Application and Database Security Auditing, Vulnerability Assessment, and Compliance

Integrigy Corporate Overview

INTEGRIGY

Integrigy Overview

- **Integrigy Corporation specializes in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. Integrigy Consulting offers security assessment services for leading databases and ERP/CRM.**

- **Corporate Details**
  - Founded December 2001
  - Privately Held
  - Based in Chicago, Illinois

INTEGRIGY

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 Oracle Applications than anyone else inside or outside of Oracle
- **Both an ERP/CRM company and a security company**
  - Products developed to support and enhance an ERP/CRM implementation – Integrigy understands the issues and risks challenging large ERP/CRM implementations
  - Integrigy bridges the gap between applications, databases, and security

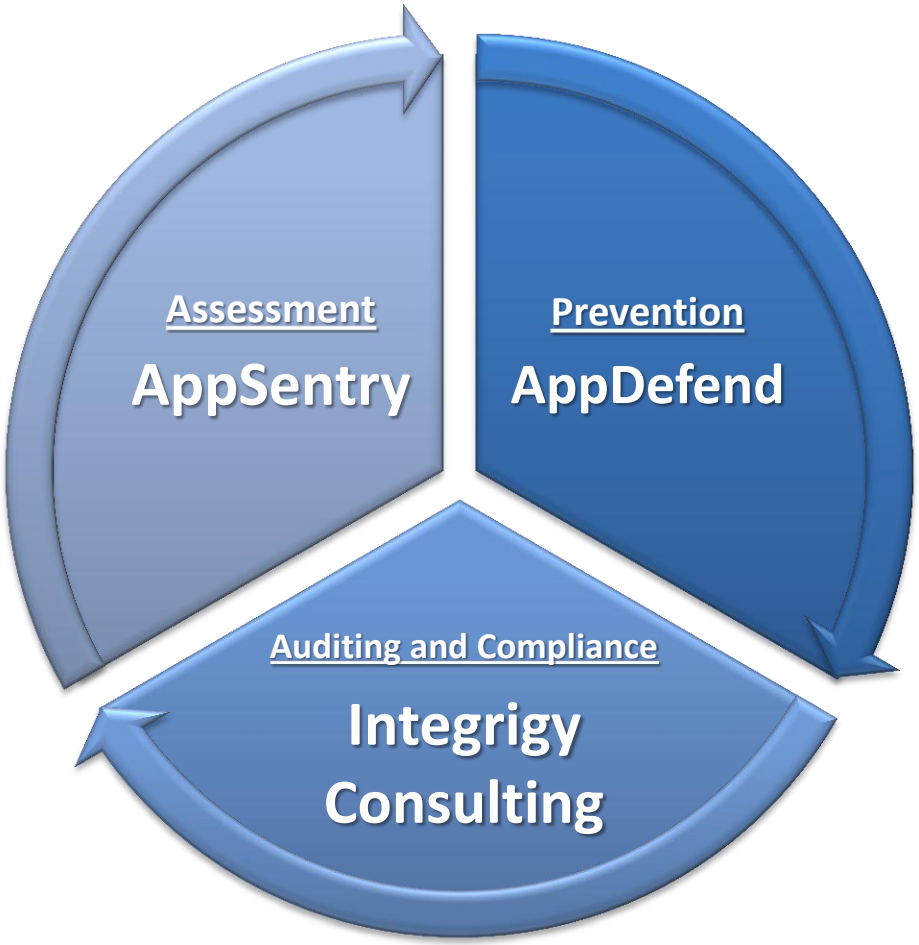
INTEGRIGY

Integrigy Security Alerts

Security Alert	Versions	Security Vulnerabilities
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	**11.5.1 – 11.5.10** **11.0.x**	▪ 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	**11.5.1 – 11.5.8** **11.0.x**	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	**11.5.1 – 11.5.8** **11.0.x**	▪ 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

INTEGRIGY

Integrigy Offerings



INTEGRIGY

Integrigy's Products

AppSentry™

- Security scanner for databases, application servers, and ERP packages
- Performs advanced penetration testing and in-depth security and controls auditing
- Performs over 300+ audits and checks on Oracle products
- Runs on any Windows PC and requires no software to be installed on the target servers

AppDefend™

- Application firewall and intrusion prevention system for ERP packages
- Blocks common attacks like SQL injection, session hijacking, and cross site scripting
- Blocks access to unimplemented Oracle Applications modules
- Runs as an Apache modules and scans all incoming web requests

