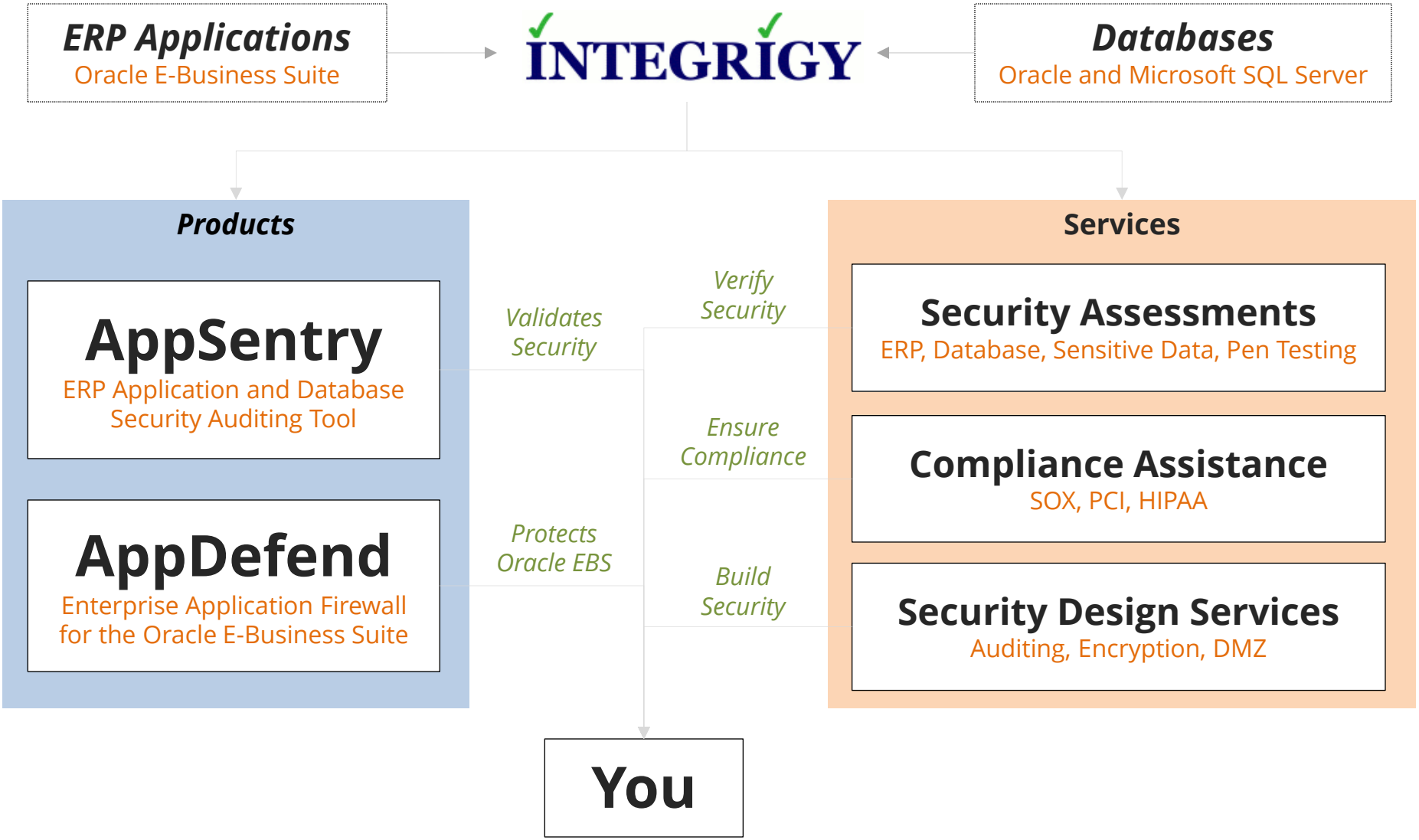
Protecting Sensitive Data in Oracle E-Business Suite

