INTEGRIGY

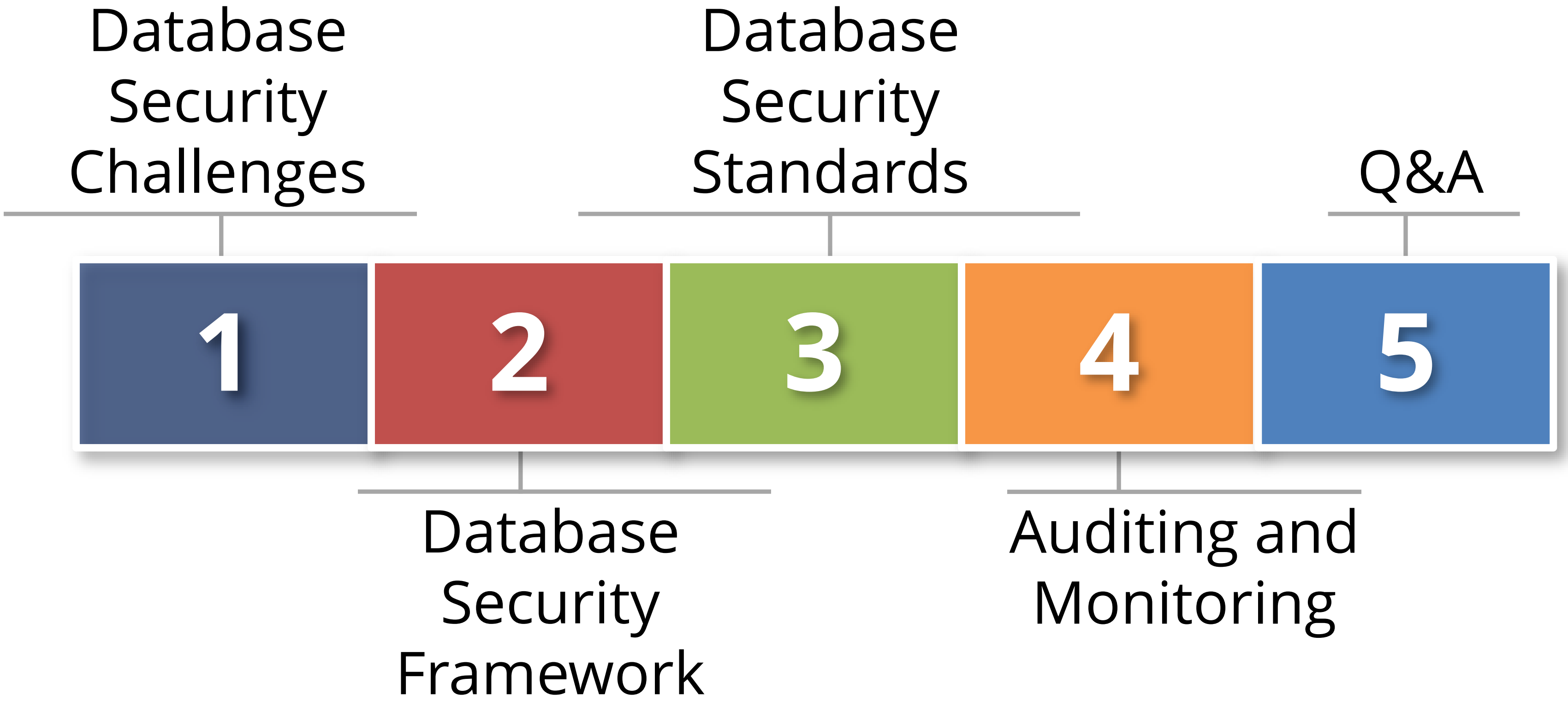
Securing **1,000** Oracle Databases – Challenges and Solutions

