cardconnect

INTEGRIGY

PCI Compliance in Oracle E-Business Suite

October 22, 2014

Mike Miller
Chief Security Officer
Integrigy Corporation

Megan Kelly
Senior Director of ERP Integrations
CardConnect

Moderated by Phil Reimann, Director of Business Development, Integrigy Corporation

Speakers

Michael Miller

Michael Miller, CISSP-ISSMP is a Vice President of Integrigy and is responsible for Integrigy's security assessment services. For the past 16 years, Michael has exclusively focused on the Oracle E-Business Suite and has sat on Oracle's customer advisory boards for security and Oracle On-Demand.

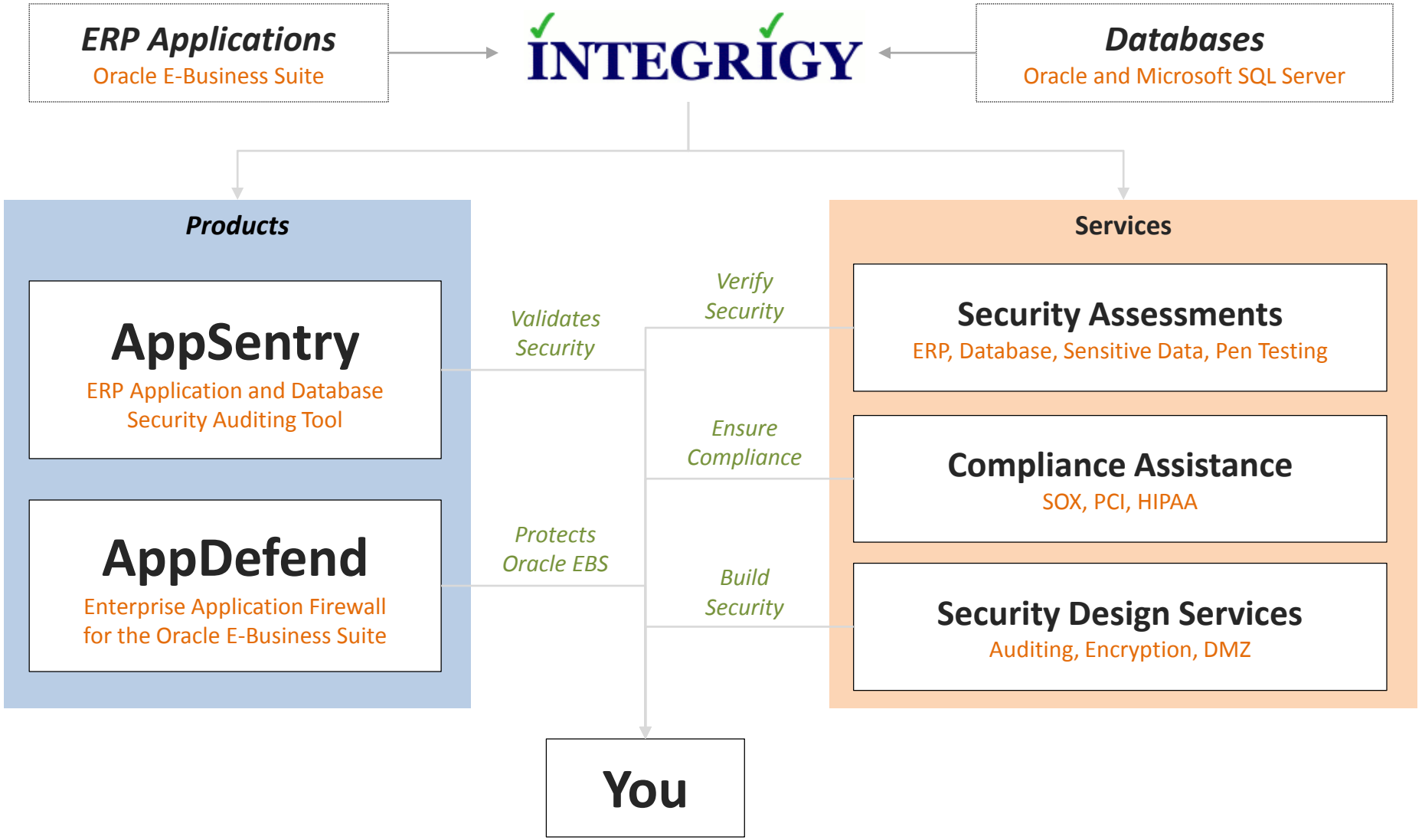
Megan Kelly

As the Director of ERP Integrations, Megan currently leads CardConnect's Integration Services department and in her career, has supported and designed solutions across Oracle modules for various business units from human resources to supply chain and finance. Megan received her Bachelor of Information Systems and Technology degree from Pennsylvania State University.

