment providing an in-depth understanding of the security risks and weaknesses associated with the 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 along with a client based action plan for applying the missing security patches.

Database PCI Security Assessment

Scope/Activities	▪ A detailed security assessment to determine compliance to PCI-DSS for the Oracle Database. Operating system and network configuration directly associated with the Oracle Database are assessed. ▪ Evaluate existing operational controls against best practices and appropriate PCI compliance requirements. ▪ 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.

Database Security Strategy & Standards

Scope/Activities	▪ Develop a comprehensive database security strategy and security standards to address all aspects for database security including secure configuration, account and password controls, security patching, auditing, monitoring, and encryption. ▪ Database security strategy and standards will address business, compliance, and security requirements, including SOX, PCI, and HIPAA. ▪ Security standards will be designed to be readily implementable and address application and organizational specific limitations.
Deliverables	▪ Database Security Strategy. ▪ Database Security Standards. ▪ Action plan to implement strategy.

Database Auditing and Monitoring Strategy

Scope/Activities	▪ Develop a database auditing and monitoring strategy based on business, compliance, and security requirements. ▪ Map security and compliance requirements including SOX, PCI, and HIPAA to detailed auditing. ▪ Minimize potential auditing and monitoring performance and operational impact through a carefully designed set of auditing techniques.
Deliverables	▪ Database Auditing and Monitoring Strategy. ▪ Action plan to implement strategy.

Contact Information

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

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

phone: **888-542-4802**