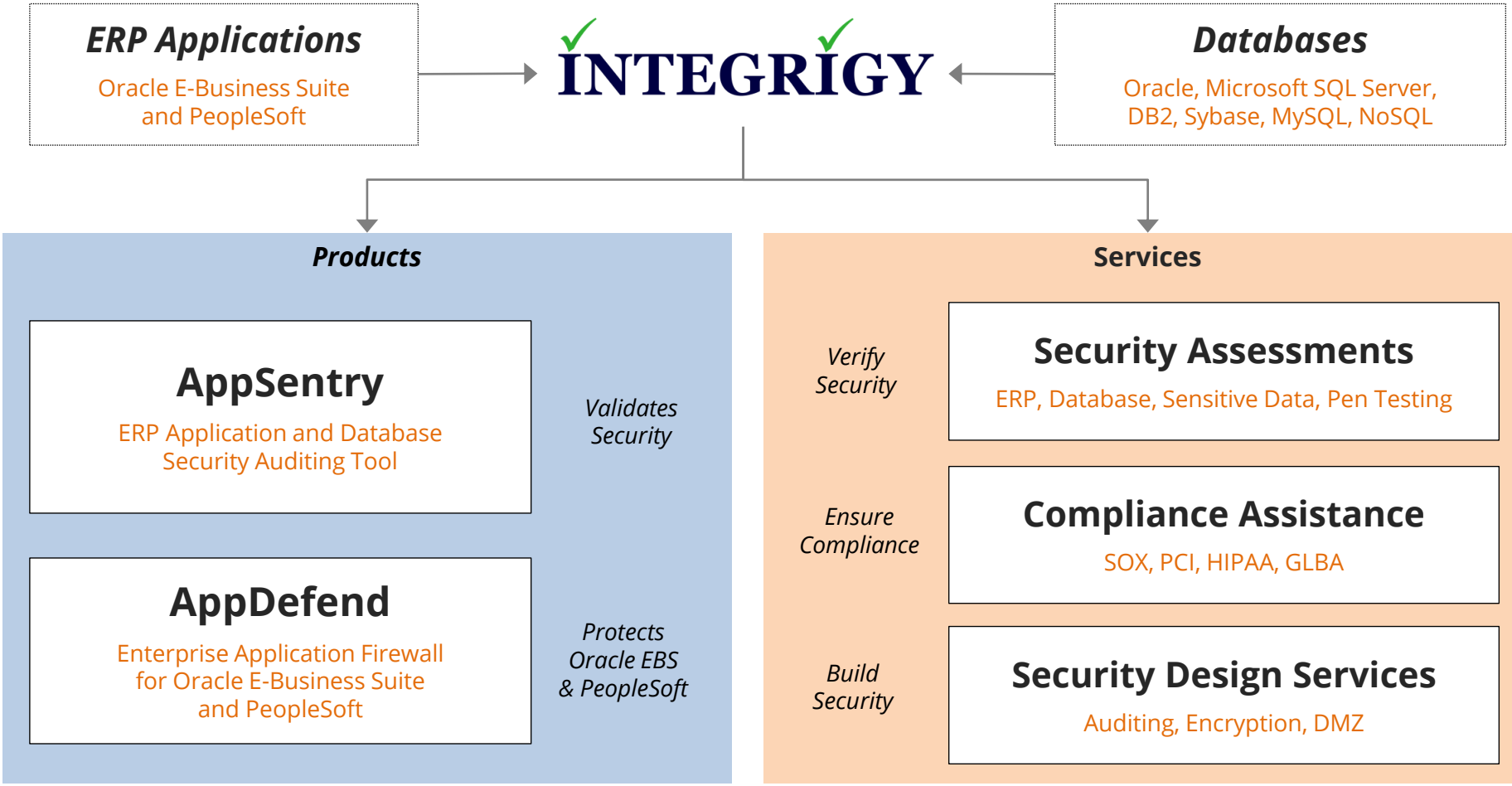
Eight Key Components of a Database Security Risk Assessment

September 17, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Database Security Risk Assessment

1. An objective analysis of the **effectiveness of the current security controls** that protect a database.

2. A determination of the **likelihood of compromise** or loss of the data stored in the database.

3. Recommended **mitigation to improve the security controls** that protect the database.

Database Security Risk Assessment

- **More than a database security scan**
  - Review, analysis, and interviews are required to assess the actual effectiveness of security controls
  - Oracle DBSAT (Database Security Assessment Tool) reports are titled “Database Security Risk Assessment” but are just a snapshot
- **More than a database security product recommendation**
  - Must address security policies, operational procedures, database design, and privilege assignments
  - There is no silver-bullet for database security
- **Context of the database matters**
  - The type, quantity, and sensitivity of the data in the database drives the security risk assessment
  - A database with no ad-hoc users is inherently more secure than one with thousands of users