INTEGRIGY

AppSentry

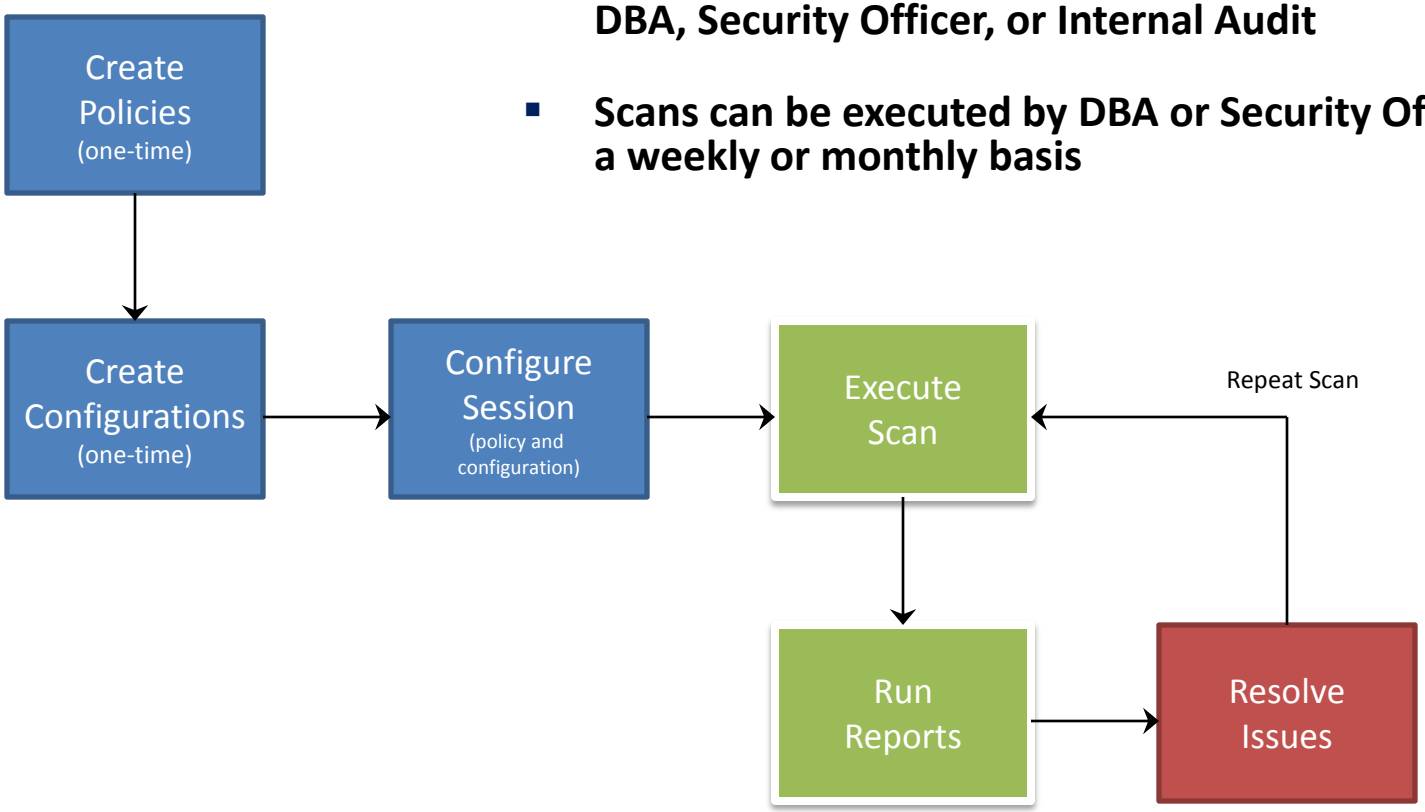
- **Security Scanner for databases, application servers, and ERP/CRM Applications**
  - Validates security of network, operating system, web server, database, and application
  - Modular design with distributed GUI and centralized server
  - Security checks written in XML and Java
  - Automatic program and security check updates

  - In-depth security and controls auditing
  - Advanced penetration testing
  - Scanning of open network ports for well-known and application specific vulnerabilities
  - Validation of application and technology stack configuration by analyzing configuration files, logs, and file versions
  - Analysis of users and roles to isolate segregation of duty issues
  - Transaction auditing to detect possible fraud