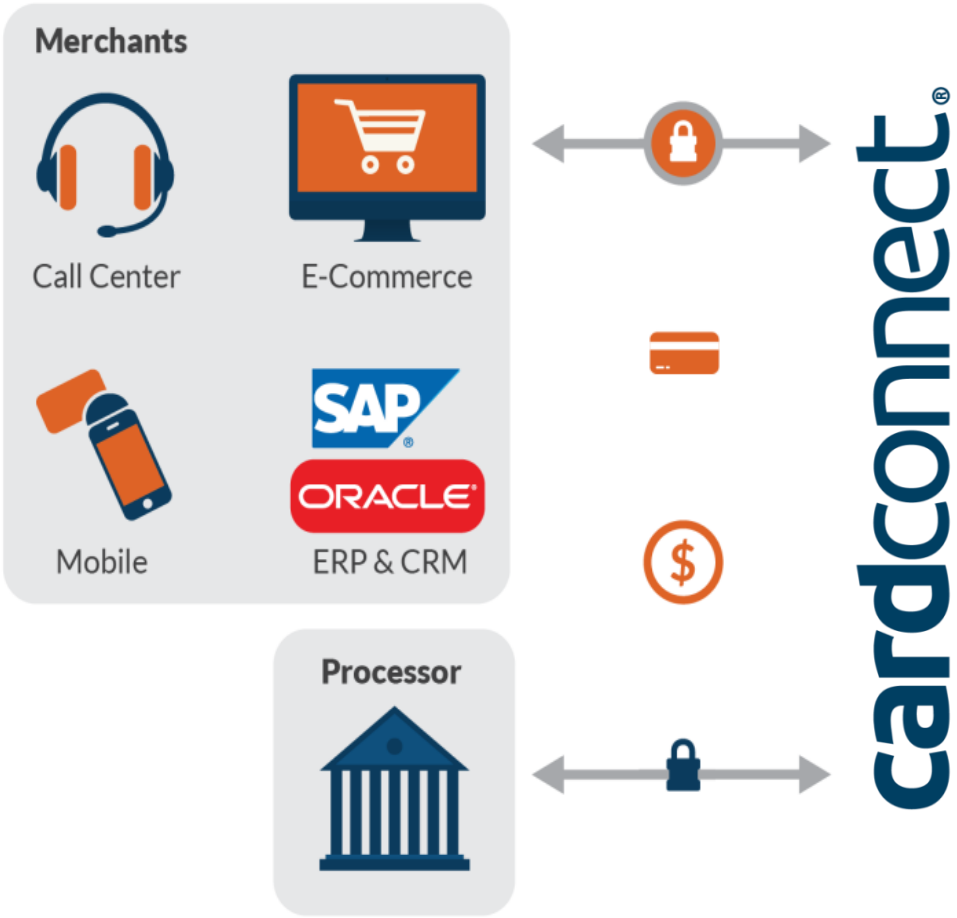
cardconnect®

INTEGRIGY

About Integrigy



About CardConnect



CardConnect Gateway

- Credit, debit, p-cards, ACH
- Level 2/3
- Multicurrency
- PCI Certified
- SOAP and REST API
- Oracle and SAP Validated Integration

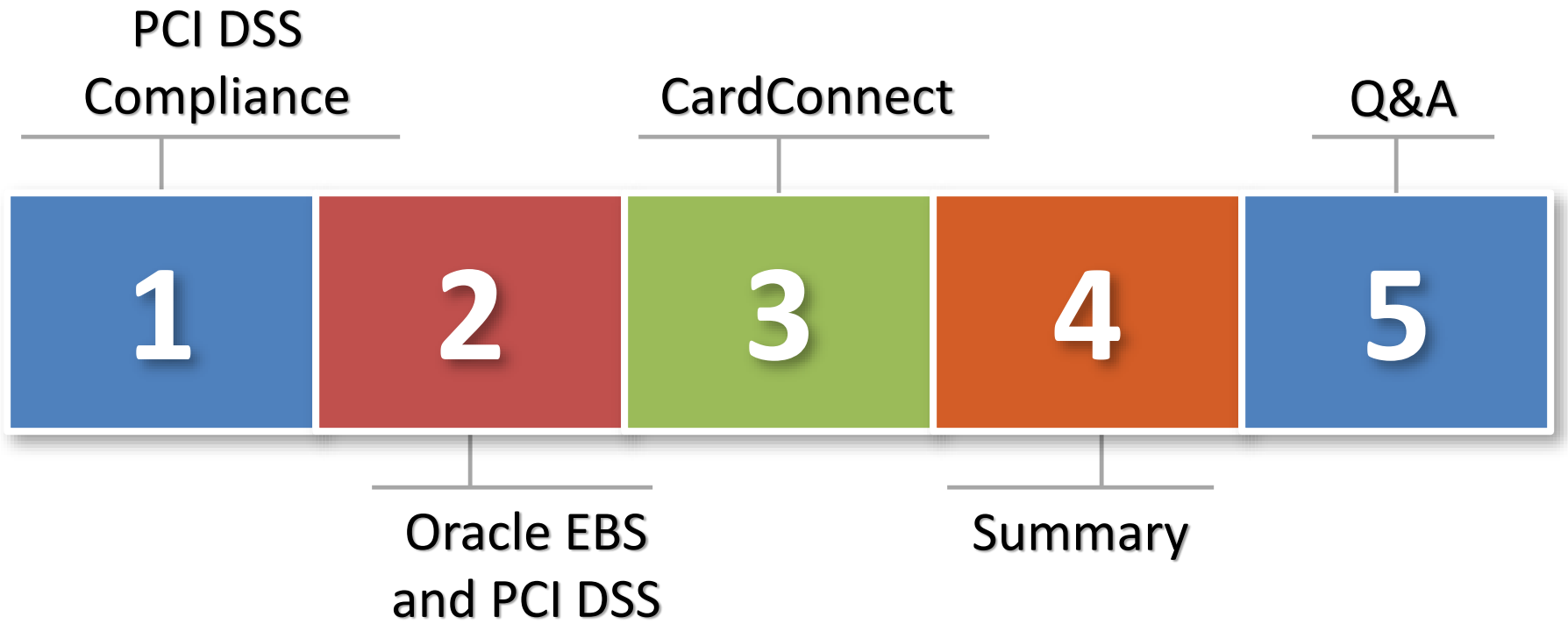
CardSecure® Vault

- 100% PCI Compliant data center
- Reduce PCI scope
- "Intelligent tokens", recognizable
- Pass validation checks
- Patented Solution