July 26, 2012

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



1 Database Security Challenges

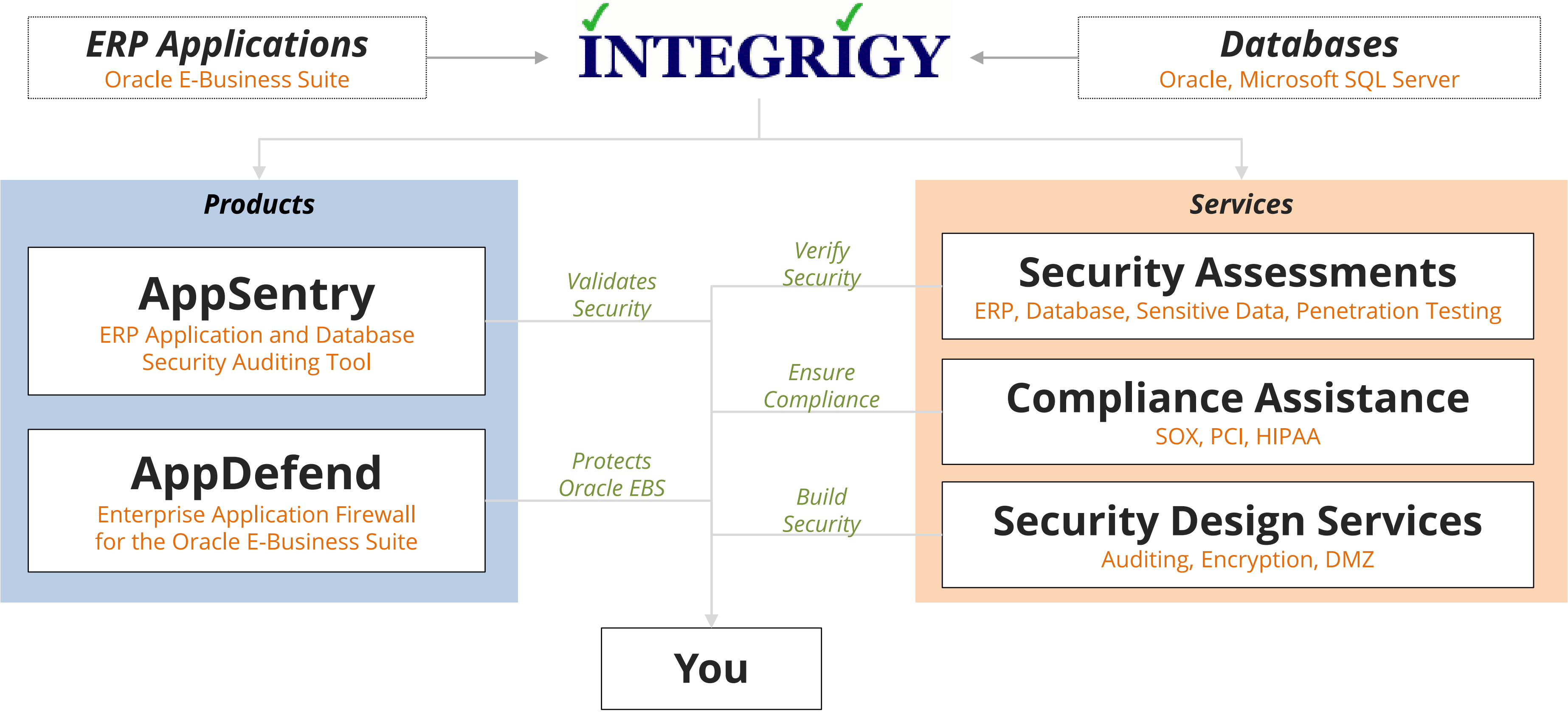
2 Database Security Framework

3 Database Security Standards

4 Auditing and Monitoring

5 Q&A

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle, Microsoft SQL Server

Products

AppSentry
ERP Application and Database Security Auditing Tool

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Verify Security

Ensure Compliance

Build Security

Services

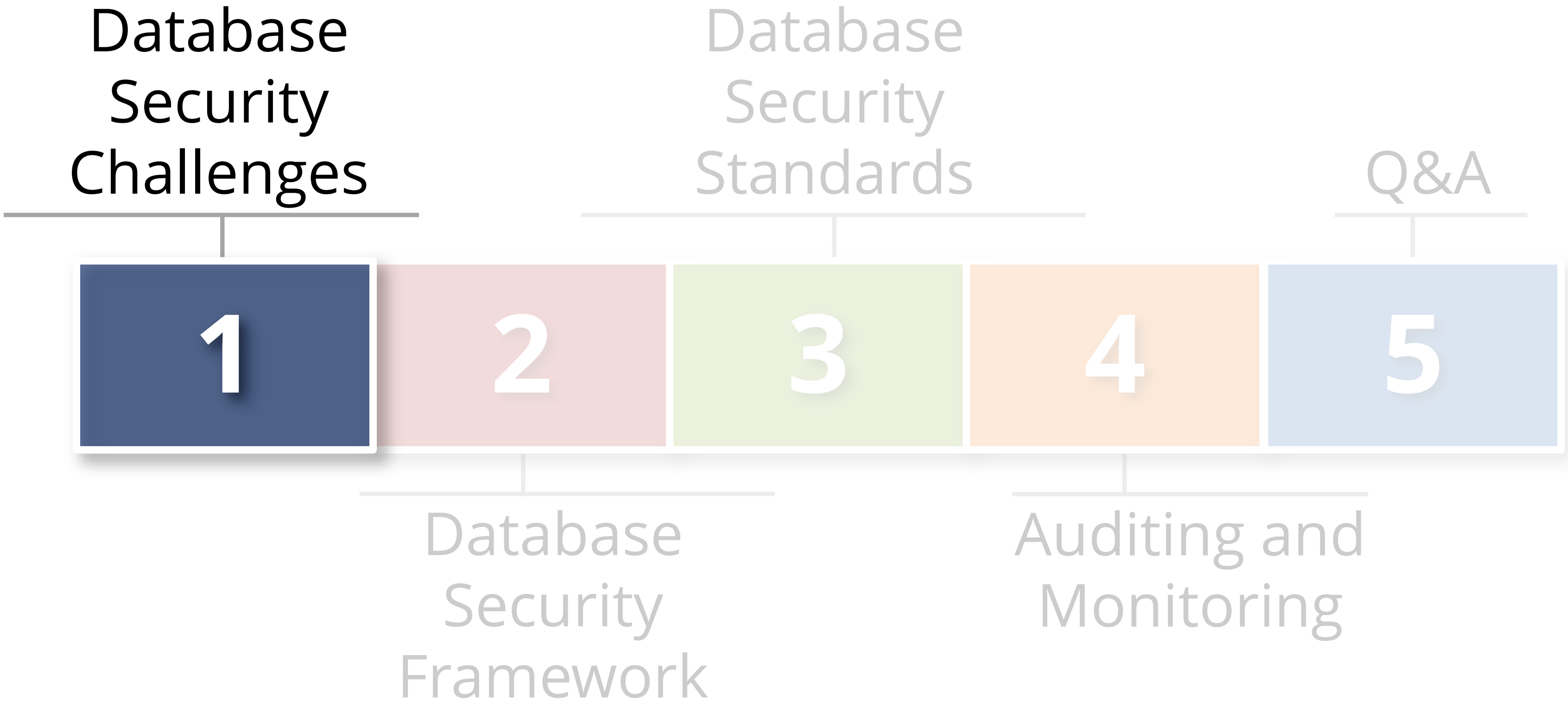
Security Assessments
ERP, Database, Sensitive Data, Penetration Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

You

Agenda



1 Database Security Challenges

2 Database Security Framework

3 Database Security Standards

4 Auditing and Monitoring

5 Q&A

Database Security Issues

Databases are security feature rich, but are **security “reality” poor**.

2005-2010	Oracle: 400+ security vulnerabilities fixed
2007	Sybase: Complex password capabilities added
2007	Oracle: Case sensitive passwords added
2008	Microsoft SQL Server: SQL audit statement added

Database Security Issues

Database security is dependent on and coupled with the **application**.

- Application architecture and design complicate many aspects of database security
- Application and business requirements dictate database upgrades and security patching