INTEGRIGY

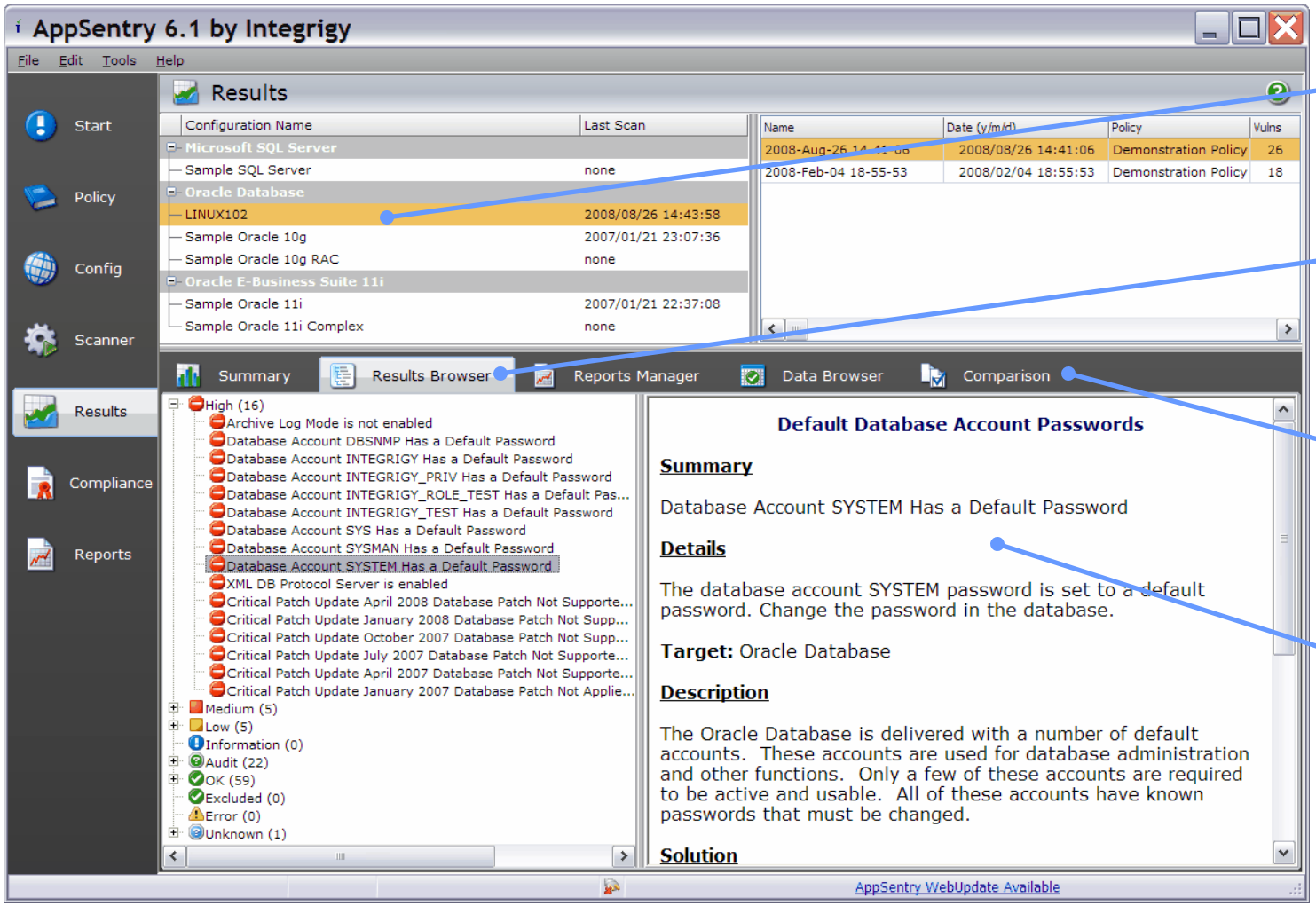
AppSentry Workflow

- **Quick and simple workflow**
- **Policies and configurations are created once by DBA, Security Officer, or Internal Audit**
- **Scans can be executed by DBA or Security Officer on a weekly or monthly basis**



INTEGRIGY

AppSentry – Screenshot



Results from all scans can be reviewed at any time

Results can be browsed or reports run

Comparisons can be run against any previous scan

Each finding includes a detailed description and solution

INTEGRIGY

AppSentry Modules - Current

Database/Web Server/Application	Supported Versions
Oracle E-Business Suite	▪ 11i (11.5.1 – 11.5.10 CU2) ▪ R12 (12.0, 12.1)
Oracle Database	▪ 8i (8.1.7) ▪ 9i (9.0.1, 9.2.0) ▪ 10g (10.1, 10.2) ▪ 11g (11.1, 11.2)
Oracle Application Server	▪ 9iAS (1.0.2, 9.0.2, 9.0.3) ▪ 10g (9.0.4, 10.1, 10.2)
Microsoft SQL Server	▪ 2000 ▪ 2005 ▪ 2008