February 28, 2013

Stephen Kost
Chief Technology Officer
Integrigy Corporation

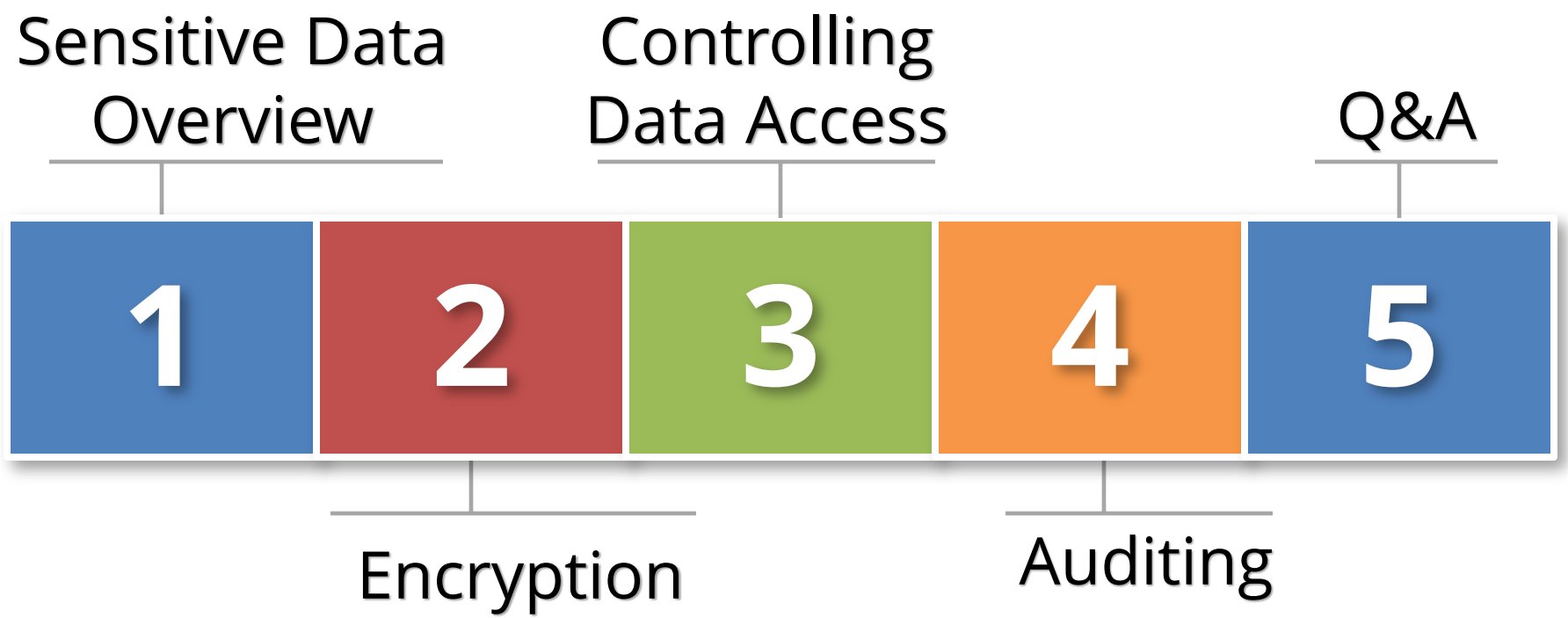
About Integrigy



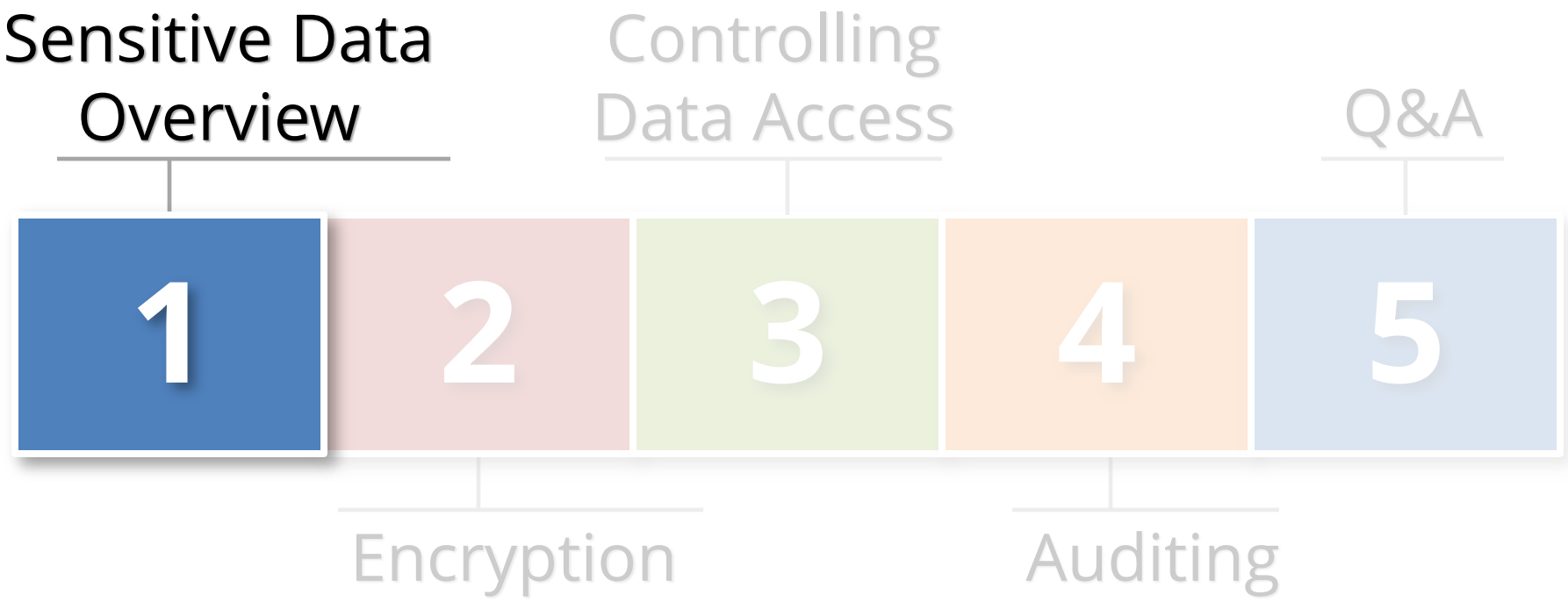
Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
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

Agenda


Sensitive Data Overview
Controlling Data Access
Q&A
1
2
3
4
5
Encryption
Auditing

Agenda


Sensitive Data Overview
Controlling Data Access
Q&A
1
2
3
4
5
Encryption
Auditing

Why - Security and Compliance Drivers

- **Payment Card Industry - Data Security Standard (PCI-DSS)**
  - 12 stringent security requirements
- **Privacy (National/State Regulations)**
  - Read access to sensitive data (National Identifier and Bank Account Number)
  - Regulations often specifically exclude encrypted data
  - California (SB1386) and Massachusetts data privacy laws
- **Sarbanes-Oxley (SOX)**
  - Database object, structure, and configuration changes
  - User and privilege creation, deletion, and modification
  - Reports for sampling of changes to change tickets

What is Sensitive Data in Oracle EBS?