Database Security Issues

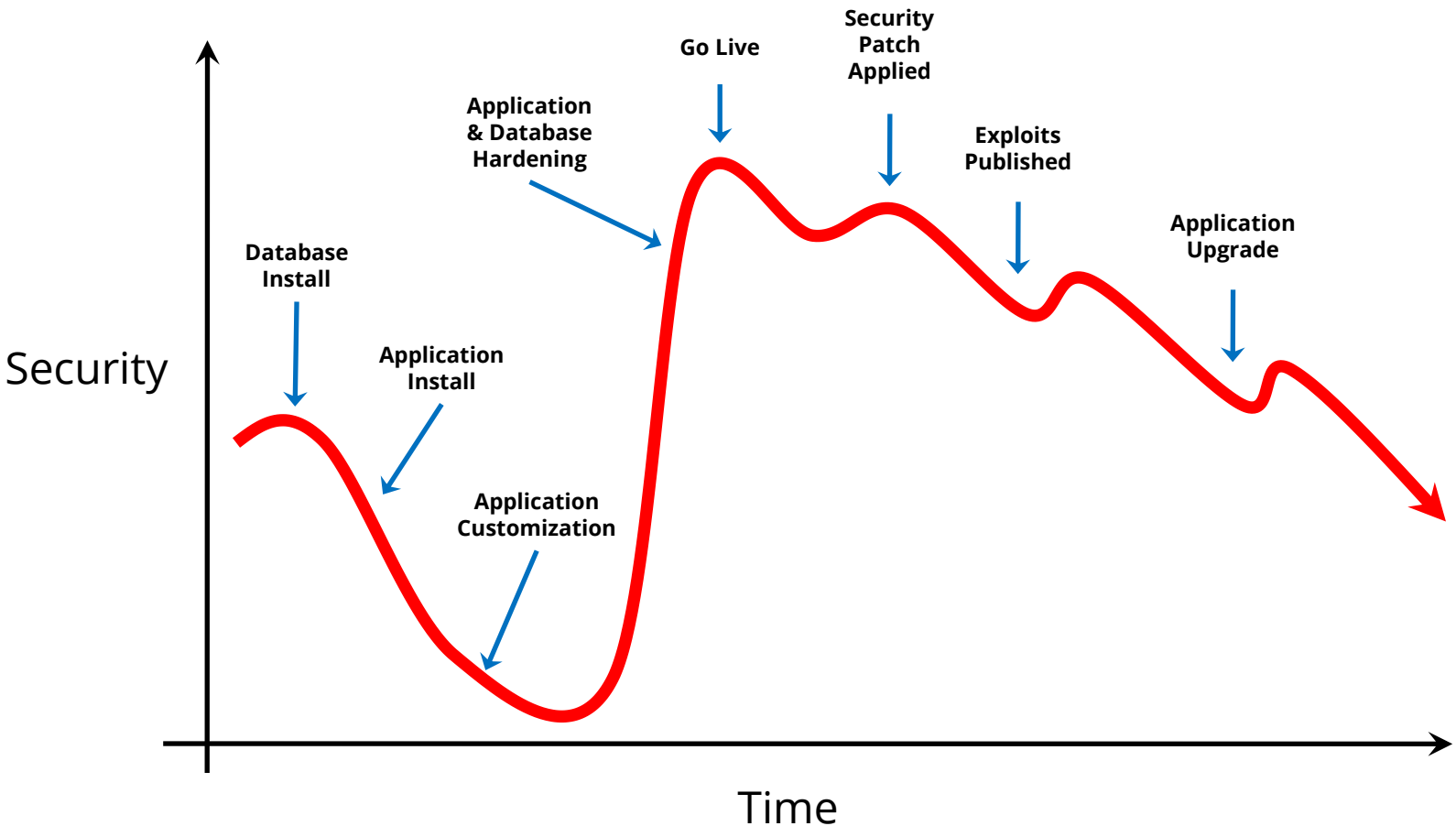
- **Database security is dependent on and coupled with the application**
  - Application determines data model, privileges, and in many cases version, patching, and configuration
- **Application architecture and design complicate many aspects of database security**
  - Application developers are application developers – not data architects or DBAs
- **Application and business requirements dictate database upgrades and security patching**
  - Old database versions may be at significantly more risk
  - Database security patches may not be applied due to operational constraints or lack of vendor support
  - Missing security patches drives the number of open and unpatched vulnerabilities