Acquiring and Reporting

- Aggressive Interchange management
- Robust reporting portal
- Full cycle reconciliation
- Transparent pricing
- Account Updater

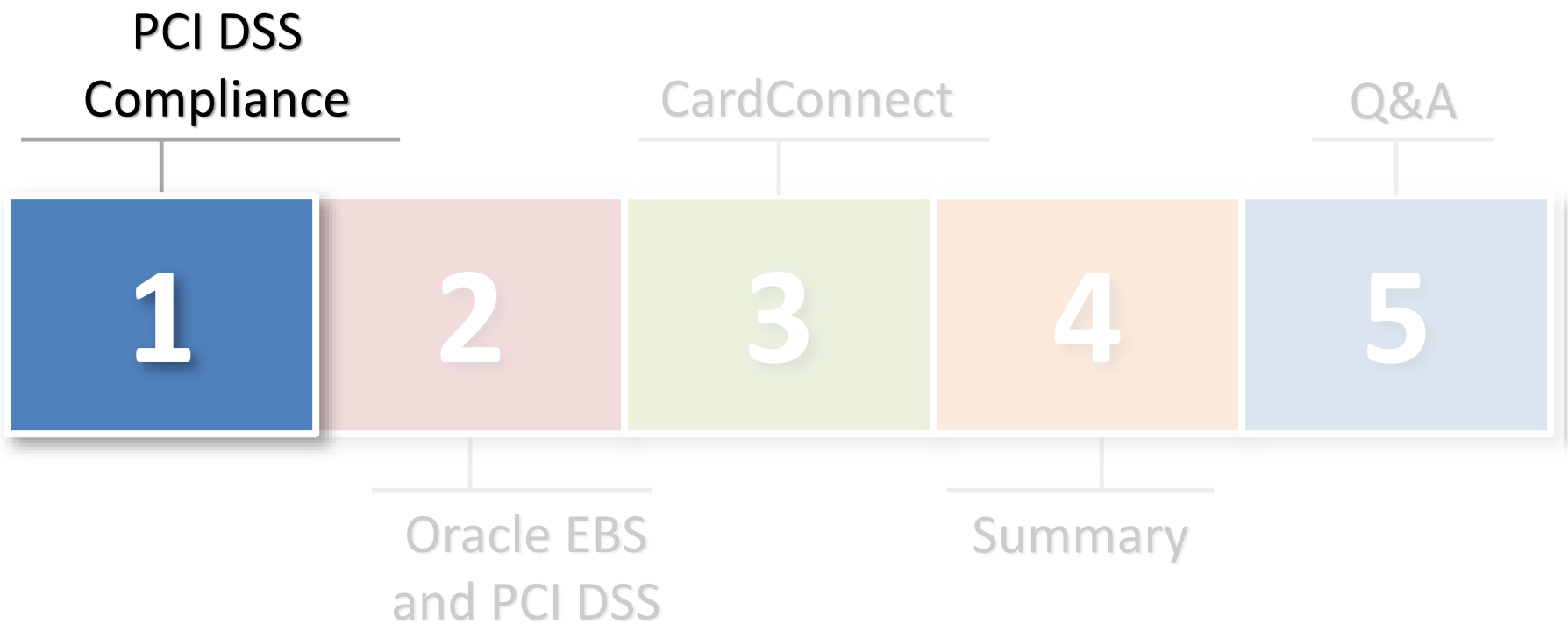
Agenda



cardconnect®

INTEGRIGY

Agenda



cardconnect®

INTEGRIGY

All Oracle E-Business Suite environments that **“store, process, or transmit cardholder data”** must comply with the Data Security Standard 3.0 (PCI DSS) regardless of size or transaction volume.

INTEGRIGY

PCI DSS 3.0 – EBS Requirement Mapping

#	Requirement	Network	Server	Database	Oracle EBS	Policy
1	Use Firewall to protect data	✓				✓
2	Do not use vendor-supplied defaults	✓	✓	✓	✓	✓
3	Protect stored cardholder data		✓	✓	✓	✓
4	Encrypt data across open, public networks	✓				
5	Use Anti-virus software		✓			✓
6	Develop and maintain secure applications	✓	✓	✓	✓	✓
7	Restrict access to cardholder data		✓	✓	✓	✓
8	Assigned unique IDs for access		✓	✓	✓	✓
9	Restrict physical access to data	✓	✓			✓
10	Track and monitor access	✓	✓	✓	✓	✓
11	Regularly test security	✓	✓	✓	✓	✓
12	Maintain information security policy					✓

INTEGRIGY

PCI DSS 3.0 – EBS Compliance Effort

#	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 data 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

INTEGRIGY

Oracle E-Business Suite and PCI Compliance

- **Standard installation is NOT COMPLIANT**
- **R12 provides new PCI DSS functionality**
  - Supersedes 11i functionality
  - **Disabled by default**
- **PCI compliance in Oracle EBS is not a one-time setup**
  - Maintenance and on-going monitoring required