Payment Card Industry Data Security Standard (PCI-DSS 2.0)	▪ Credit Card Number
	  ▪ *Primary Account Number (PAN)*
	▪ CVV/CV2/CID
	  ▪ *3 digits on the back for Visa/MC*
	  ▪ *4 digits on the front for AMEX*
	▪ Magnetic Stripe Data (very rare)

State Privacy Regulations (employees, customers, Vendors)	▪ First and last name
	▪ Plus one of the following:
	  ▪ Social security number
	  ▪ Credit card number
	  ▪ Bank account number
	  ▪ Financial account number
	  ▪ Driver license or state ID number

HIPAA Privacy Standard/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 is Sensitive Data in Oracle EBS?

Credit Card Data	`iby_security_segments (encrypted)`
	`ap_bank_accounts_all`
	`oe_order_headers_all`
	`aso_payments`
	`oks_k_headers_*`
	`oks_k_lines_*`
	`iby_trxn_summaries_all`
	`iby_credit_card`

Social Security Number
(National Identifier)
(Tax ID)
	`per_all_people_f`
	`hr_h2pi_employees`
	`ben_reporting`
	`ap_suppliers`
	`ap_suppliers_int`
	`po_vendors_obs`

Bank Account Number	`ap_checks_all`
	`ap_invoice_payments_all`
	`ap_selected_invoice_checks_all`

Protected Health Information (PHI)	Order Management Accounts Receivables Human Resources

Where else might be Sensitive Data?

Custom tables

- Customizations may be used to store or process sensitive data

"Maintenance tables"

- DBA copies tables to make backup prior to direct SQL update
- hr.per_all_people_f_011510

Interface tables

- Credit card numbers are often accepted in external applications and sent to Oracle EBS

Oracle EBS Flexfields

- It happens – very hard to find

Interface files

- Flat files used for interfaces or batch processing

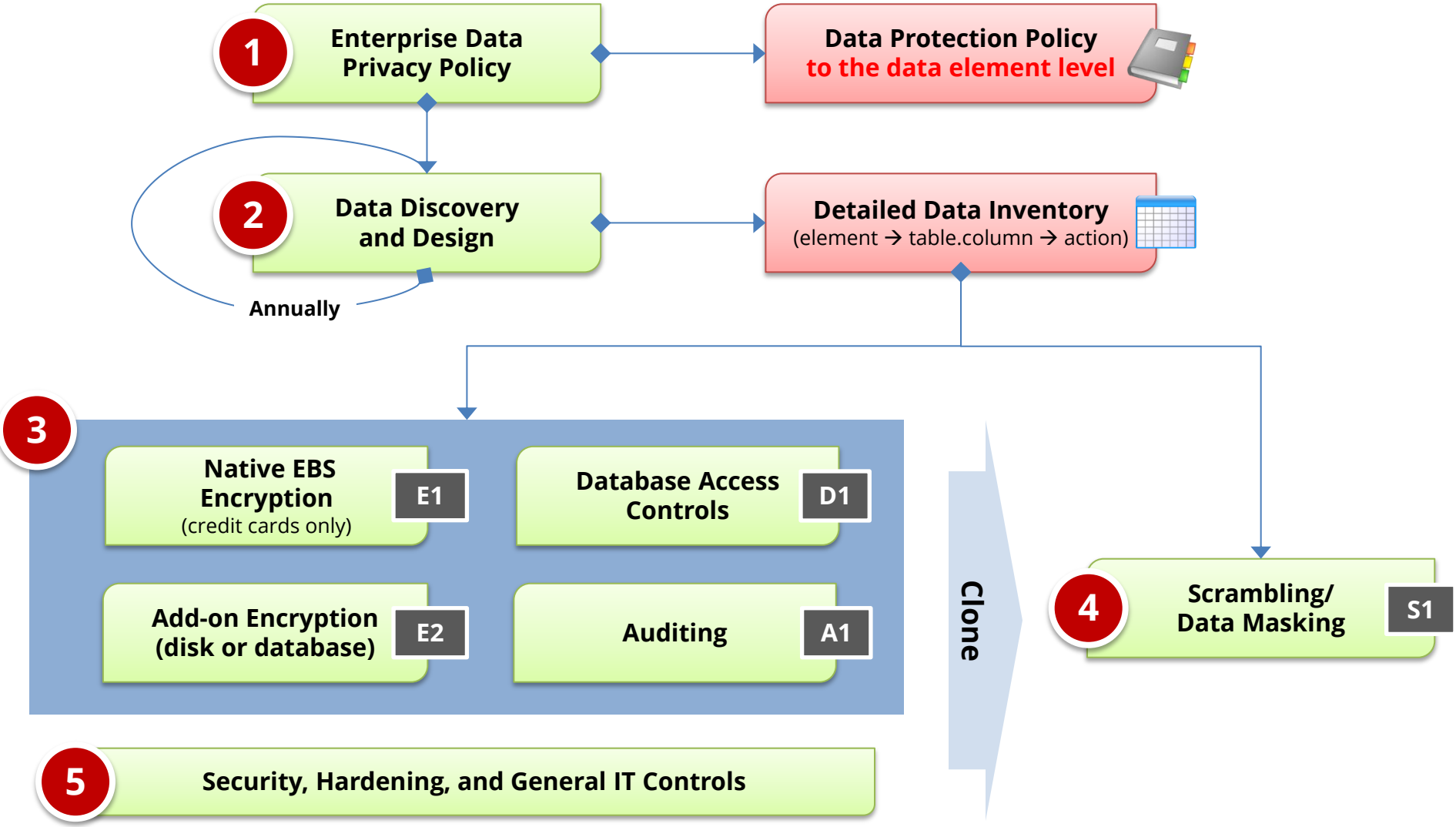
Log files

- Log files generated by the application (e.g., iPayment)