Database Security Dynamic

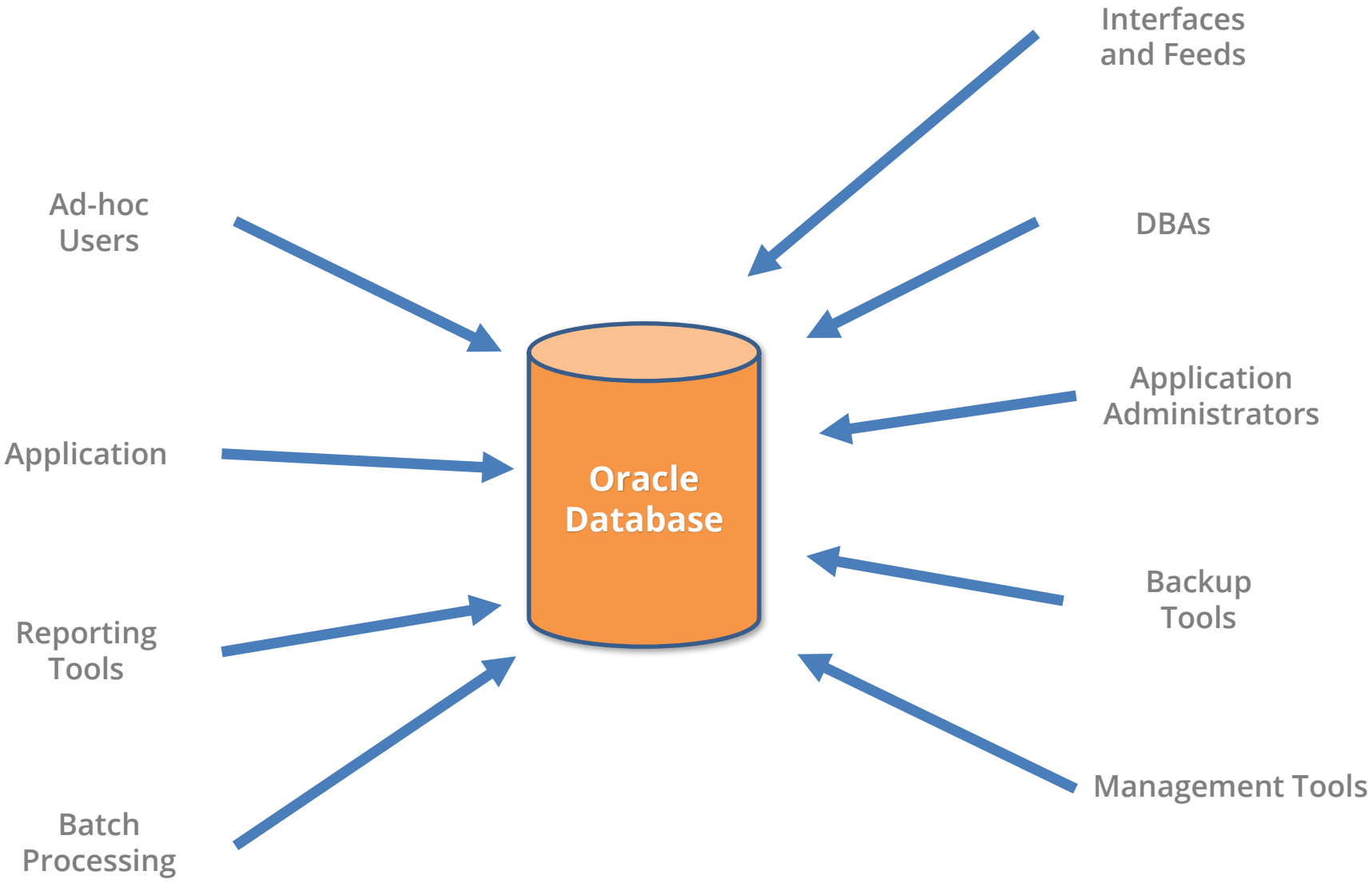
Snowflakes	▪ Databases are installed one by one to support new applications – not like servers and desktops ▪ Version, configuration, and installer may be different per database install ▪ Database configuration, data model, access patterns, and privileges are driven by the application
Evolutionary	▪ Databases are installed one by one ▪ Application heavily influences the database upgrade and patching cycles ▪ Databases may live for long periods (5, 10, 20 years) ▪ Database population may have distinct sub-groups based versions, acquisitions, even DBA manager

Database Security Decay

Database security decays over time due to complexity, usage, application changes, upgrades, published security exploits, etc.