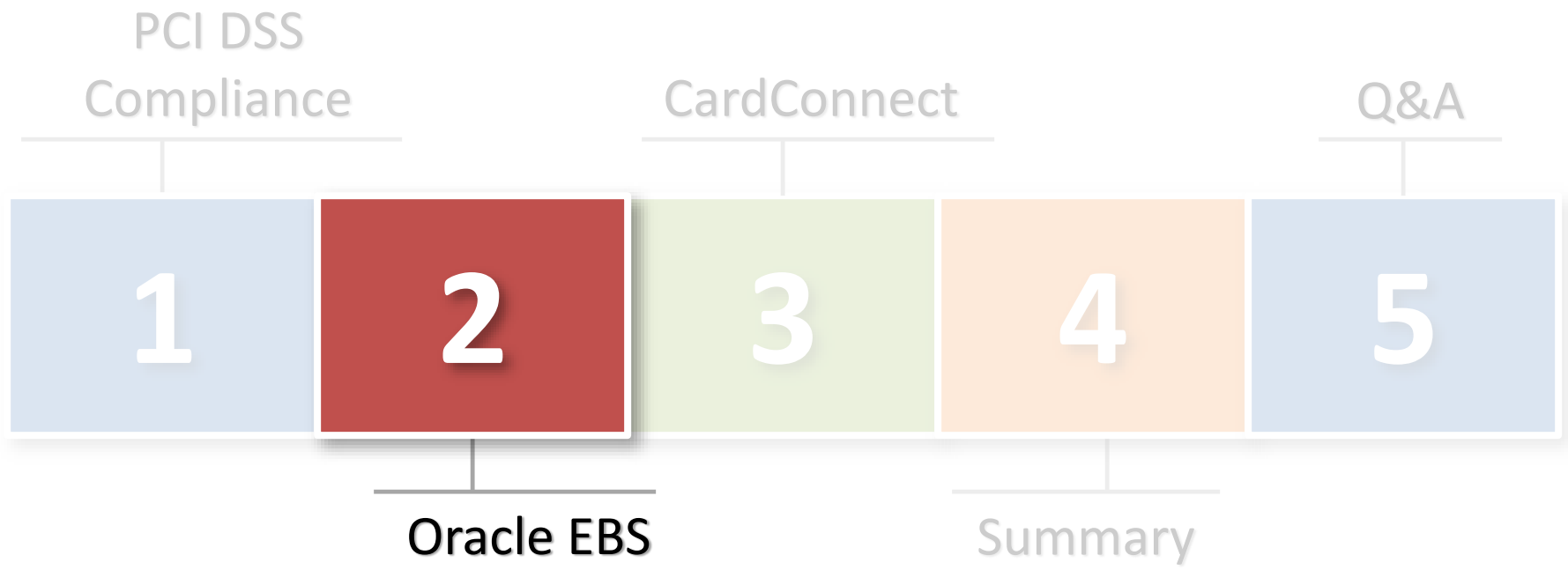
INTEGRIGY

Non-Encryption PCI Requirements

Requirement 6 – Develop and maintain secure systems	• Apply Application and database CPU security patches within 30 days of release
Requirement 8 - Assign unique ID to each person with access	• No generic accounts • Every 90 days disable inactive users and change user passwords • Strict password complexity
Requirement 10 – Track and monitor all access to network resources	• Log all activity to cardholder data • Implement automated audit trails • Daily log review
Requirement 11 – Regularly test security systems and processes	• Annual application penetration test • Quarterly internal and external vulnerability scans • Deploy file integrity monitoring

INTEGRIGY

Agenda



cardconnect.

INTEGRIGY

R12 Oracle Payments

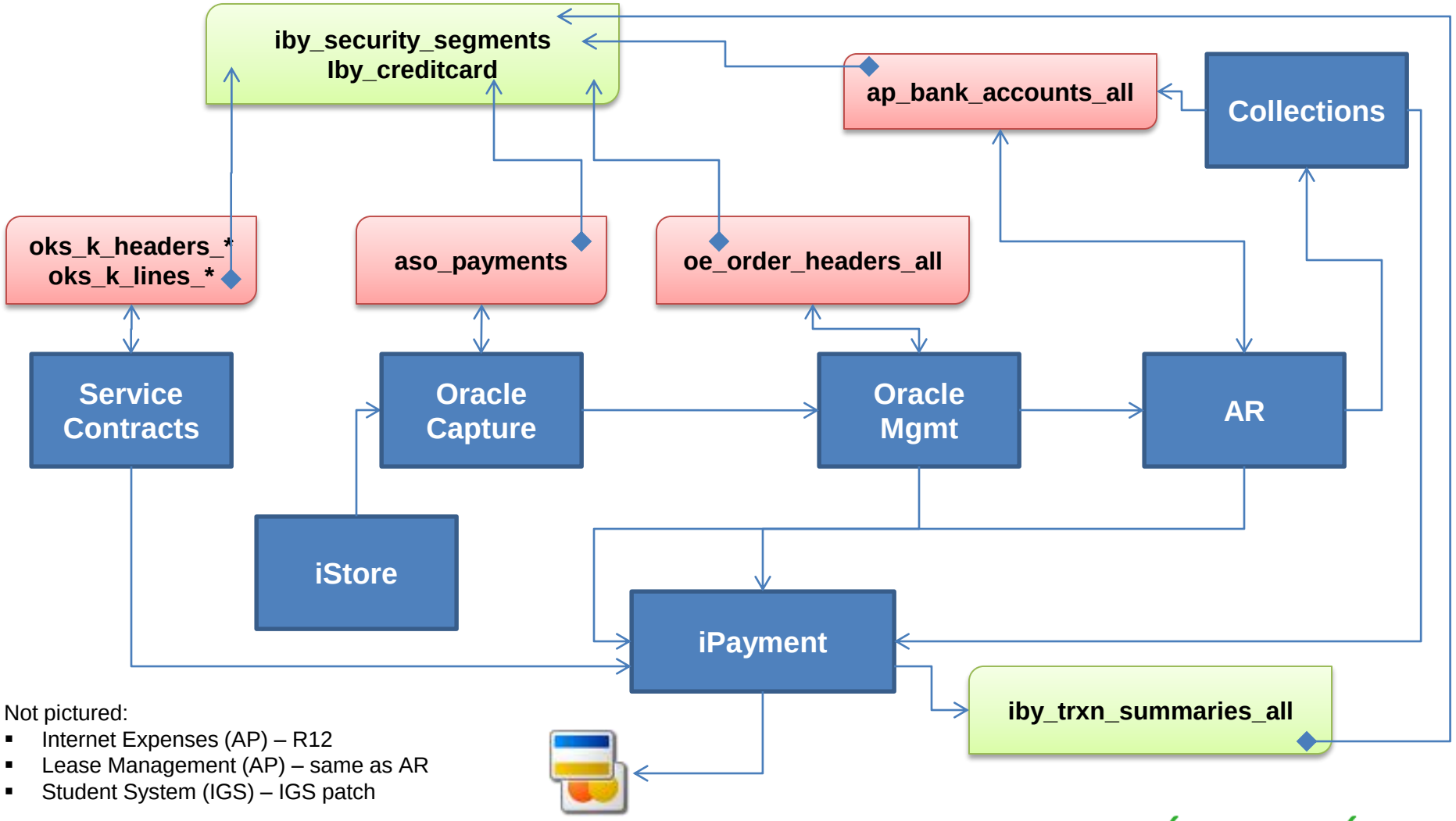
- **Oracle Payments** – new R12 module consolidates all payment activity within Oracle Financials
  - Including processing and storage of credit cards