Database

File System

How – EBS Data Protection Process

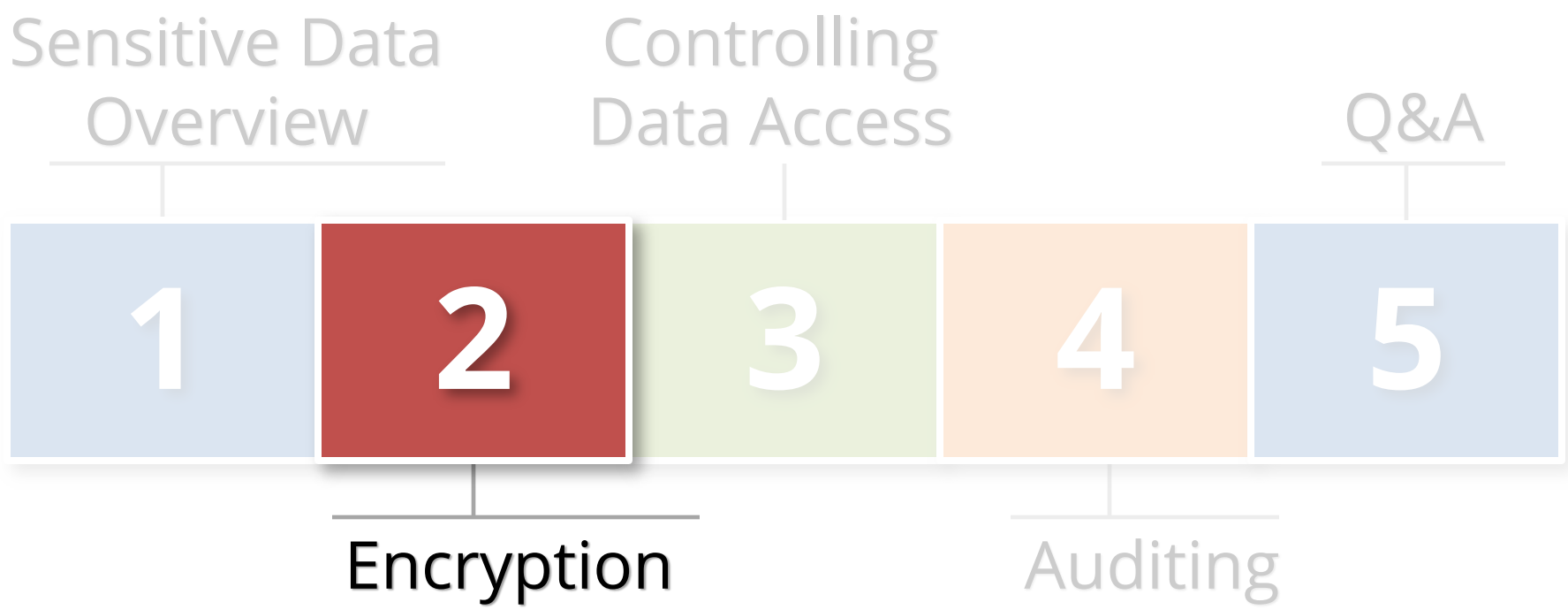


How - Data Protection vs. Threats

Data Access Method and Threats	Options						
	1 EBS Encrypt	2 Trigger View	3 Oracle TDE	4a FGAC	4b Internal Audit	4c External Audit	3 + 4 TDE + Auditing
1. Application access by end-users (responsibility)	E	E		C	A	A	A
2. Application access by application administrators	E+	E-		C	A	A	A
3. Database access by DBA	E	E		C	A+	A	A
4. Database access by Applications DBA (SYSTEM, APPS)	E+	E+			A+	A+	A+
5. Database access by other database accounts	E	E		C	A	A	A
6. Operating system access to database data files	E	E	E				E
7. On-line or off-line access to database backups	E	E	E				E
8. Exploitation of Oracle Applications security vulnerabilities	E-	E-		C+	A+	A+	A+
9. Exploitation of Oracle Database security vulnerabilities	E+	E+		C+	A+	A+	A+
10. Exploitation of operating system security vulnerabilities	E	E	E				E

E = Encrypted, **C** = Access Controlled, **A** = Access Audited, **+** = Mostly **-** = Partially

Agenda


Sensitive Data Overview
Controlling Data Access
Q&A
1
2
3
4
5
Encryption
Auditing

Types of Encryption

- **Storage (Data at rest)**
  - **Disk level encryption**
  - Encryption of data at rest such as when stored in files or on media
- **Access (Data in use)**
  - **Application or database level encryption**
  - Encryption of data with access permitted only to a subset of users in order to enforce segregation of duties
- ***Network (Data in motion)***
  - *Encryption of data when transferred between two systems*
  - *SSL/HTTPS (users) and SQL*Net encryption (database)*

Oracle EBS Encryption Solutions

Application (access = responsibility)	▪ **Oracle EBS Credit Card Number Encryption** ▪ Encryption Customization (DBMS_CRYPTO/FND_VAULT)
Database (access = db account)	▪ ~~View/Trigger Encryption Solutions~~
Disk/Storage (access = database)	▪ **Oracle Transparent Data Encryption (TDE)** ▪ Third-party Solutions (e.g., Vormetric) ▪ Disk/SAN Vendor Encryption Solutions