INTEGRIGY

AppSentry Modules - Development

Database/Web Server/Application
Oracle PeopleSoft
SAP
Oracle Collaboration Suite
Oracle Clinical
Oracle Retail
Oracle Siebel
IBM DB2
Sybase
Apache (AppSentry Open-Source Edition)
Oracle WebLogic

INTEGRIGY

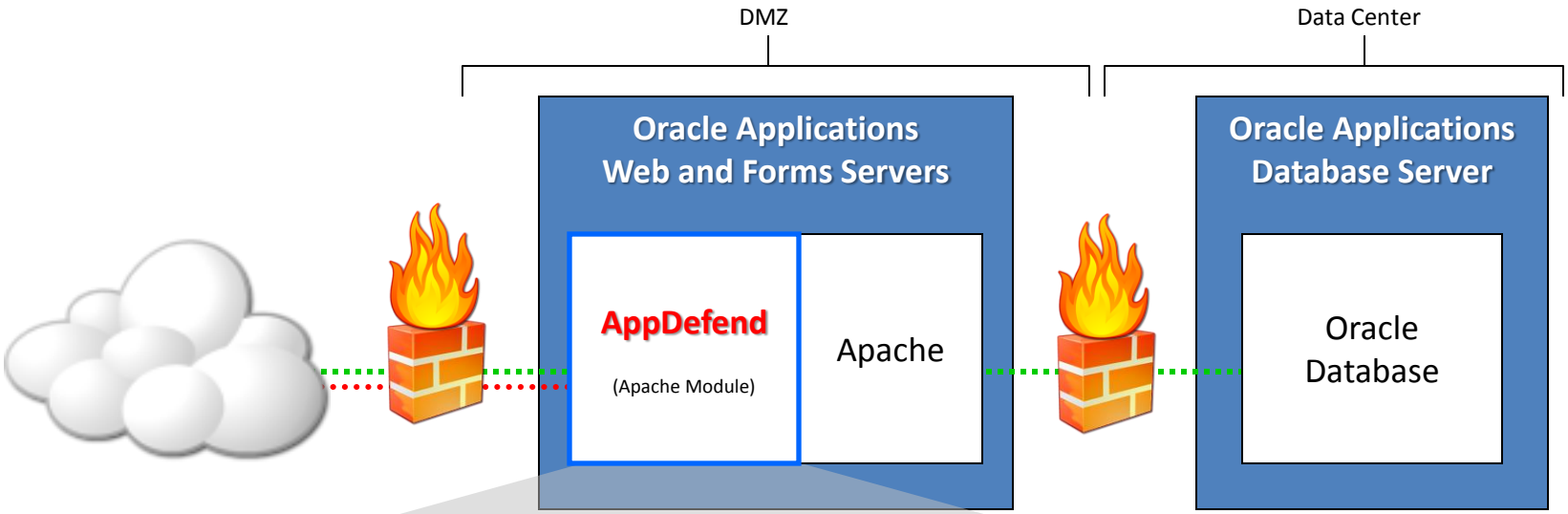
AppDefend

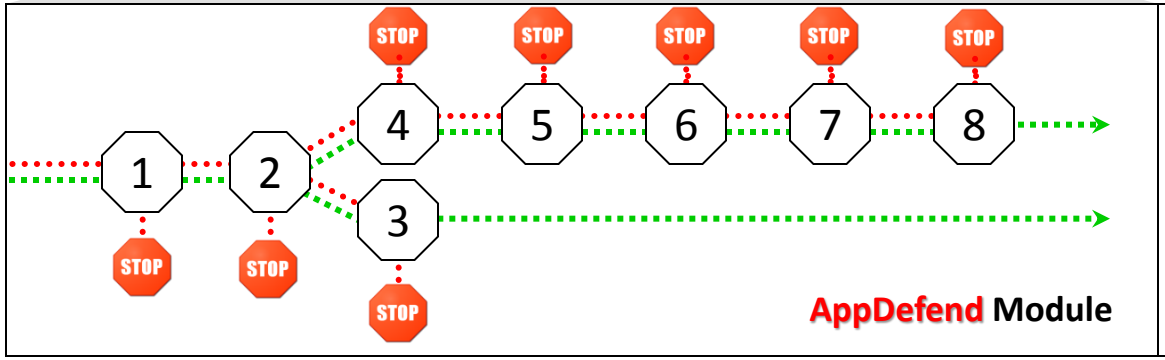
- **Application-level intrusion prevention system for the ERP/CRM Applications**
  - Scans all incoming web requests for common web application vulnerabilities including –
    - SQL Injection
    - Cross Site Scripting
    - Session Hijacking
  - Blocks unused CGI-Bin programs and sample applications
  - Users can specify filters to block other programs or files