- **Secure Payments Repository** – part of Oracle Payments
  - Consolidates storage of TCA party external accounts
  - Provides PCI encryption and masking – **disabled by default**

Oracle Financial Modules Using Secure Payment Repository		
▪ Oracle Advanced Collections	▪ Oracle Order Capture	▪ Oracle Payments
▪ Oracle iExpenses	▪ Oracle Order Management	▪ Oracle Quoting
▪ Oracle iReceivables	▪ Oracle Partner Management	▪ Oracle Service Contracts
▪ Oracle iStore	▪ Oracle Payables	

INTEGRIGY

Oracle Credit Card Encryption Design



Not pictured:

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

INTEGRIGY

Enabling E-Business Credit Card Protection

Three step process to enable encryption

1. Create Payment wallet
2. Set protection configuration options
3. Encrypt existing cardholder data

INTEGRIGY

Issue: Test and Development Instances

- **6.4.3** – No production or “live” cardholder data allowed for test or development
- **3.5** – Protection of encryption keys
- **Building non-production instances**
  1. Production payment wallet rotated and securely wiped
  2. Location of Payment wallet reset
  3. Remove, purge and/or scramble production cardholder data

INTEGRIGY

Issue: Purge Cardholder Data

- **3.1** – Keep cardholder data storage to a minimum
  - Limit storage and retention time to that which is required for legal, regulatory, and business requirements
  - A quarterly process to purge data that exceeds defined retention

- Oracle does not provide a single solution to purge Cardholder data
  - Most modules **DO NOT** provide purging solutions – bugs and enhancements exist

- **Purging Cardholder data**
  1. Consult module implementation guides
  2. Custom purge or obfuscate (scramble)
  3. Include all instances (test and non-production)

INTEGRIGY

Issue: Where Else Might Cardholder Data Exist?

- **Custom tables**
  - Customizations may be used to store or process credit card data
- **"Maintenance tables"**
  - DBA copies tables to make backup prior to direct SQL update
  - iby.iby_security_segments_011510
- **Interface tables**
  - Credit card numbers are often accepted in external applications and sent to Oracle EBS
- **Interface files**
  - Flat files used for interfaces or batch processing
- **Log files**
  - Log files generated by the application (e.g., Oracle Payments)