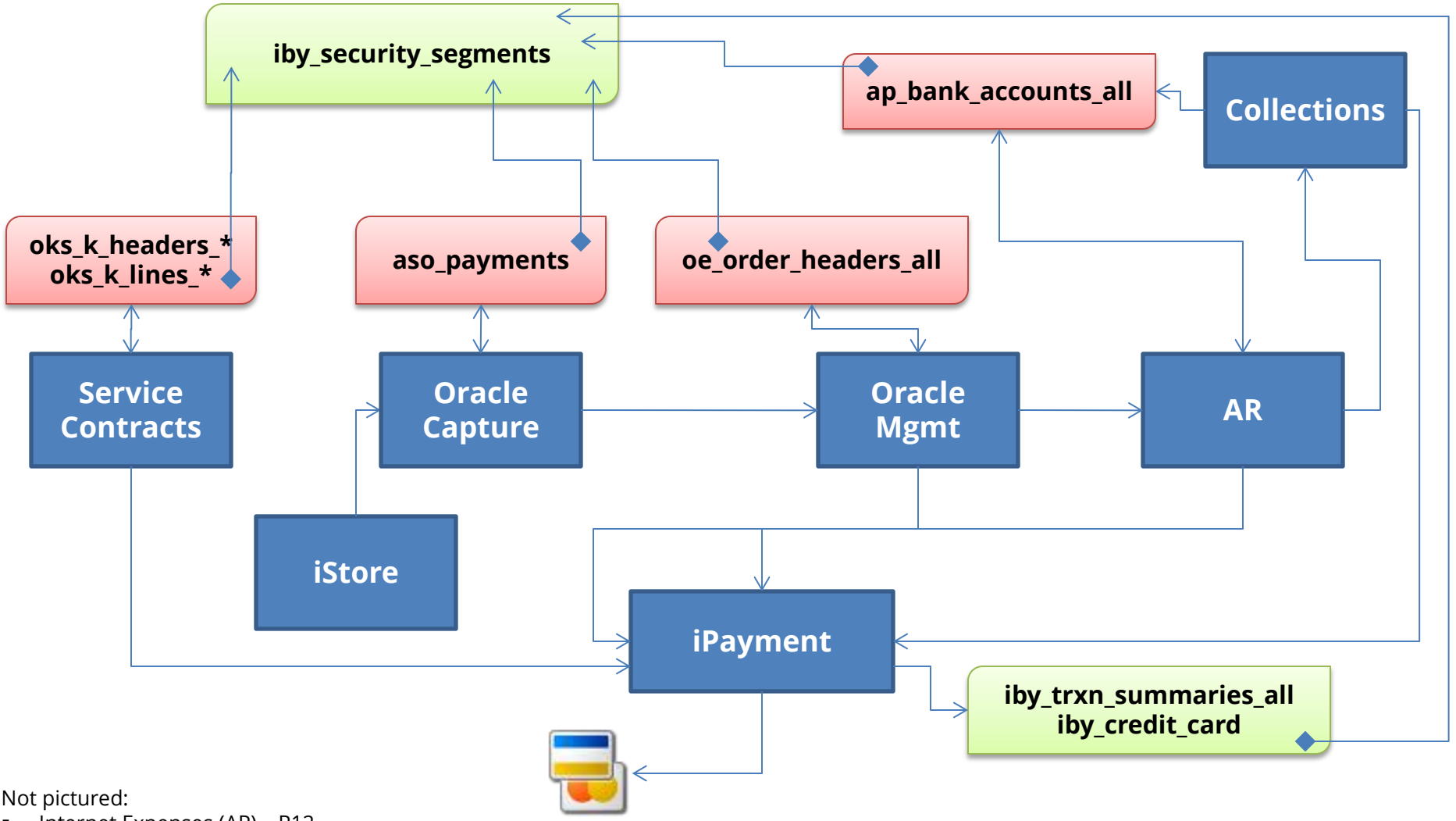
Native EBS Encryption (Credit Card Numbers)

Oracle Credit Card Encryption (no TDE)

- **Application-level encryption**
  - **Not enabled by default in 11i or R12**
  - Better solution than other technologies such as Oracle Transparent Data Encryption (TDE)
  - General patch release availability October 2006
  - Significant modification to application – 64 packages, 60 web pages, and 18 forms

- **11i = MOS Note ID 338756.1, Patch 4607647**
- **R12 = MOS Note ID 863053.1**
  - Consolidates card numbers into IBY_SECURITY_SEGMENTS table
  - Encrypts card numbers in IBY_SECURITY_SEGMENTS
  - Uniform masking of card numbers
  - Significant functional pre-requisites (11.5.10.2)

Oracle Credit Card Encryption Design



Not pictured:

- Internet Expenses (AP) – R12
- Lease Management (AP) – same as AR
- Student System (IGS) – IGS patch

Oracle Transparent Data Encryption (TDE)

What is Oracle TDE?

- **Transparent database encryption**
  - Requires no application code or database structure changes to implement
  - Only major change to database function is the Oracle Wallet must be opened during database startup
  - Add-on feature licensed with Advanced Security Option

- **Limited to encrypting only certain columns**
  - Cannot be a foreign key or used in another database constraint
  - Only simple data types like number, varchar, date, …
  - Less than 3,932 bytes in length

What does TDE do and not do?