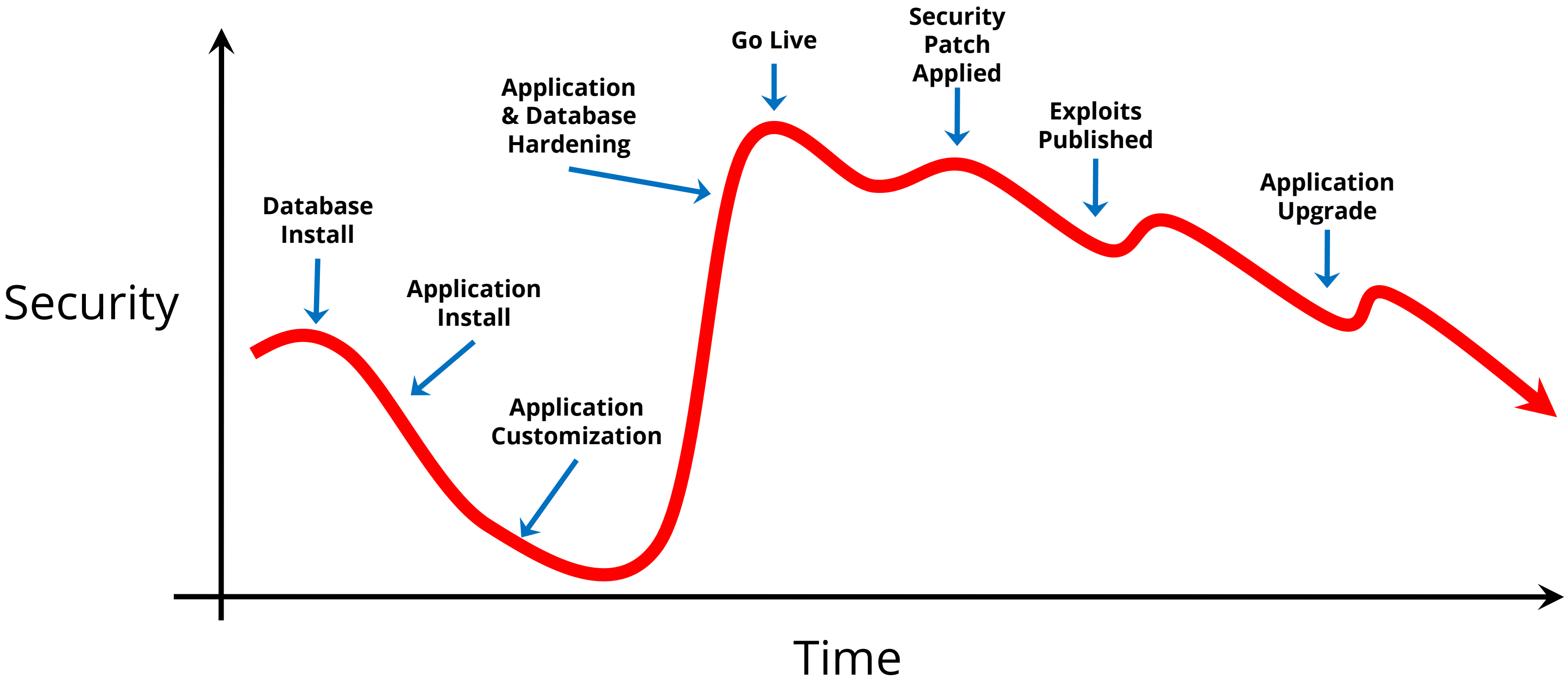
Database Security Issues

Database security patches are a fact of life and must be addressed by the business.

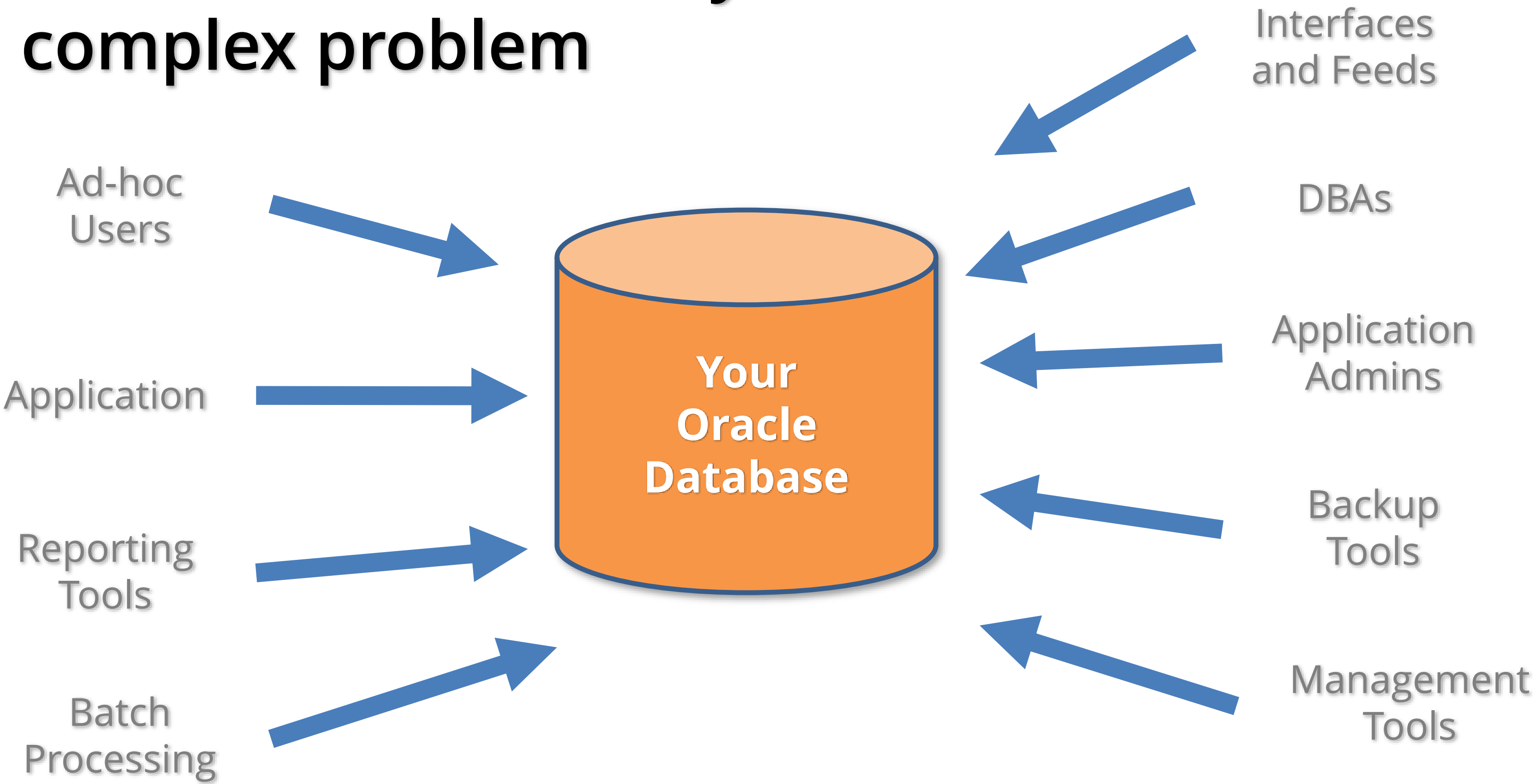
- **Code quality issue**, not a feature issue
- Security patches often require database upgrades or other changes

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



Traditional Database Security Approaches

Database security checklists are used to secure databases one at a time.

- Excellent baseline and starting point
- Often in conflict with application configuration
- Too many exceptions required to handle application limitations
- Security decay requires constant or periodic assessments

Traditional Database Security Approaches

Database security assessments are performed periodically to fix database security.