Database connectivity is a complex problem

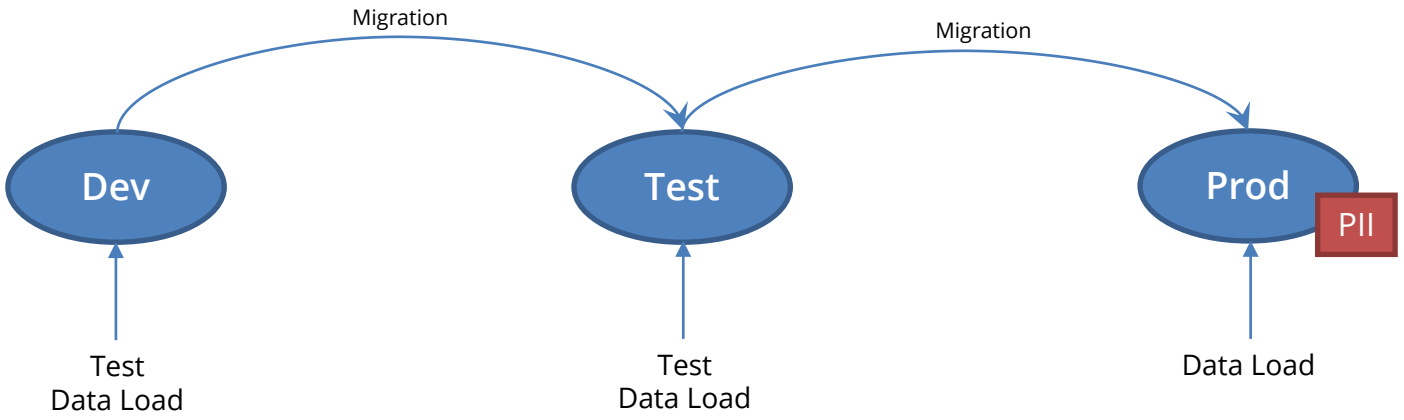


Assessment Scope

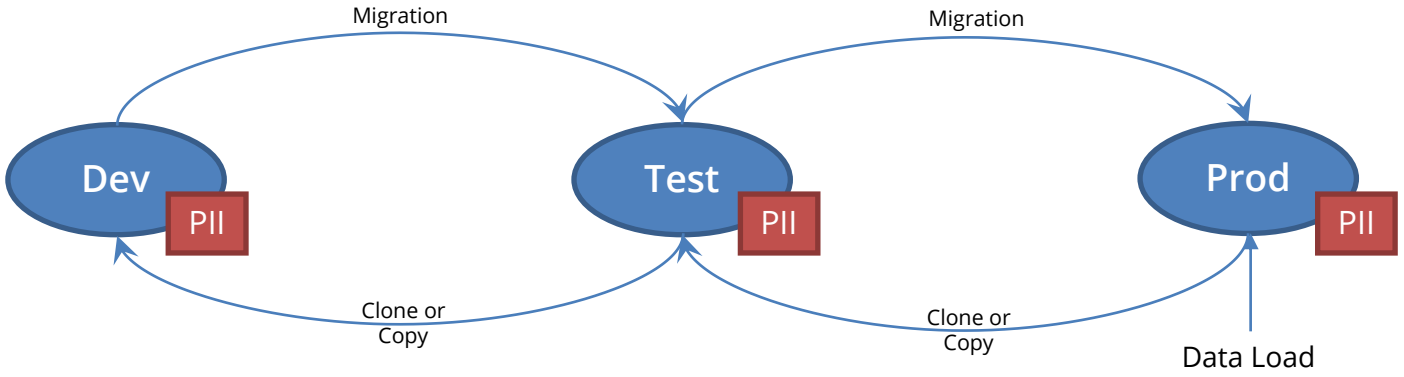
Single Database	▪ Typical database assessment is focused on single database ▪ **In-depth review** of database installation, configuration, operation, privileges, and sensitive data protection ▪ Difficult to extrapolate findings to all databases
Database Sample	▪ Sample **critical databases** (e.g., top 10) – across platform, versions, compliance, sensitive data, **DBA "siloes"** ▪ Review enterprise-wide database security controls, processes, and operational procedures ▪ Use to understand and evaluate **database security posture** and extrapolate to all databases
All Databases	▪ How to perform assessments across 100 or 1,000 databases? ▪ Emphasis on **enterprise-wide** database security controls, processes, and operational procedures ▪ Sample critical databases – across platform, versions, compliance, sensitive data, DBA "siloes" ▪ **Scan all databases** for baseline developed from assessment – should be a project to establish enterprise database scanning

Assessment Scope – Test and Development

Custom Application



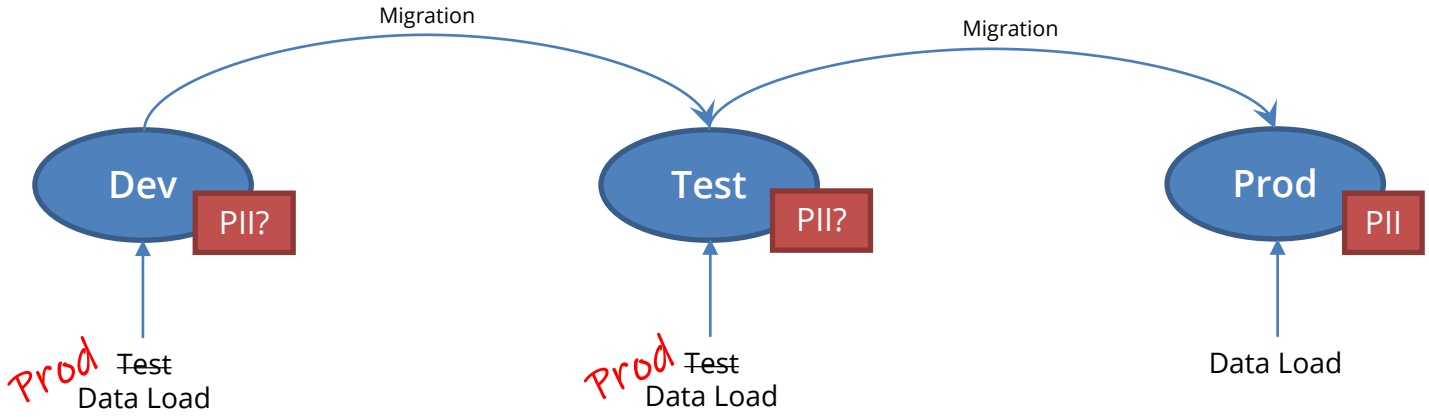
Package Application (e.g., ERP)