- **TDE only encrypts "data at rest"**
- **TDE protects data if following is stolen or lost -**
  - disk drive
  - database file
  - backup tape of the database files
- **An authenticated database user sees no change**
- **Does TDE meet legal requirements for encryption?**
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department

Data Center Theft

From Chicago Police Report -

- At least two masked intruders entered the suite after cutting into the reinforced walls with a power saw.
- During the robbery, the night manager was repeatedly tazered and struck with a blunt instrument.
- At least 20 data servers were stolen.

Column vs. Tablespace Encryption

Column encryption

- Fairly straight forward for simple cases such as NATIONAL_IDENTIFIER in HR.PER_ALL_PEOPLE_F
- Encryption done in place using ALTER TABLE
- Do not use SALT for Oracle EBS columns
- **Use for standard Oracle EBS columns**

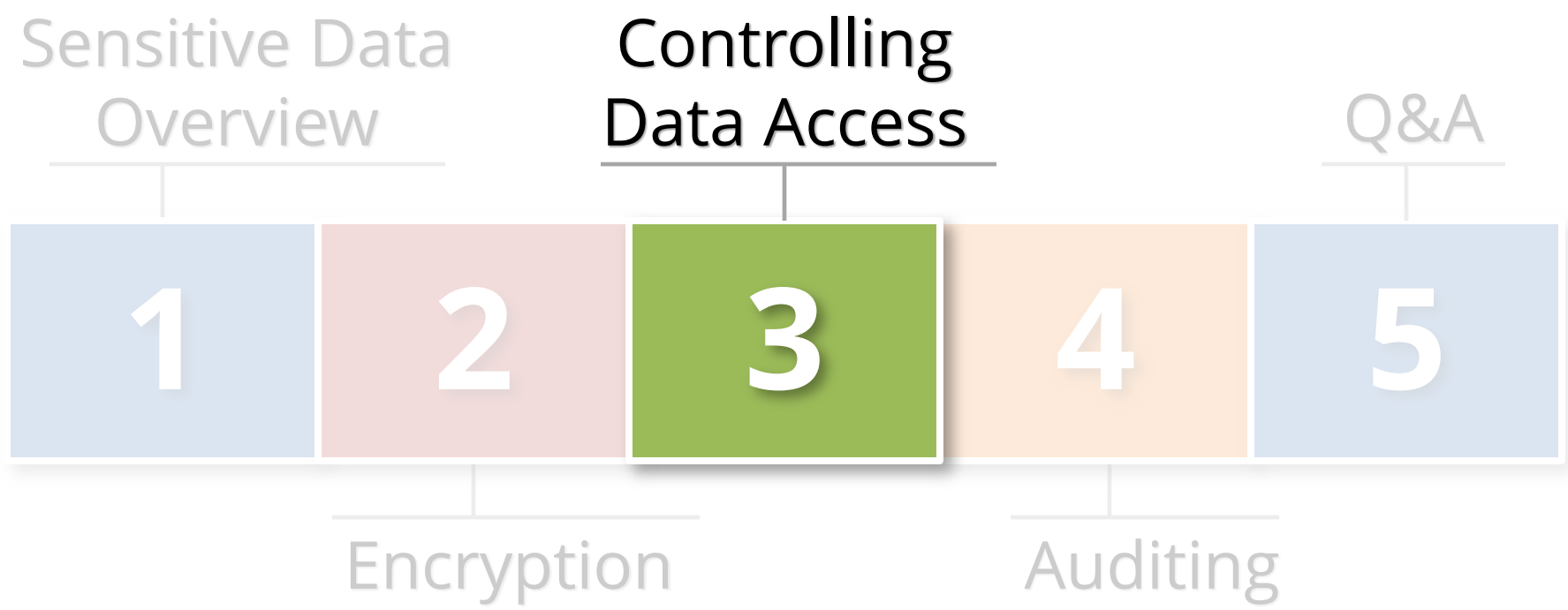
Tablespace encryption

- Tablespace encryption only supported in 11g for 11i/R12
- Tablespace must be exported and imported to implement encryption
- OATM uses large tablespaces (APPS_TS_TX_DATA)
- **Use for custom tablespaces**

Performance Considerations

- **Impact is limited to CPU performance**
  - Data must be encrypted and decrypted
  - Highly dependent on access patterns to data
- **No disk I/O read or write impact**
  - Change is not significant
- **Column Encryption**
  - 5% to 20% CPU performance impact for several customers
- **Tablespace Encryption**
  - 10% to 15% CPU performance impact for one customer

Agenda


Sensitive Data Overview
Controlling Data Access
Q&A
1
2
3
4
5
Encryption
Auditing

Oracle EBS Database Access Controls

Defense in depth – implement layers!

Application	▪ Oracle EBS Application Security (roles/responsibilities/menus/functions) ▪ Oracle EBS Personalizations ▪ Application Data Masking (e.g., Mentis)
Database	▪ Database Security (roles/privileges) ▪ Fine Grained Access Controls (FGAC) ▪ Oracle Database Vault
Operating System	▪ Operating System Security ▪ Sudo and Powerbroker

Access to Sensitive Data

- **Block ad-hoc access to production database whenever possible**
  - **Integrigy #1 Security Recommendation**
  - Managed SQL*Net access
  - Oracle Connection Manager
  - Data center firewall – use VPN or jump servers
- **Database access is a key problem**
  - APPS_READ
- **Access to sensitive data by generic accounts**
  - Granularity of database privileges, complexity of data model, and number of tables/views make it difficult to create limited privilege database accounts
  - Must use individual database accounts with roles limiting access to data along with other security

Oracle Fine Grained Access Controls (FGAC)

- **FGAC included with Oracle EBS database license**
- **FGAC policies allow blocking of access to column (returns null)**
  - Modifies SQL at runtime to include a predicate clause for users included in policy
- **Create policies by database role to block access to sensitive columns**
  - Create roles so “default deny” – if role then allow

Oracle Database Vault with Oracle E-Business Suite

What is Database Vault?