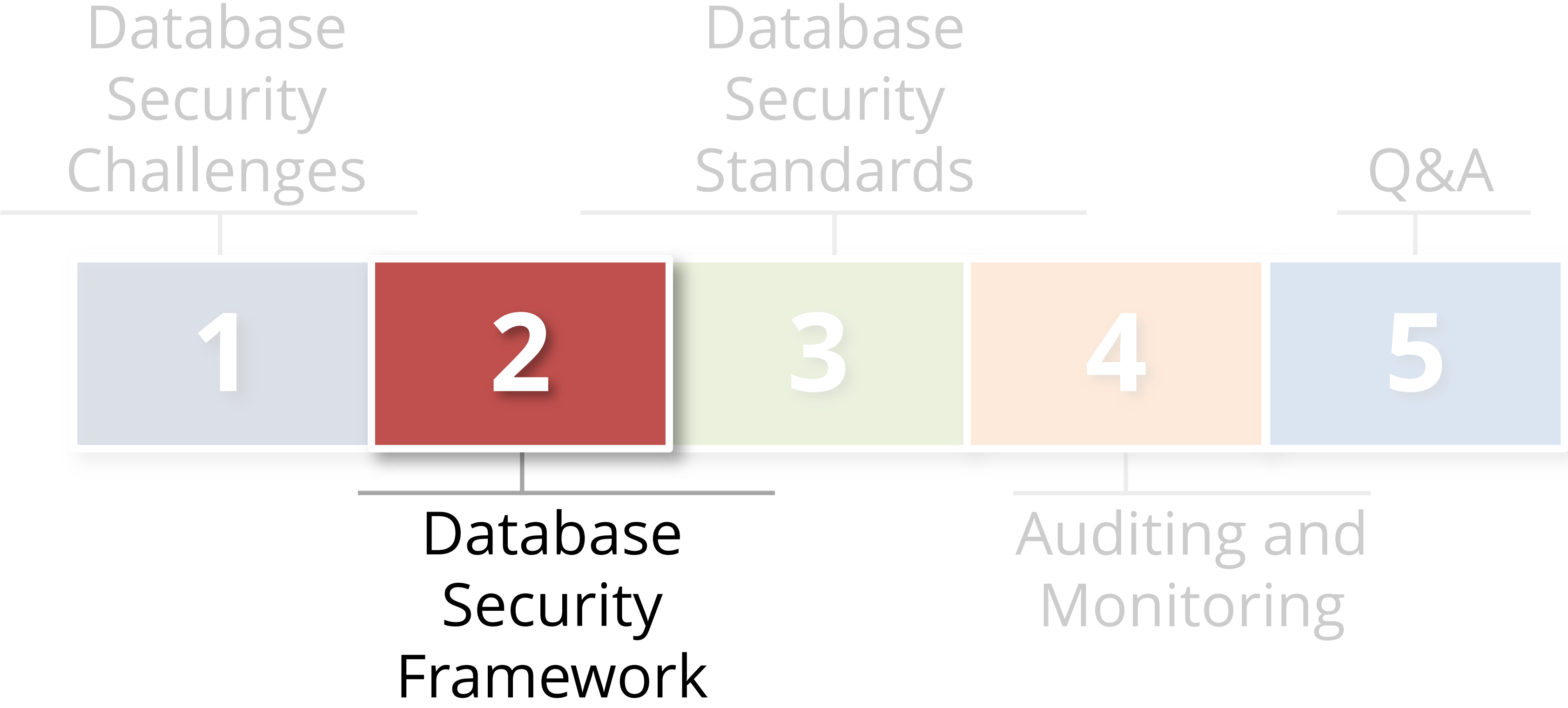
- Expensive and time consuming
- Must be performed periodically to be effective
- Database-centric or arbitrary standards often used

Traditional Database Security Approaches

The database security tool is purchased to solve the database security problem.

- Database monitoring and auditing tools are only part of the solution
- Expensive and time consuming to implement
- Complex applications cause deployment problems

Agenda



1. Database Security Challenges
2. Database Security Framework
3. Database Security Standards
4. Auditing and Monitoring
5. Q&A

Defensive Security Strategies Themes

#1 Reduce security vulnerability exposure

- Almost all database security vulnerabilities require a valid database session
- Jump off or slow down the security patch hamster wheel
- “Virtual Perimeters” to reduce access to databases

Defensive Security Strategies Themes

#2 Classify databases and act appropriately

- The data determines the acceptable level of risk per database

Defensive Security Strategies Themes

#3 Intelligent and business-focused auditing and monitoring

- Capturing audit data is the easy part
- Storing, protecting, and reporting is the hard part
- Must transform audit data into actionable information

Defensive Security Strategies Themes

#4 Database security must be tightly coupled with application security

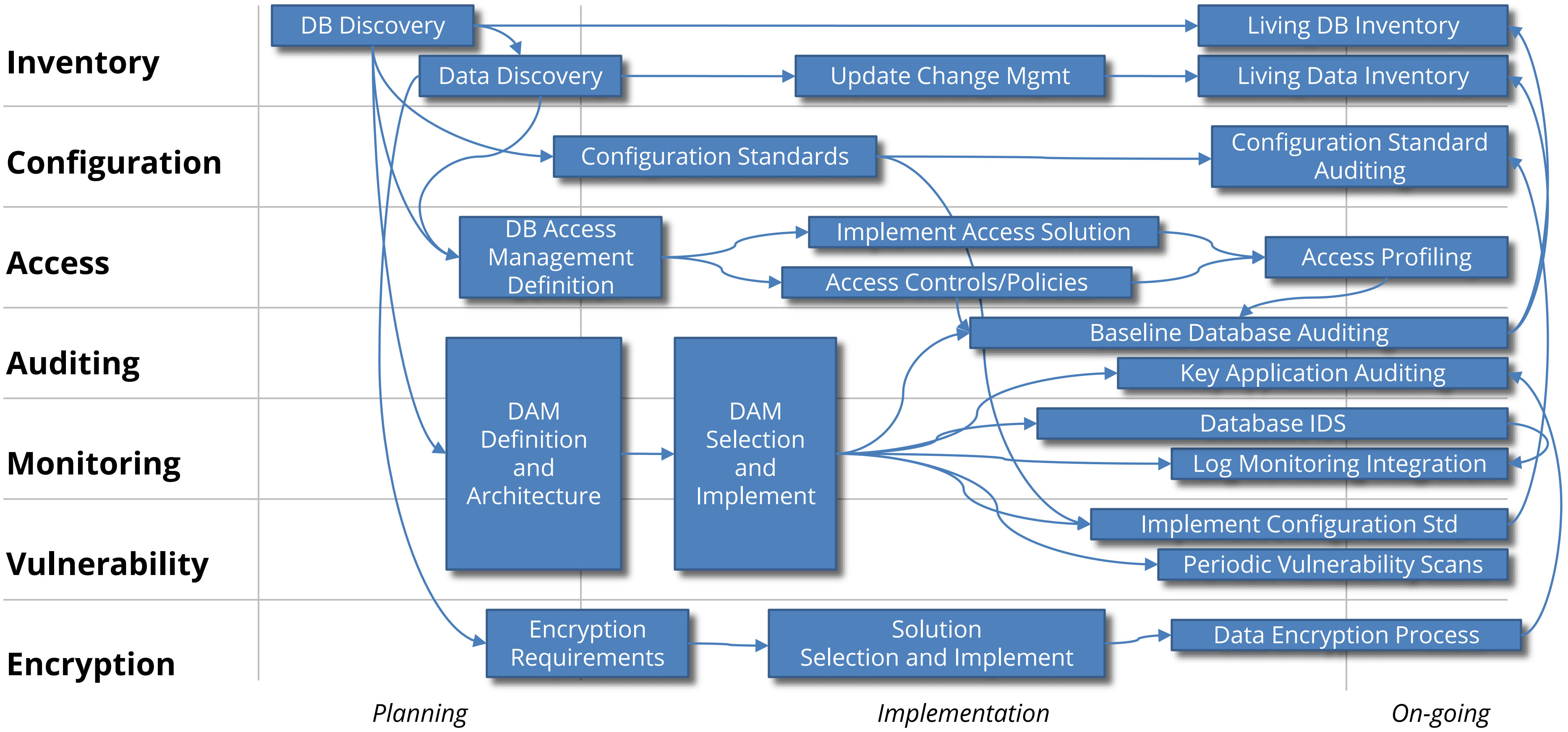
- Incorporate application requirements and variation into all aspects of database security
- Don’t handle applications security as an exception but as part of the database security framework
- Service/application accounts, stupid application design, and other application limitations are a fact of life