PII = Personally Identifiable Information

Assessment Scope – Test and Development

Custom Application

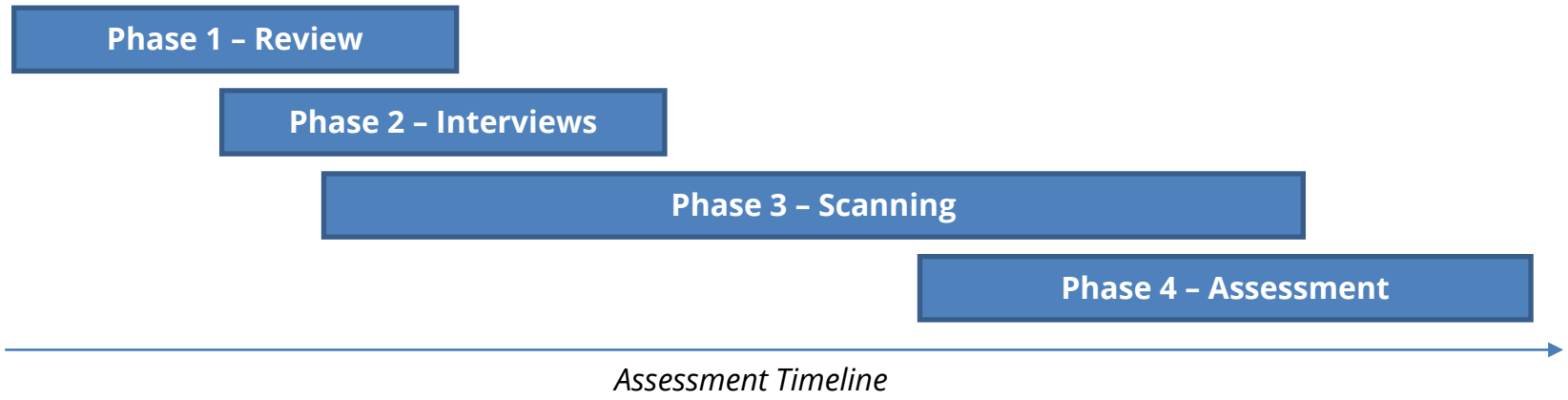


Package Application (e.g., ERP)

PII = Personally Identifiable Information

Assessment Approach – Phases

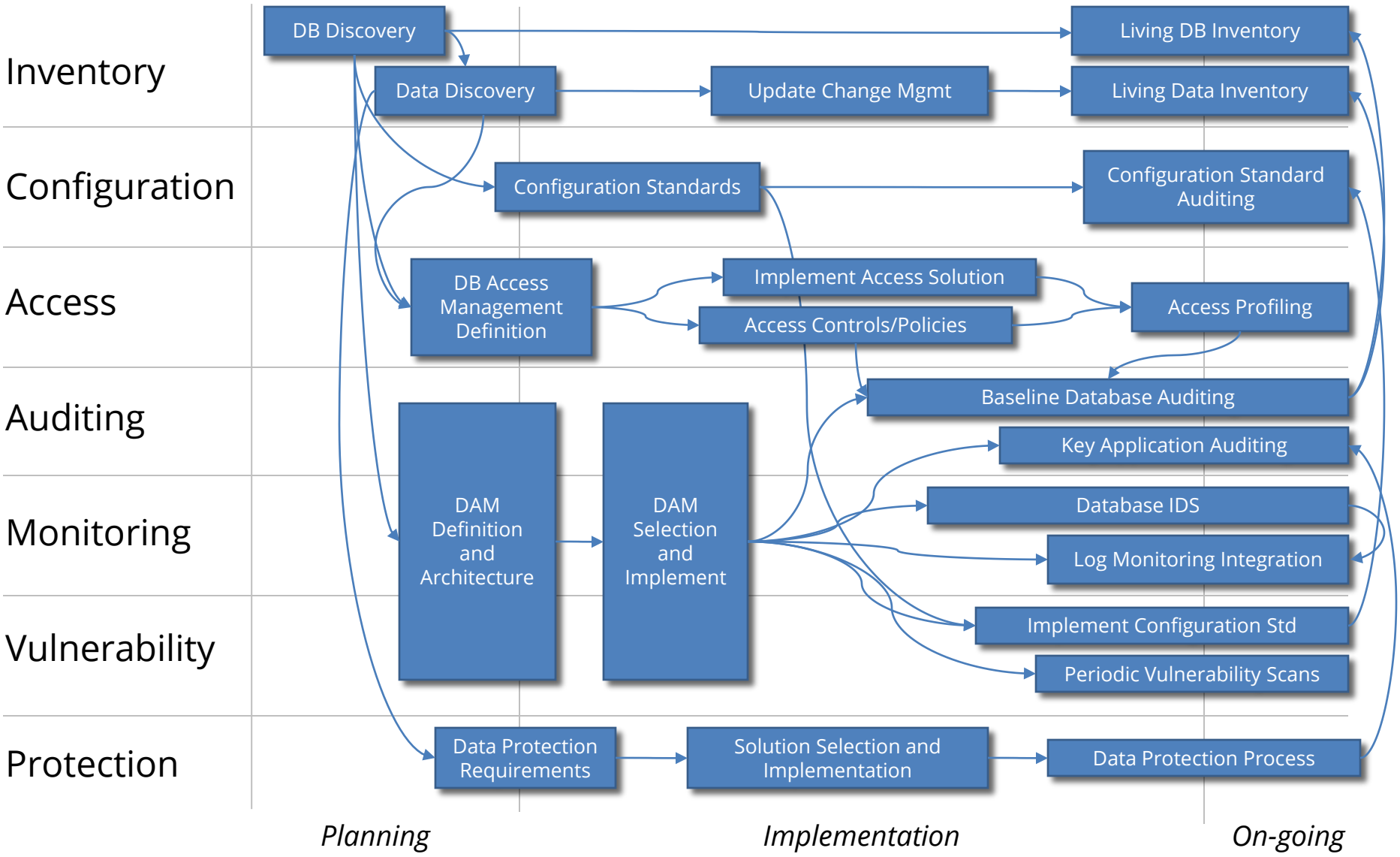
Phase 1	Database Security Policies, Standards, and Procedures Review
Phase 2	Database Security Stakeholder Interviews
Phase 3	Database Security Scans
Phase 4	Risk Assessment