INTEGRIGY

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

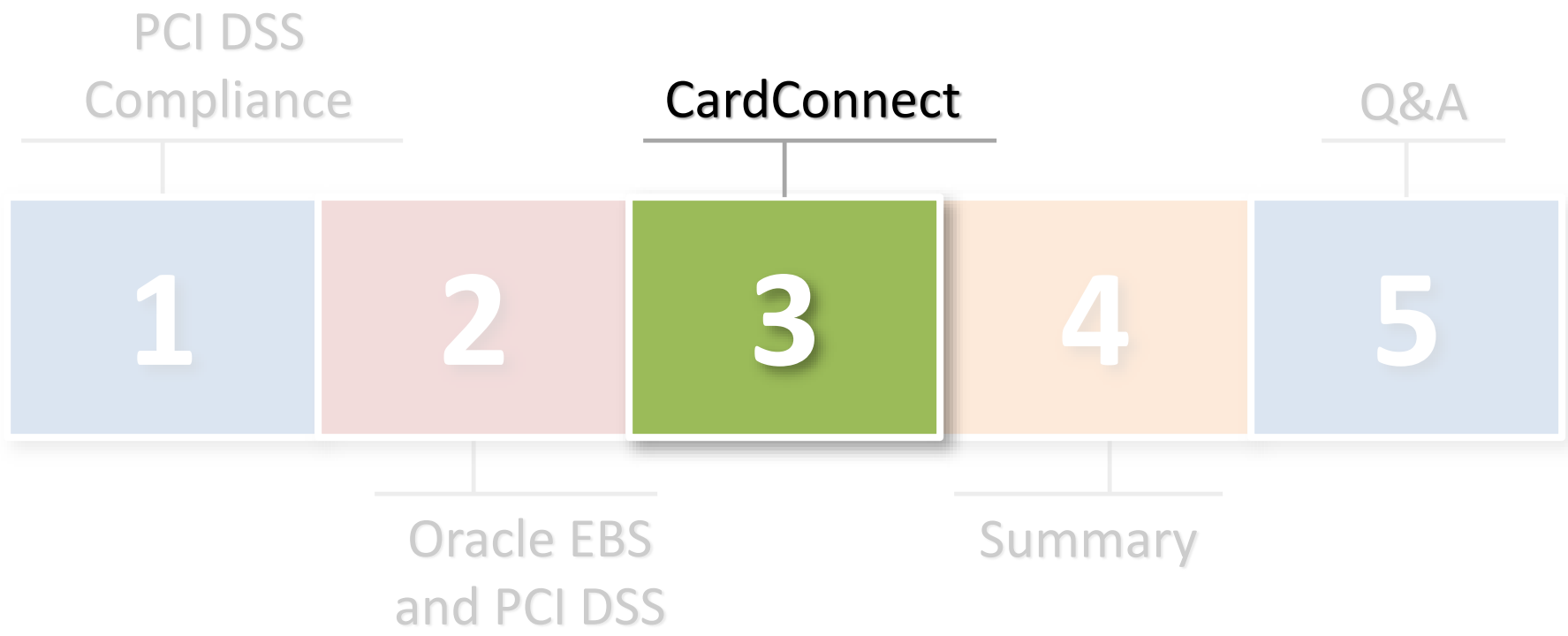
INTEGRIGY

Protection of Cardholder Data

- **PCI DSS compliance is costly and on-going**
  - Financial costs and velocity to business
- **PCI DSS secures the entire environment**
  - Encryption is only one requirement
- **Tokenization alternative**
  - Store cardholder data outside of Application