Framework = Consistency

Database Security Program Components

	Inventory	Configuration	Access	Auditing	Monitoring	Vulnerability	Encryption
	▪ Review existing database inventories ▪ Define scope of database discovery ▪ Perform hybrid database discovery	▪ Review existing database configuration standards ▪ Define database security and compliance requirements ▪ Develop measureable database security standards	▪ Define database access management definition ▪ Select and implement access solutions or policies for privileged and end-user accounts	▪ Development auditing requirements for DAM ▪ Define baseline auditing for all databases ▪ Define auditing for key applications and databases based on compliance and data	▪ Development monitoring requirements for DAM ▪ Define and implement database IDS ▪ Define and implement log monitoring integration	▪ Development vulnerability assessment requirements for DAM ▪ Implement monitoring and compliance of configuration standard ▪ Implement periodic scanning	▪ Define encryption requirements ▪ Select and implement encryption solution for initial databases ▪ Develop on-going encryption implementation
Outputs	▪ Database inventory ▪ Data inventory for key databases	▪ Database security and compliance requirements ▪ Database security standards	▪ Database access management ▪ Policies for database account management	▪ Database auditing definition for (1) all databases and (2) key databases	▪ Database monitoring and alerting definition ▪ Log monitoring integration	▪ Rules for measuring compliance with database security standards	▪ Encryption requirements with policies ▪ Encryption implementation process

Program Implementation



Inventory

Configuration

Access

Auditing

Monitoring

Vulnerability

Encryption

DB Discovery

Data Discovery

Update Change Mgmt

Living DB Inventory

Living Data Inventory

Configuration Standards

Configuration Standard Auditing

DB Access Management Definition

Implement Access Solution

Access Controls/Policies

Access Profiling

Baseline Database Auditing

Key Application Auditing

DAM Definition and Architecture

DAM Selection and Implement

Database IDS

Log Monitoring Integration

Implement Configuration Std

Periodic Vulnerability Scans

Encryption Requirements

Solution Selection and Implement

Data Encryption Process

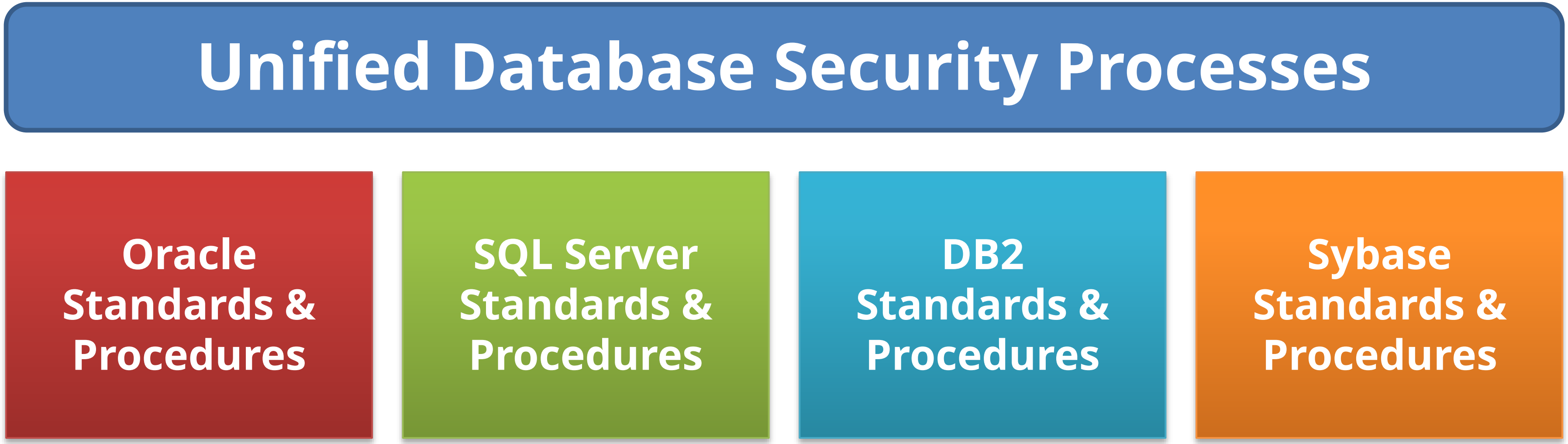
Planning

Implementation

On-going

Database Security Program Silos

Processes should be unified, but standards and procedures should be vendor specific.