Phase 1 –Policies, Standards, and Procedures Review

Policies	▪ IT Security standards (password, access, auditing, logging, …) ▪ IT General Controls (ITGC) ▪ Compliance (SOX, GDPR, HIPAA, CCPA, …) requirements ▪ Data protection and encryption
Standards	▪ Database and data inventory ▪ Database configuration and installation standards ▪ Database access management ▪ Database auditing and logging ▪ Database security monitoring ▪ Database vulnerability management ▪ Database development
Procedures	▪ Database installation ▪ Database backup ▪ Database cloning ▪ Database monitoring ▪ Database change control ▪ Access management (account creation/termination, privilege assignment, …) ▪ Sensitive data scrambling

Phase 1 – Database Security Program



Interviews with key stakeholders in database security

Data Management	▪ Review organizational structure to determine if there are silos of DBAs or infrastructure and application DBAs ▪ Database administration manager ▪ Senior/lead database administrator
IT Security	▪ IT Security lead with oversight for databases ▪ IT Security vulnerability management and logging ▪ CSO/CISO for enterprise security vision and direction
Compliance and Audit	▪ IT internal auditor ▪ Compliance around sensitive data and regulations
Application Owners	▪ IT application owner to understand application data, sensitivity, and risk

Phase 2 – Database Security Stakeholder Interviews (Enterprise)

Inventory	▪ Inventory of all databases and sensitive data locations ▪ Methods and processes to maintain the inventories
Configuration	▪ Database security standards and baseline ▪ Periodic validation with compliance to the standard
Access	▪ Database access management policies, procedures, and tools ▪ Database access profiling and monitoring
Auditing	▪ Database auditing requirements, processes, and definitions ▪ Centralized auditing retention and reporting solution
Monitoring	▪ Database real-time security monitoring and intrusion detection ▪ Database monitoring definition and tools
Vulnerability	▪ Vulnerability assessment and management for databases ▪ Vulnerability remediation strategy and processes
Protection	▪ Sensitive data protection strategy – encryption, data masking, redaction, scrambling ▪ Data protection policies, procedures, and tools

Phase 3 – Database Security Scanning

- **Single database**
  - Straight-forward scan of the database
  - Data retrieval of database accounts, privileges, etc. for review
  - Sensitive data scan to identify locations of data elements
  - Access database audit trail for analysis of access patterns
- **Sampling of Databases**
  - Obtain database inventory if one exists to identify databases
  - Segment databases based one or more of the following attributes and this information may have to be compiled –
    - Platform
    - Version
    - Compliance regulations (SOX, GDPR, PCI, …)
    - Sensitive data elements
    - If multiple DBA teams or organizational units, ensure a sample from each is included
    - Custom vs package applications
  - Sample the largest databases based on size when possible
  - Avoid randomly sampling databases