- **AppDefend for the Oracle E-Business Suite**
  - Blocks published and un-published Oracle Applications security vulnerabilities
  - Permits access to only enabled/installed Oracle Applications Modules
    - Oracle Applications delivered with 12,000 accessible Java Server Pages and Java servlets, even though only a 1,000 or fewer may be used by the customer
  - Implemented as an Apache module

INTEGRIGY

AppDefend Architecture





1. Method Check
2. Static/Dynamic
3. Static Deny List
4. Dynamic Deny List
5. Module Permit List
6. Length Byte Check
7. SQL Injection Check
8. XSS Scripting Check

INTEGRIGY

AppDefend vs. Traditional IDS/IPS

AppDefend	Traditional IDS/IPS
▪ Designed for Oracle Applications – highly specialized rules in-place with the default configuration	▪ Must be heavily customized for Oracle Applications – rules must be developed and tested
▪ Blocks unused Oracle Applications modules	▪ Complex configuration required to block unused Oracle Applications modules
▪ 30 minute installation and configuration	▪ Significant effort and skill required to deploy and configure
▪ Scans entire web request including POST	▪ Many IDS/IPS solutions do not scan POST data
▪ AppDefend is distributed to each application server for resiliency and performance	▪ Potential single point of failure and a possible performance bottleneck

INTEGRIGY

AppDefend for the Oracle E-Business Suite

- **Oracle E-Business Suite**
  - 11.5.7 – 11.5.10.2, R12
    - 11.5.1 and 11.5.7 not supported due to Oracle desupport
  - Industry Verticals (Automotive, Clinical, Exchange)
  - AutoConfig and non-AutoConfig implementations supported
  - Apache 1.3.9, 1.3.12, and 1.3.19

- **Supported Operating Systems**
  - Sun SPARC Solaris 2.6, 8, and 9
  - HP PA-RISC HP/UX 11.0 and 11.11
  - IBM AIX 4.3.2, 4.3.3, and 5L
  - Linux x86
    - Red Hat Enterprise Linux AS/ES 2.1 and AS/ES 3
    - SuSe 7.0, 7.1, 7.2, SLES7, and SLES8
    - United Linux 1.0

INTEGRIGY

Integrigy Consulting

- **Integrigy Consulting provides on-site security audit and assessment services for databases and applications, including penetration testing and vulnerability assessments**

- Application Security Assessment for the Oracle E-Business Suite
- Database Security Assessment for Oracle and SQL Server
- Oracle E-Business Suite Security Design, Configuration, and Testing
- Oracle E-Business Suite Internet Deployment Penetration Testing

INTEGRIGY

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**

INTEGRIGY

Application Assessment Technical Scope

- **Oracle Applications Production Environment**
  - Web servers, forms servers, concurrent manager servers, and database servers
- **Oracle Applications Development Environments**
  - Assessed using Integrigy's AppSentry assessment tool
  - 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.).

INTEGRIGY

Application Customization Assessment

- **All customizations assessed from a design and source code perspective**
  - web customizations
  - interfaces
  - 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**

INTEGRIGY

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 and COBIT
  - Interview questions and tests/validations for each domain are defined in the assessment methodology

INTEGRIGY

Operational Security Domains

Operational Processes	Oracle Applications	Database	Application Server	Operating System
	Oracle Applications Technical Components			
1. Security	1.1 User Management	1.3 Database Security	1.4 Network and Web	1.5 OS Security
	1.2 Segregation of Duties			
2. Auditing	2.1 Application Auditing	2.2 Database Auditing	2.3 Web Logging	2.4 OS Auditing
3. Monitoring and Troubleshooting	3.1 Application	3.2 Database	3.3 Web and Forms	3.4 Operating System
4. Change Management	4.1 Object Migrations	4.3 Change Control	4.5 Change Control	4.6 Change Control
	4.2 Application Configuration	4.4 Database Configuration		
5. Patching	5.1 Application Patches	5.2 Database Patches	5.3 Application Server Patches	5.4 OS Patches
6. Development	6.1 Application	6.2 Database	6.3 Web	6.4 Shell and File Transfer

INTEGRIGY

Integrigy Contact Information

Integrigy Corporation P.O. Box 81545 Chicago, Illinois 60681 888/542-4802	Website: www.integrigy.com Sales: sales@integrigy.com Development: development@integrigy.com Support: support@integrigy.com Security Alerts: alerts@integrigy.com

INTEGRIGY