Unified Database Security Processes

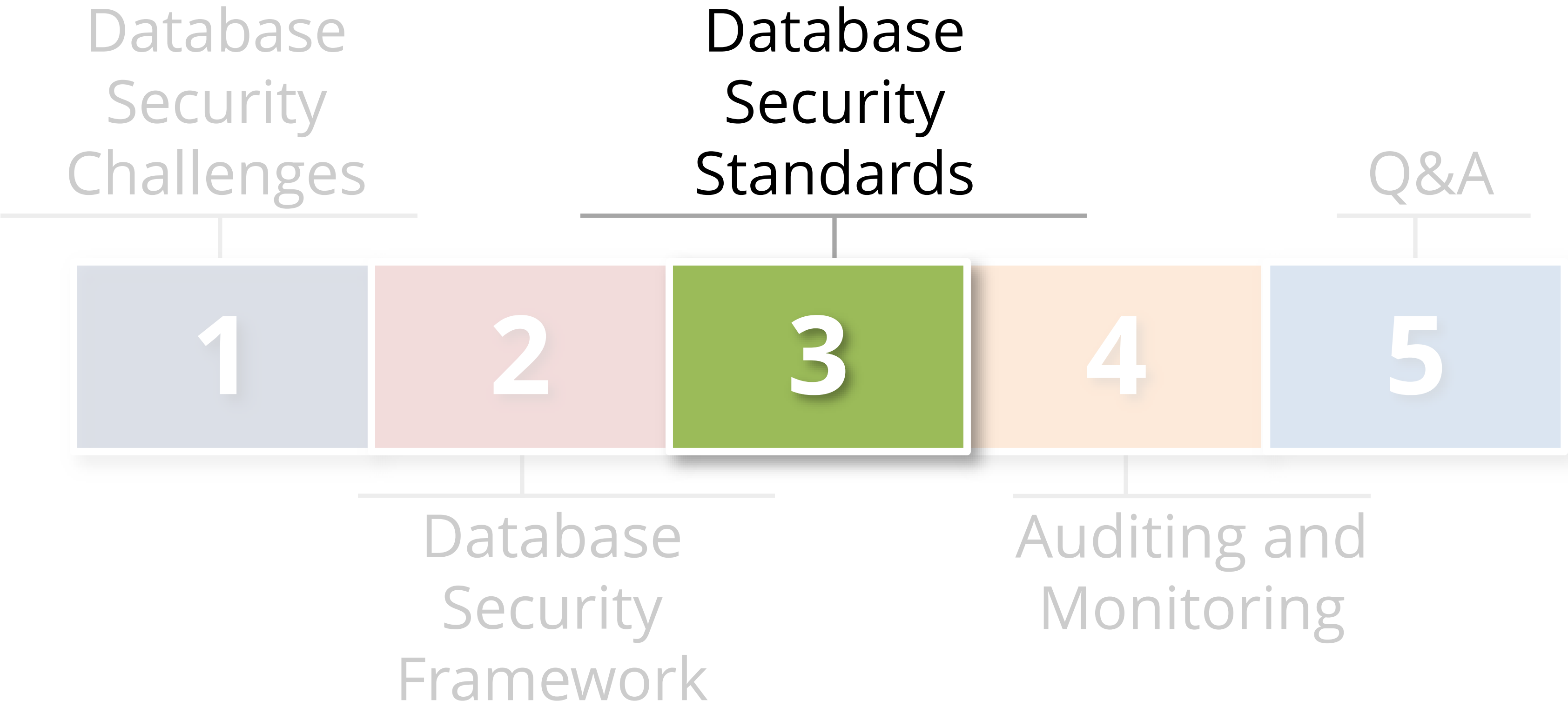
Oracle Standards & Procedures

SQL Server Standards & Procedures

DB2 Standards & Procedures

Sybase Standards & Procedures

Agenda



1 Database Security Challenges

2 Database Security Framework

3 Database Security Standards

4 Auditing and Monitoring

5 Q&A

Edwards Deming’s System of Profound Knowledge

Appreciation of a system

Knowledge of variation

Theory of knowledge

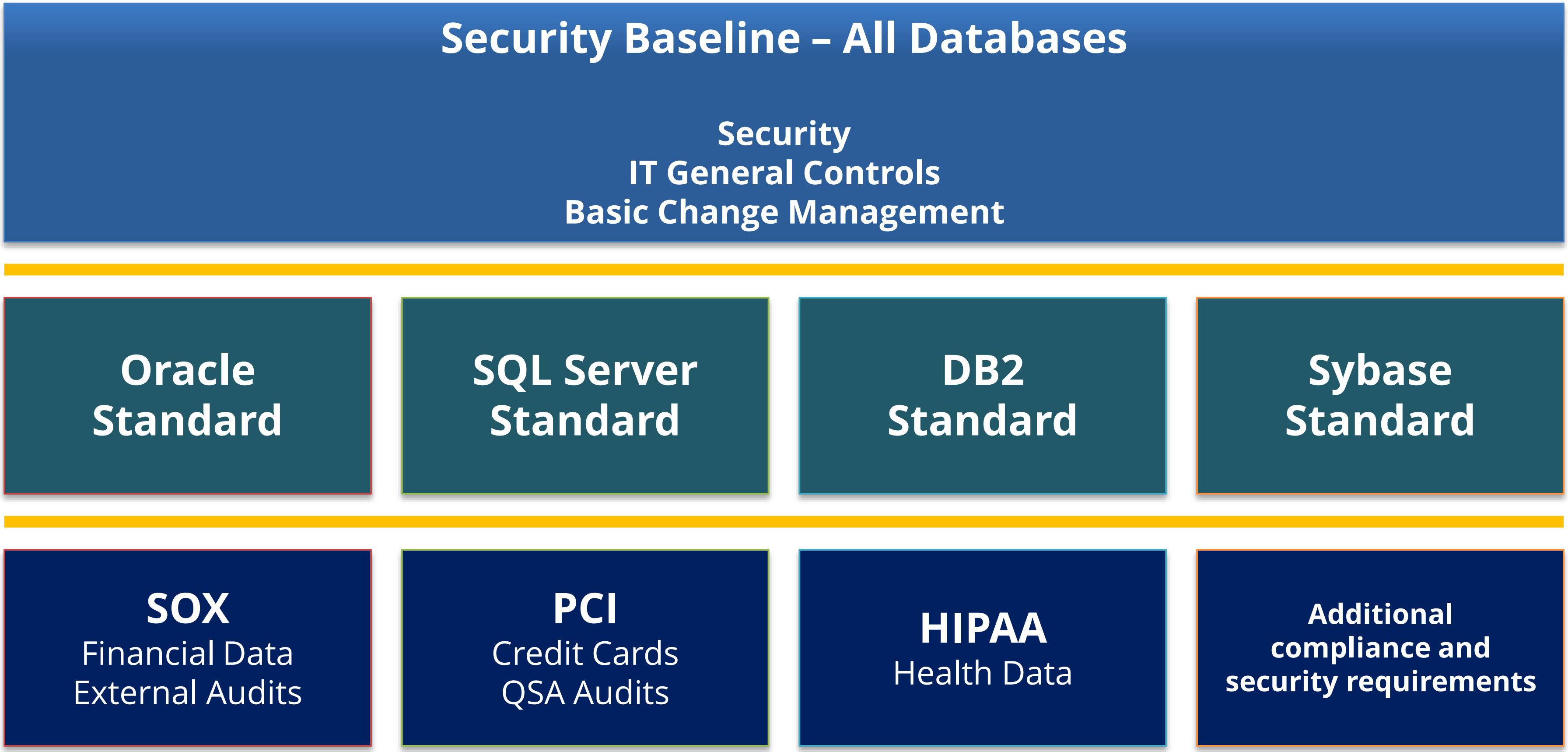
Knowledge of psychology

Database Security Standards

Security standards will be designed to be readily implementable and address application and organizational specific limitations.

- Address business, compliance, and security requirements, including SOX, PCI, and HIPAA.