Phase 3 – Database Security Scanning

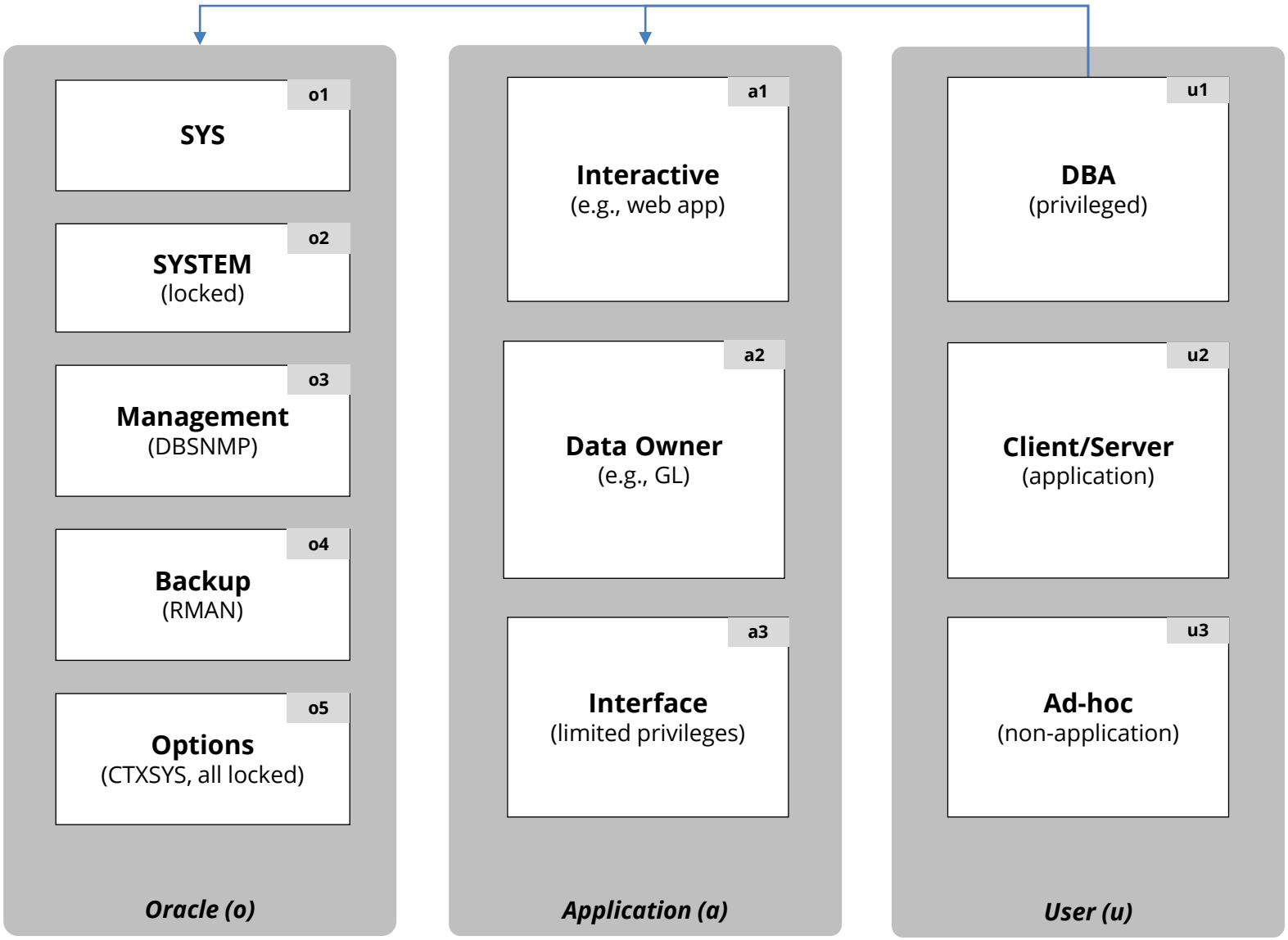
Database Security Scanning	▪ A software tool should be used to perform database security scans ▪ Security scan should be customized to the organization's security standards ▪ For single database assessments, Oracle DBSAT works is ▪ For assessments, Integrigy uses our product AppSentry
Data Retrieval	▪ SQL scripts or a query tool is required to dump data regarding users, privileges, etc. ▪ A query only database account with SELECT ANY DICTIONARY is required to gather information on database accounts, privileges, etc. ▪ SQL script may also be given to the DBA for execution, however, output may be manipulated by the DBA ▪ For assessments, Integrigy uses an internal tool Jintplus to dump database tables to an Excel workbooks for analysis and review

Phase 4 – Database Risk Assessment

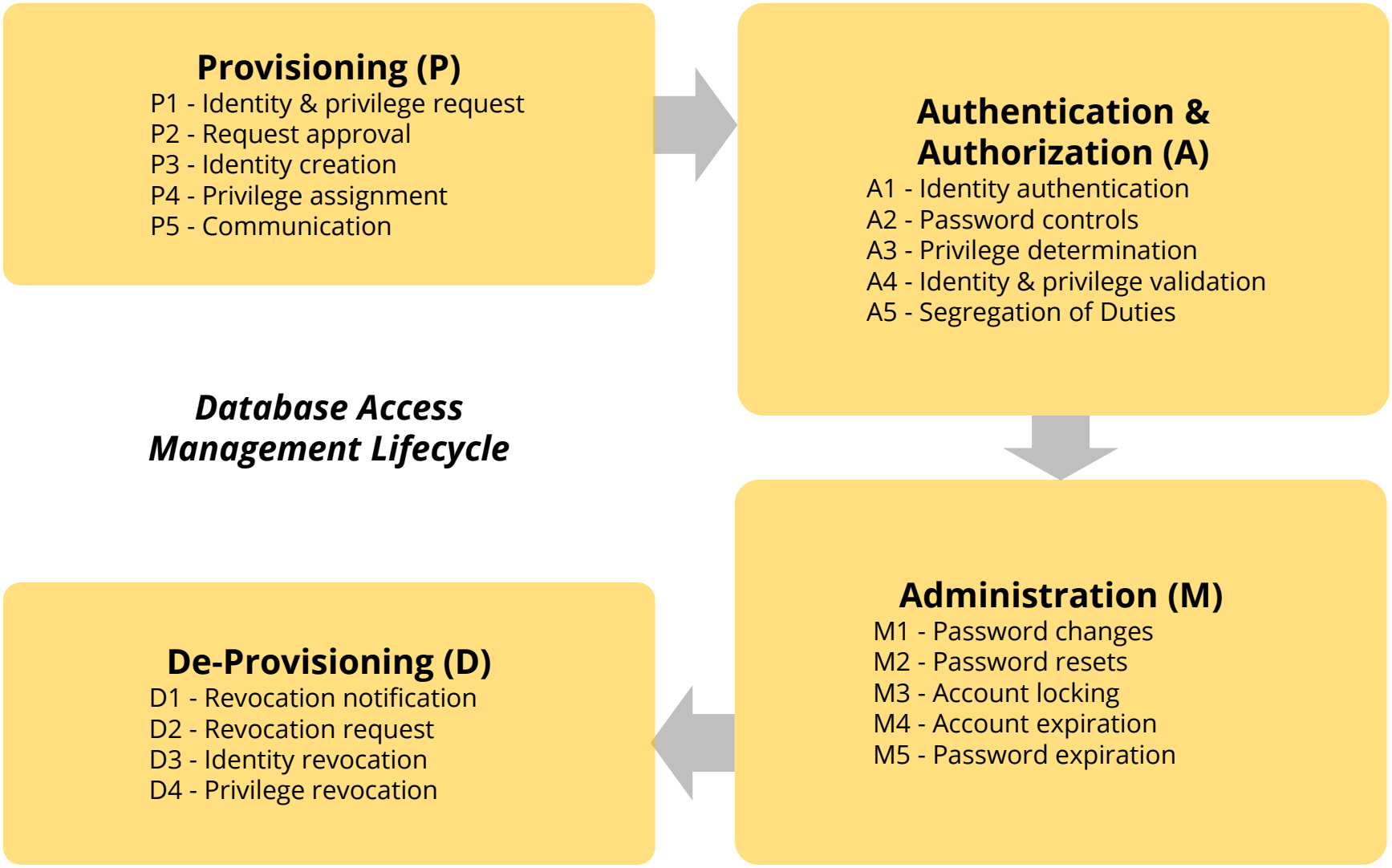
- **Based on review and analysis of the policies, standards, interviews, and database scans, risk assessment is developed**
  - effectiveness of the current security controls that protect a database
  - likelihood of compromise or loss of the data stored in the database
  - recommendations to improve the security controls that protect the database