INTEGRIGY

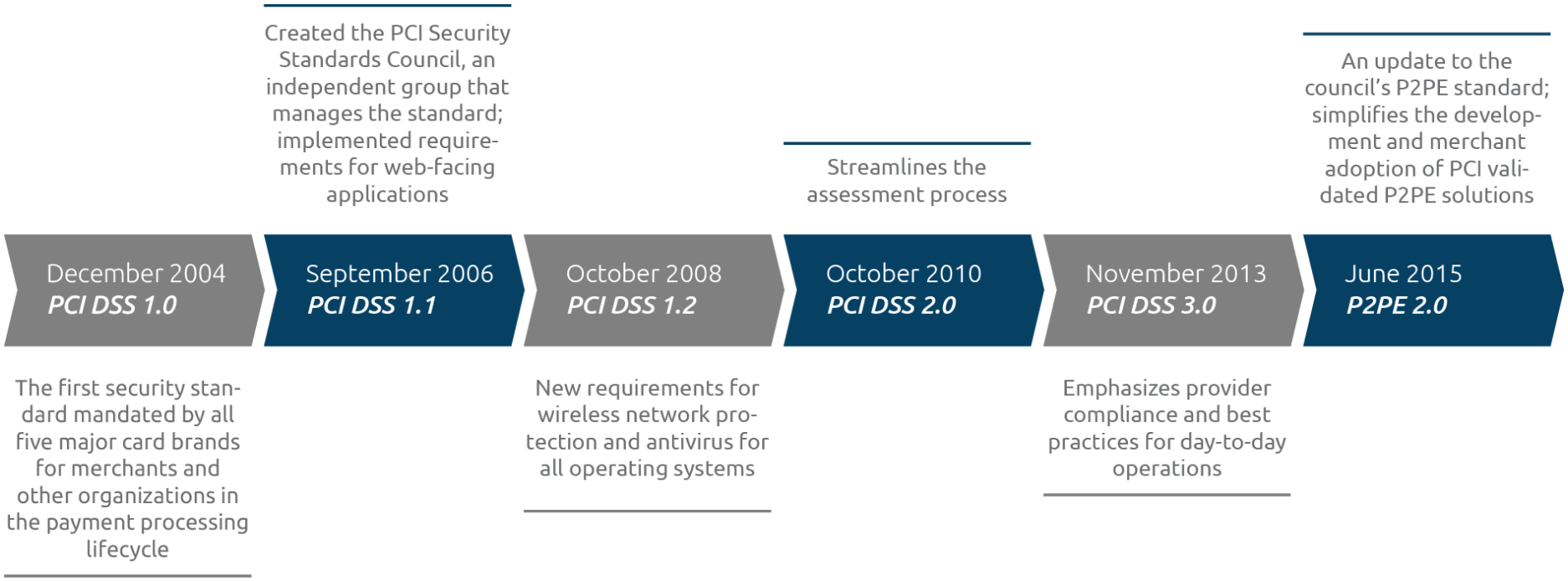
Agenda



cardconnect®

INTEGRIGY

A Decade of PCI



cardconnect

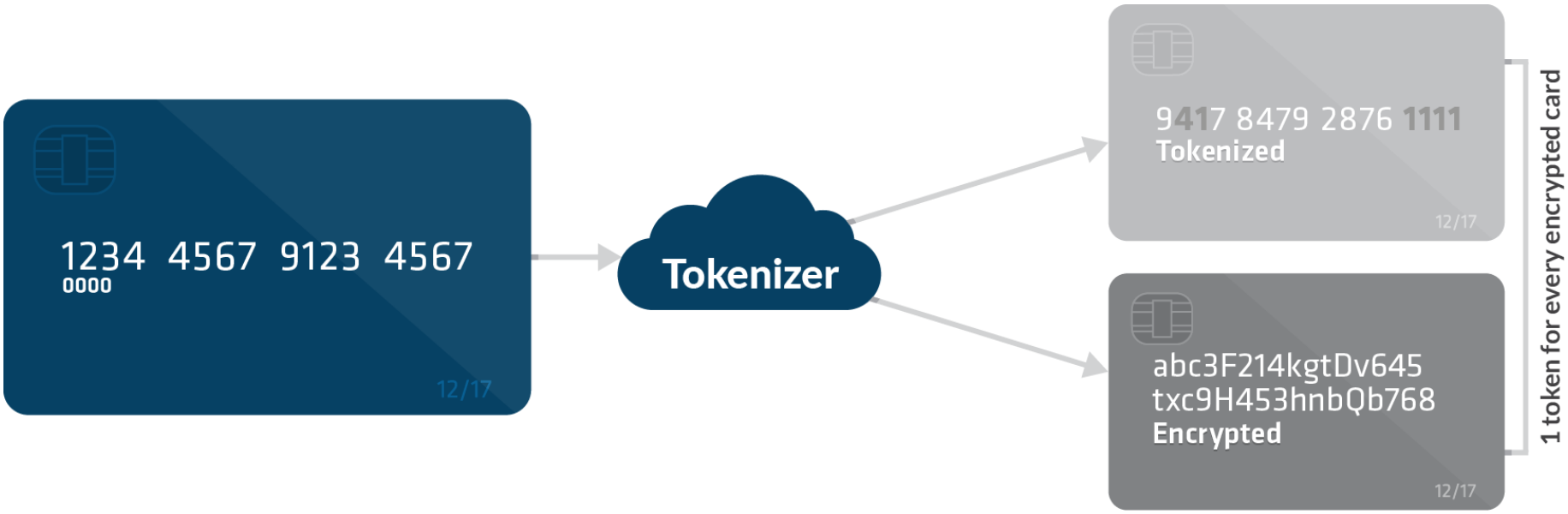
Compliance in Oracle

ORACLE®

E-BUSINESS SUITE

cardconnect®

Why Tokenize?