DB Security Standards - Structure



Security Baseline – All Databases

Security
IT General Controls
Basic Change Management

Oracle Standard

SQL Server Standard

DB2 Standard

Sybase Standard

SOX
Financial Data
External Audits

PCI
Credit Cards
QSA Audits

HIPAA
Health Data

Additional compliance and security requirements

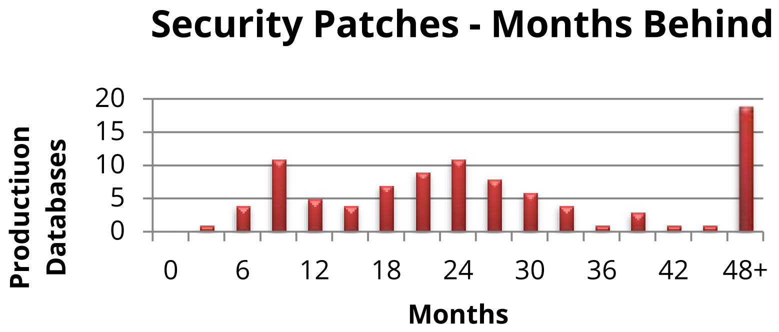
DB Security Standards - Content

What	What needs to be secured in the database?
Why	Why is this a security issue? What's the impact?
How	What are the exact steps required to secure this? Step by step
Verification	How is this setting verified precisely? A single SQL statement
Mitigation	Besides an exception, what else can be done? Auditing?

Fact-based Security Standards

- **Based on facts**
- Use statistics during scans and database discovery
- Continuous monitoring