- **Powerful protection**
  - Data protection realms
  - Control by IP address, time, etc.
  - Control SQL commands and other database operations
- **Provides segregation of duties between DBA and security administrator**
- **Add-on option licensed separately**

Database Vault and EBS Scenarios

- **Protect <u>some</u> DBAs from application data**
  - **No protection for the SYSTEM, APPS, CTXSYS, or Oracle EBS module schema accounts**
  - Named, non-application database accounts must be used for this level of protection – can be granted DBA role

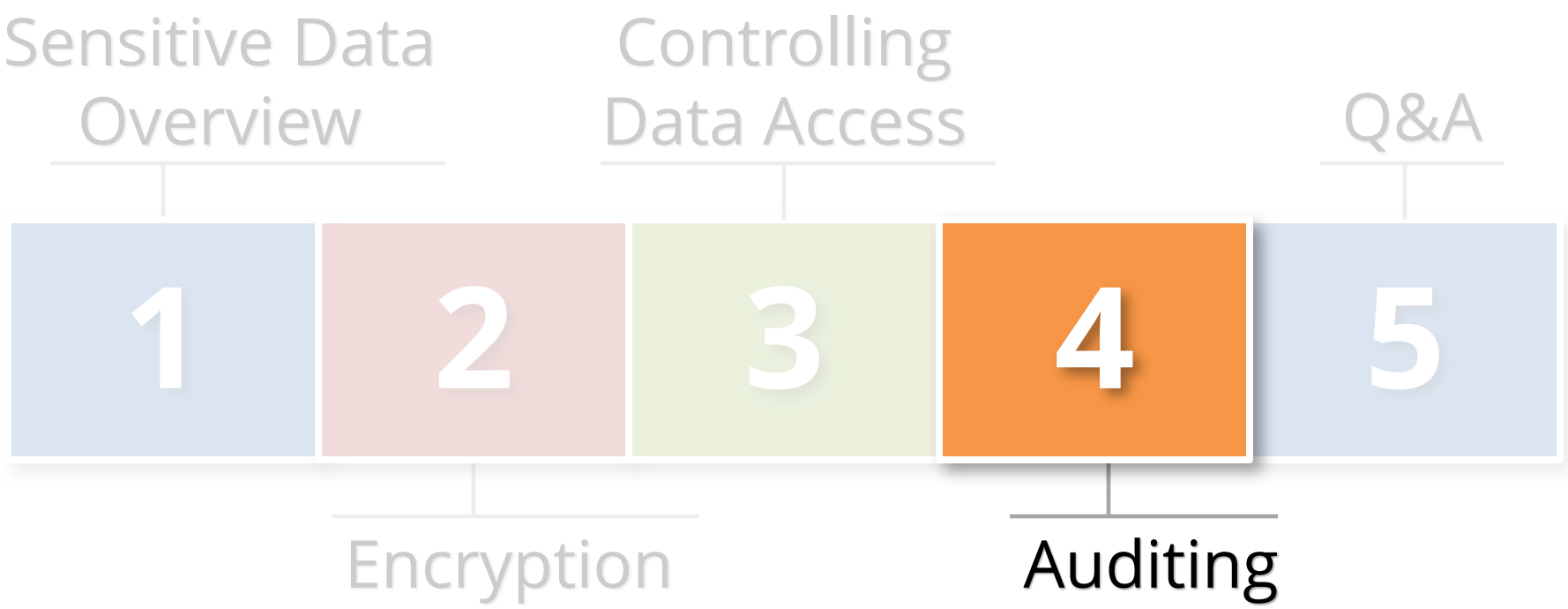
- **Server/Database Consolidation**
  - Multiple applications running in Oracle E-Business Suite database (against best practice)
  - DBAs for other applications cannot access EBS data

Default Oracle EBS Realms

Realm Name	What is Protected?	Who is authorized to access?
EBS Realm	All tables in Oracle E-Business Suite Product Schemas	All Oracle E-Business Suite Product Schemas, and APPS, APPLSYS, SYSTEM, CTXSYS
EBS Realm - Applsys Schema	Most tables in the APPLSYS Schema	APPS, APPLSYS, SYSTEM and CTXSYS
EBS Realm - Apps Schema	All objects in the APPS Schema (except the views)	APPS, APPLSYS, SYSTEM, CTXSYS and All product schemas, that uses intermedia indexes
EBS Realm - Applsyspub Schema	Objects required for EBS authorization	APPS, APPLSYS, SYSTEM, APPLSYSPUB and CTXSYS
EBS Realm - MSC Schema	Tables in the MSC Schema - except those that require partitions to be exchanged	APPS, APPLSYS, SYSTEM, CTXSYS and MSC
CTXSYS Data Dictionary	Objects in the CTXSYS Schema	All Oracle E-Business Suite 11i Product Schemas and APPS, APPLSYS, SYSTEM

Source: Oracle Metalink Note ID 428503.1

Agenda


Sensitive Data Overview
Controlling Data Access
Q&A
1
2
3
4
5
Encryption
Auditing