- **Database scans against database security standards and configuration**
- **Database access including access management**
- **Database privilege and sensitive data access**
- **Sensitive data protection**
- **Database auditing and monitoring**

Database Account Definition (Oracle)



Database Access Management



Database Access Management (Example)

Type of Account	Provisioning (P)	Authentication & Authorization (A)	Administration (M)	De-Provisioning (D)
o1 – SYS	P1: Installed by default per database security standards P4: Privileges pre-defined	A1: Local authentication A2: Profile ORA_DEFAULT A3: Privileges pre-defined A4: Review of all changes A5: No SOD review	M1: Password Vault M3: No; M4: No; M5: 360d	D1: Installed by default D2: Per database security standards D3: Locked or removed per database security standards D4: Privileges pre-defined
o2 - SYSTEM			M4: Locked	
o3 - Management			M1: Password Vault M3: 6; M4: Yes; M5: 360d	
o4 – Backup			M1: Password Vault M3: 6; M4: Yes; M5: 360d	
o5 – Options			M4: Locked	
a1 - Interactive	P1: Standard IT request workflow P2: DBA and IT Security review P3: DBA created P4: Privileges defined by app	A1: Local authentication A2: Profile APPLICATION A3: Privileges defined by app – roles when possible A4: Review of all changes – sample tickets A5: No SOD review	M1: Password Vault M3: No; M4: No; M5: 360d	D2: Standard IT request workflow D3: Locked, but never drop per standards D4: Standard IT request workflow
a2 – Data Owner			M4: Locked	
a3 – Interface			M1: Password Vault M3: No; M4: No; M5: 360d	
u1 – DBA	P1: Standard user request workflow P2: User manager approval/review P3: Security admin created P4: Privileges via local DB roles	A1: Active Directory authentication A2: AD password controls A3: Privileges via local DB roles A4: Quarterly manager review A5: Quarterly manager review	M1 – M5: AD controlled	D1: AD controlled D2: Standard user request workflow or per quarterly manager review process D3: Drop after 180 when locked D4: Request via quarterly manager review process
u2 – Client/Server				
u3 – Ad-hoc				

Database Access and Privilege Analysis (Example)

Type of Account	Access	Privileges	Auditing
o1 – SYS	▪ How is account controlled	▪ Fixed – highly privileged	▪ Requires SYS operations auditing
o2 - SYSTEM	▪ Can be disabled	▪ Fixed – highly privileged	▪ Audit privileged actions
o3 - Management	▪ How is account controlled	▪ Review privileges	▪ Access auditing
o4 – Backup	▪ How is account controlled	▪ Fixed – highly privileged	▪ Access auditing
o5 – Options	▪ Must be disabled	▪ Fixed	▪ Access auditing
a1 - Interactive	▪ How is account controlled	▪ Review privileges	▪ Access auditing
a2 – Data Owner	▪ How is account controlled	▪ Review – limited privileges only – no DBA privileges	▪ Access auditing
a3 – Interface	▪ How is account controlled	▪ Review – limited privileges only	▪ Access auditing
u1 – DBA	▪ Access management review	▪ Review privileges	▪ Determine auditing required
u2 – Client/Server	▪ Access management review	▪ Review privileges	▪ Determine auditing required
u3 – Ad-hoc	▪ Access management review	▪ Review privileges	▪ Determine auditing required

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**