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

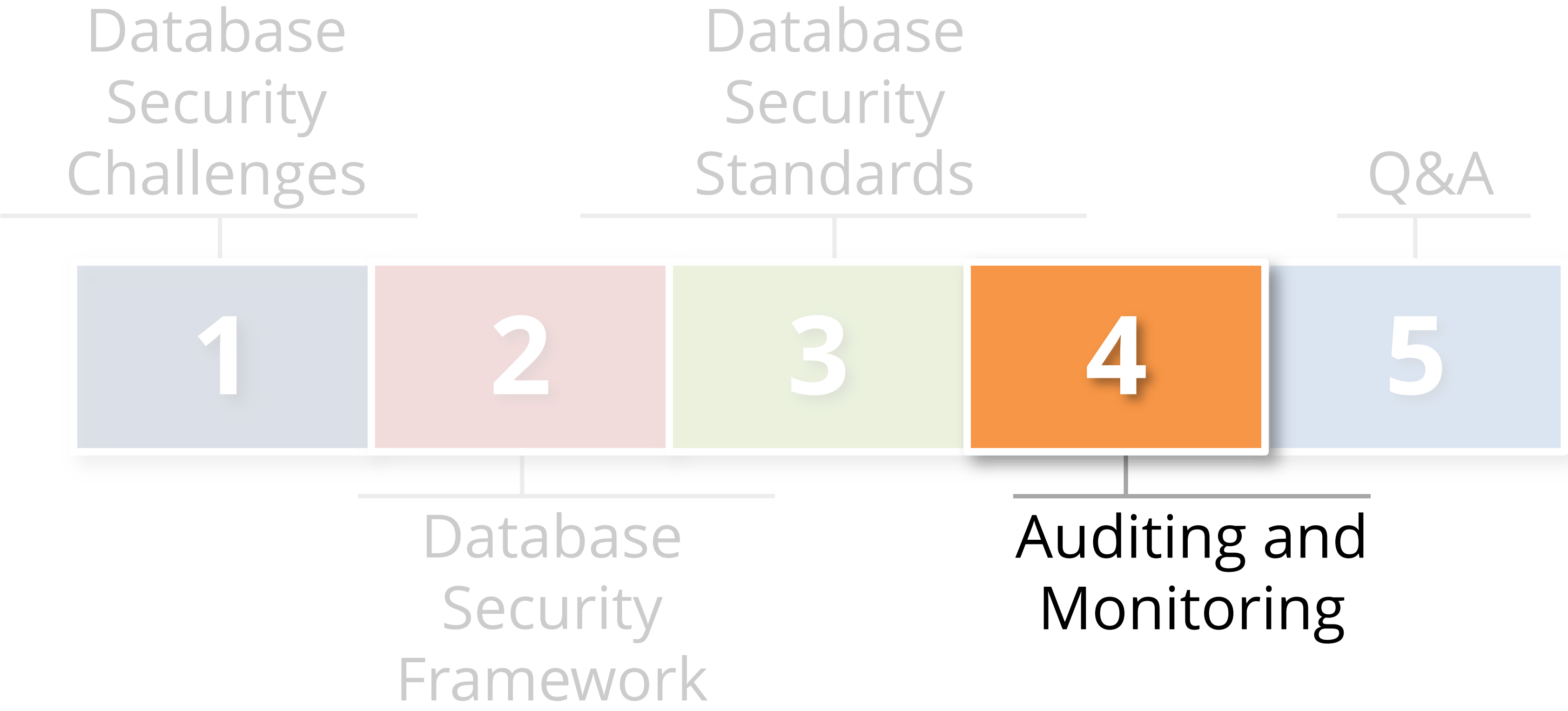

Security Patches - Months Behind

High percentage of exceptions or variances

= FAILURE

Database security standards must anticipate common exceptions

Agenda



1

Database Security Challenges

2

Database Security Framework

3

Database Security Standards

4

Auditing and Monitoring

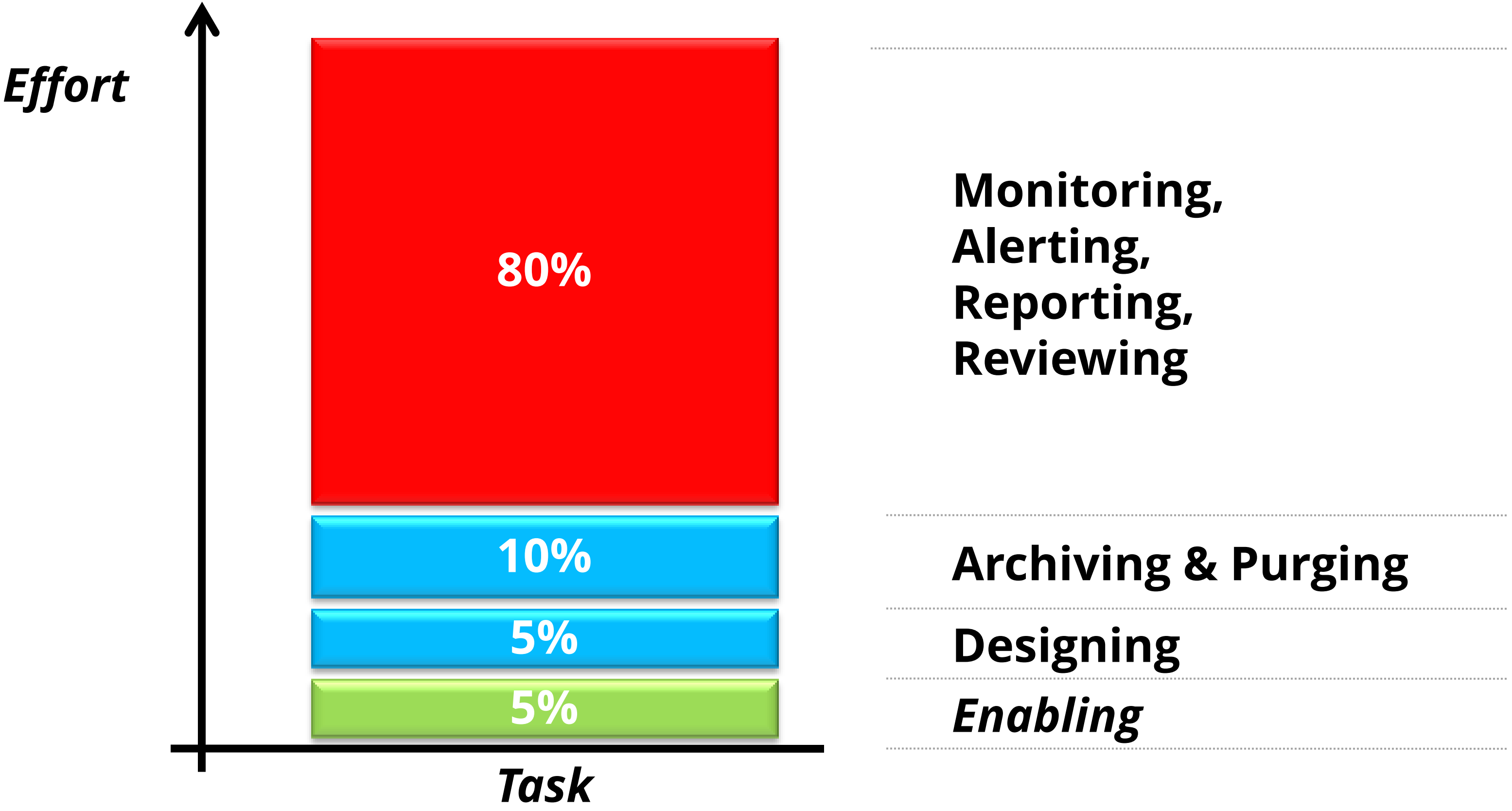
5

Q&A

Database Auditing – Current State

Database auditing in most organizations done done simply for a **compliance checkbox**.

- Auditing poorly defined
- No review of audit data
- Zero value to the organization



Monitoring,
Alerting,
Reporting,
Reviewing

Archiving & Purging

Designing

Enabling

Database Auditing and Monitoring

Intelligent and business-focused auditing and monitoring

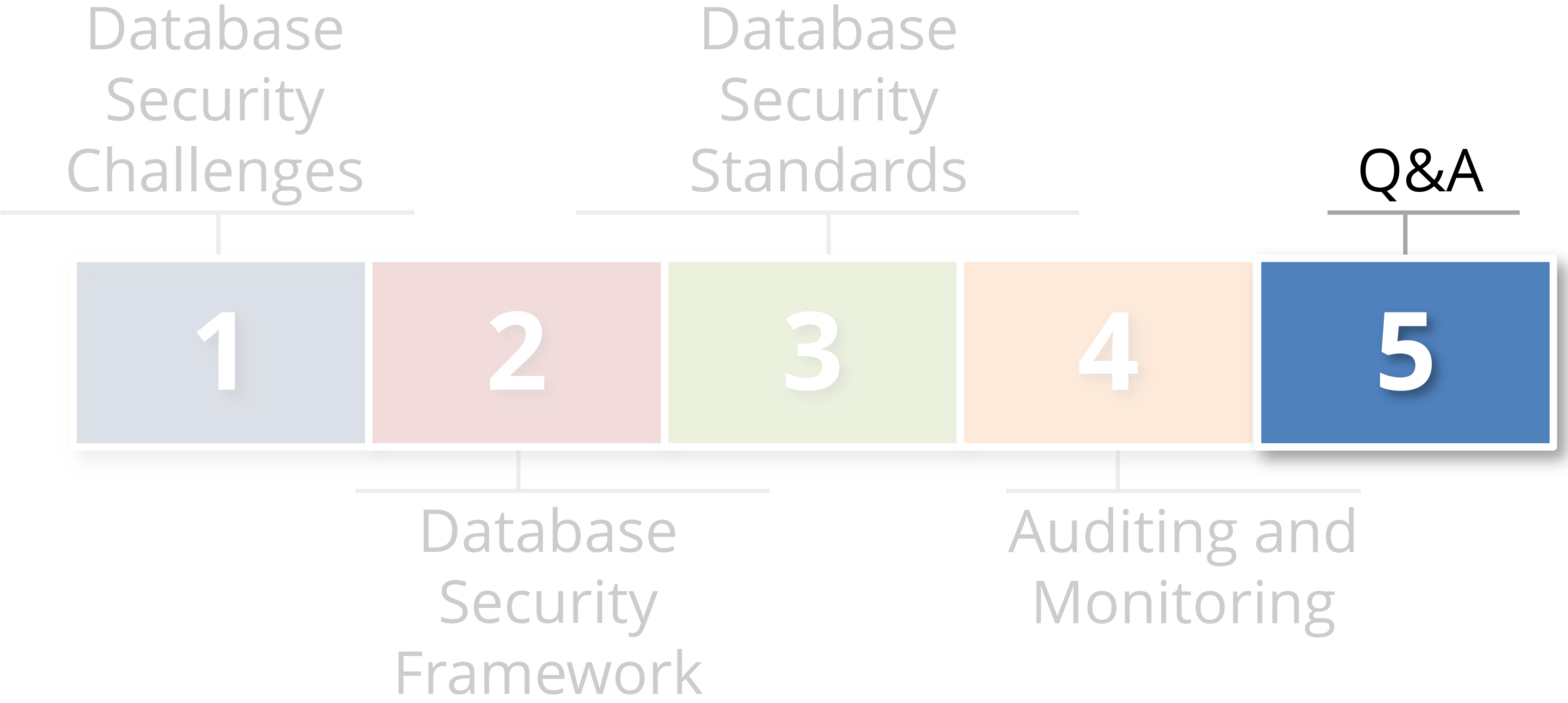
- Transform audit data into actionable information
- Use auditing as mitigating control when necessary
- Auditing is in harmony with database security program to proactively identify non-compliance

Database Auditing and Monitoring Strategy

A strategy for auditing and monitoring should be based on 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.
- Auditing should be multi-level – OS, DB, Application

Agenda



1 Database Security Challenges

2 Database Security Framework

3 Database Security Standards

4 Auditing and Monitoring

5 Q&A

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**