Auditing Access to Sensitive Data

- **Native audit trail in Oracle Database and Oracle EBS can be accessed and manipulated by the DBA**
  - SYSLOG auditing can be used to protect native database audit trail – DBA can disable it
- **External auditing solution required**
  - Protect audit trail in external database/appliance
  - Provide reporting and archiving of audit data

Data Scrambling/ Data Masking

Data Scrambling/Data Masking

- **Sensitive data in test & development must be scrambled**
  - Sensitive data inventory is critical to scrambling
  - Must periodically review database for instances of non-scrambled data as often in custom, interface, and temporary tables
- **Purge production as well as scramble**
  - Review data and transaction retention policy
  - Oracle EBS is “data in” for life – seldom purged
  - PCI Compliance = 1 to 2 years recommended retention

Data Scrambling/Data Masking

- **Data scrambling solutions**
  - Custom scripts – when just a few data elements
  - Oracle OEM Data Masking Pack (EBS Template)
  - Oracle AMP Data Masking (Cloning)
  - Mentis iScramble

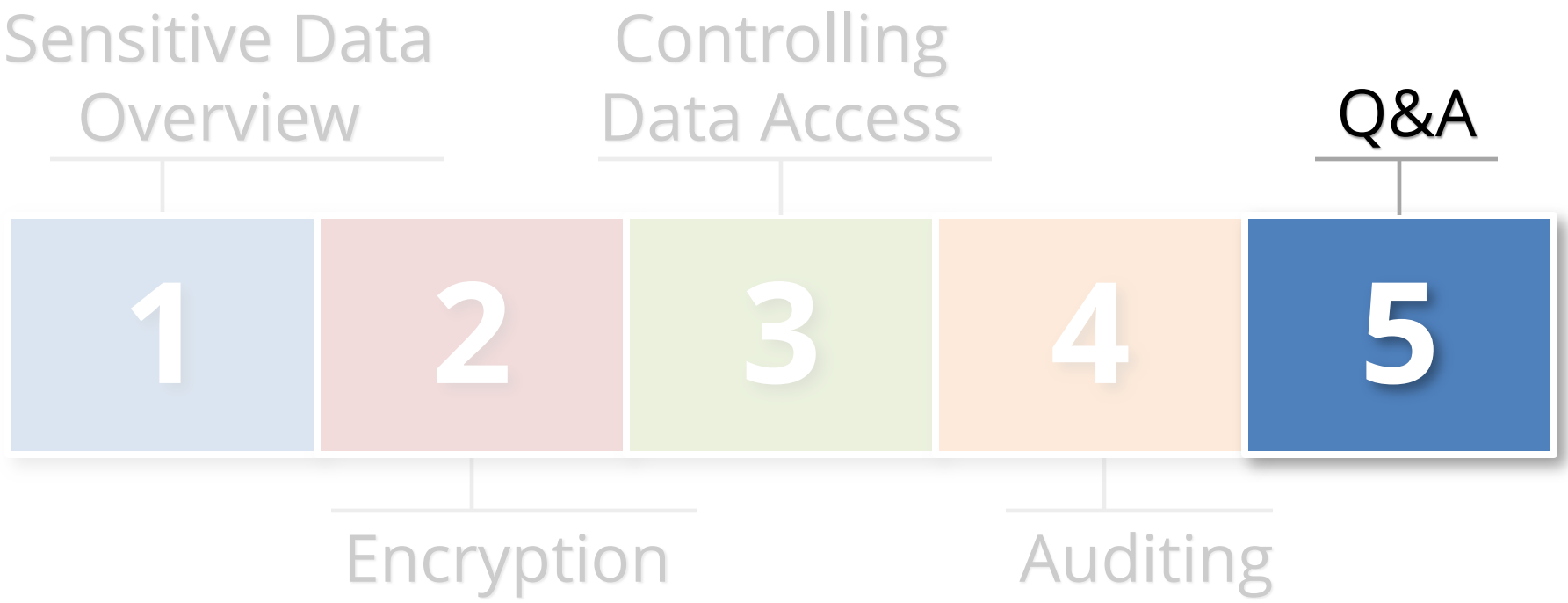
- **Data Scrambling best practices**
  - Keep it simple – runtime and data issues
  - Use predictable data patterns to act as an ad-hoc control such as 7xx-xx-xxx for SSN

How - Data Protection vs. Threats

Data Access Method and Threats	Options						
	1 EBS Encrypt	2 Trigger View	3 Oracle TDE	4a FGAC	4b Internal Audit	4c External Audit	3 + 4 TDE + Auditing
1. Application access by end-users (responsibility)	E	E		C	A	A	A
2. Application access by application administrators	E+	E-		C	A	A	A
3. Database access by DBA	E	E		C	A+	A	A
4. Database access by Applications DBA (SYSTEM, APPS)	E+	E+			A+	A+	A+
5. Database access by other database accounts	E	E		C	A	A	A
6. Operating system access to database data files	E	E	E				E
7. On-line or off-line access to database backups	E	E	E				E
8. Exploitation of Oracle Applications security vulnerabilities	E-	E-		C+	A+	A+	A+
9. Exploitation of Oracle Database security vulnerabilities	E+	E+		C+	A+	A+	A+
10. Exploitation of operating system security vulnerabilities	E	E	E				E

E = Encrypted, **C** = Access Controlled, **A** = Access Audited, **+** = Mostly **-** = Partially

Agenda


Sensitive Data Overview
Controlling Data Access
Q&A
1
2
3
4
5
Encryption
Auditing

Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web: **www.integrigy.com**
e-mail: **info@integrigy.com**
blog: **integrigy.com/oracle-security-blog**