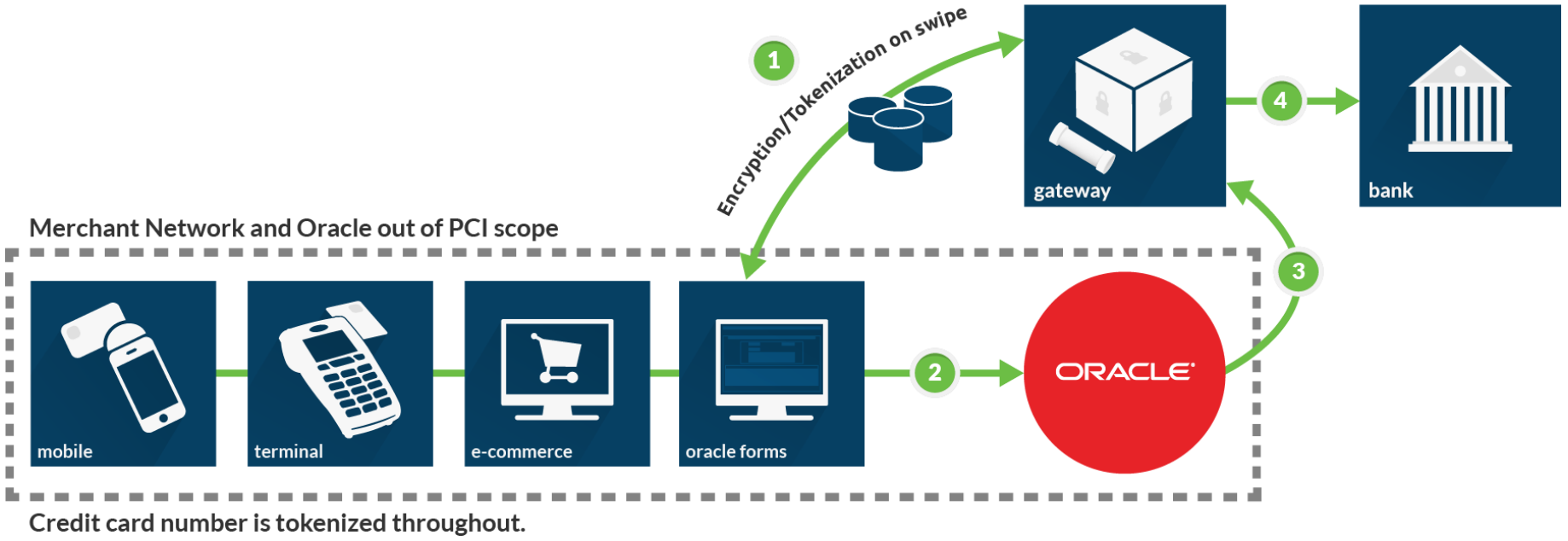


Tokenizing in Oracle

- Implementation
- The challenge of existing data

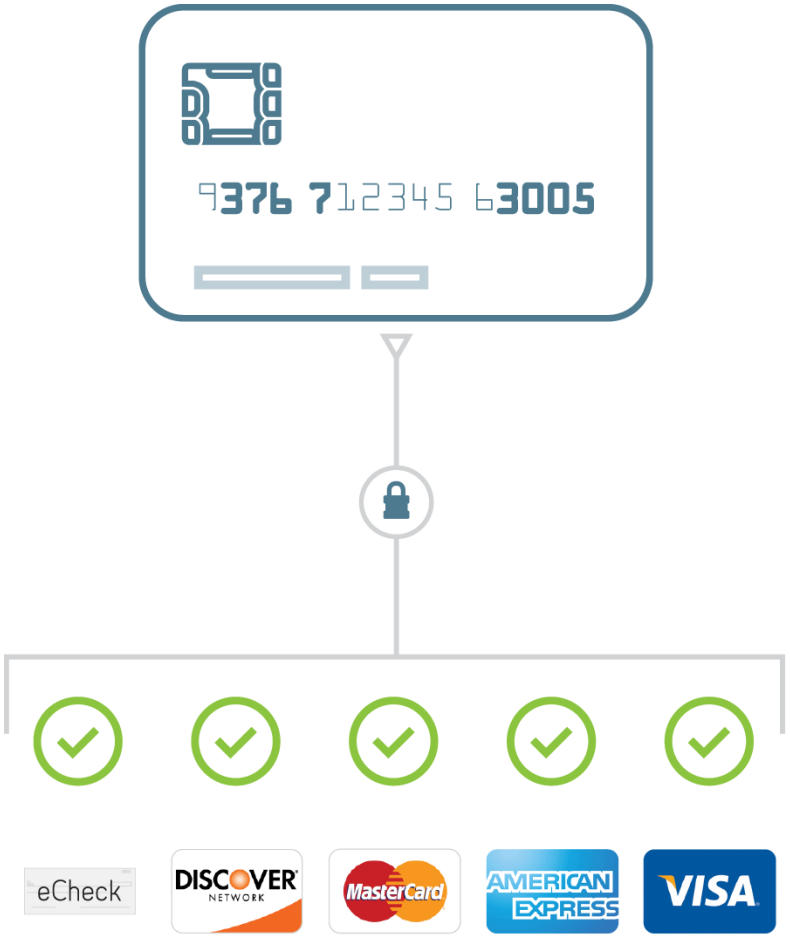
Secure Future Transactions

With existing data secured, all new data must be tokenized before entering the network.



cardconnect

Tokens in Detail



Token Security

> Random (irreversible) vs. Derivative

Token Intelligence

> Luhn Test, BIN Recognition

"High Value" Token

> Persistent Token vs. Individually Administered Token

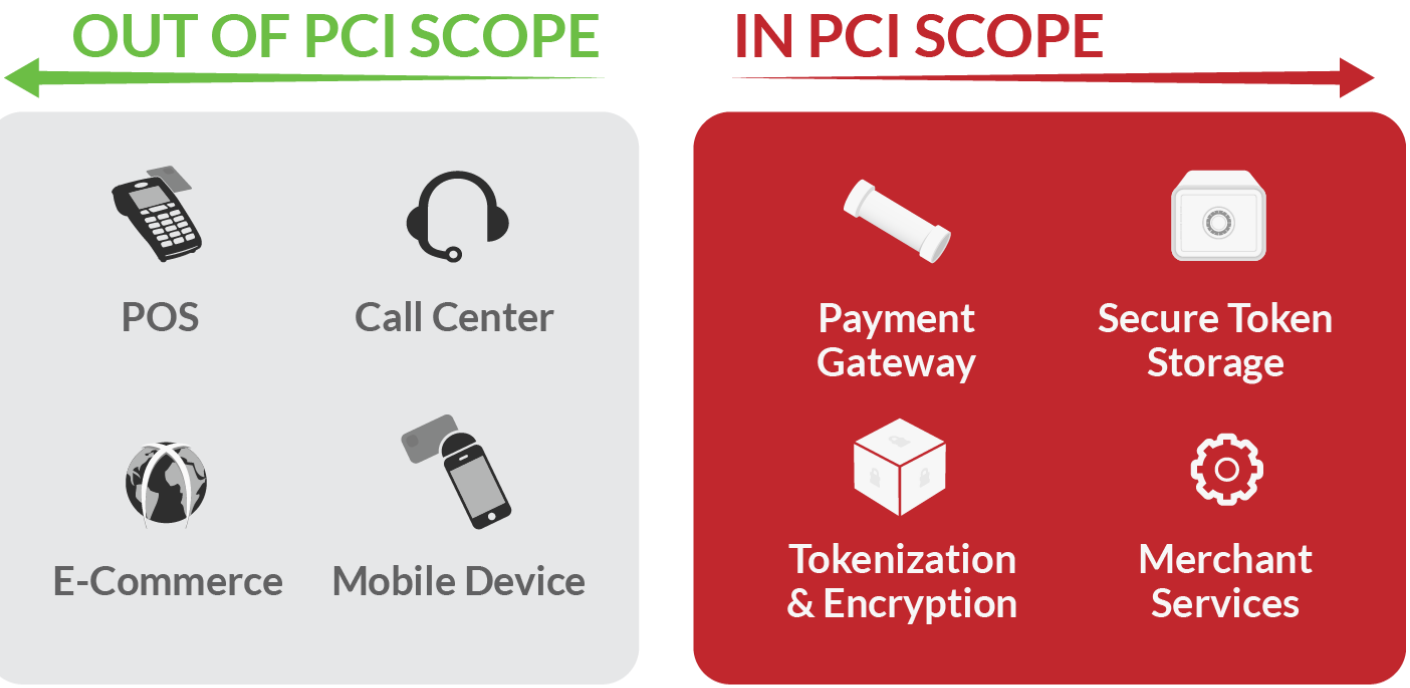
Security: Vaulted Hosting

Step 1: Tokenization

Step 2: Off-site hosting

> Without off-site hosting, **Oracle is still in PCI scope**

PCI Scope Reduction



Before	After
SAQ-D	SAQ-A/B
QSA Costs	Reduced Audit Requirements
2 Full-Time Equivalents	1 Full-Time Equivalent

cardconnect

Impact of PCI 3.0

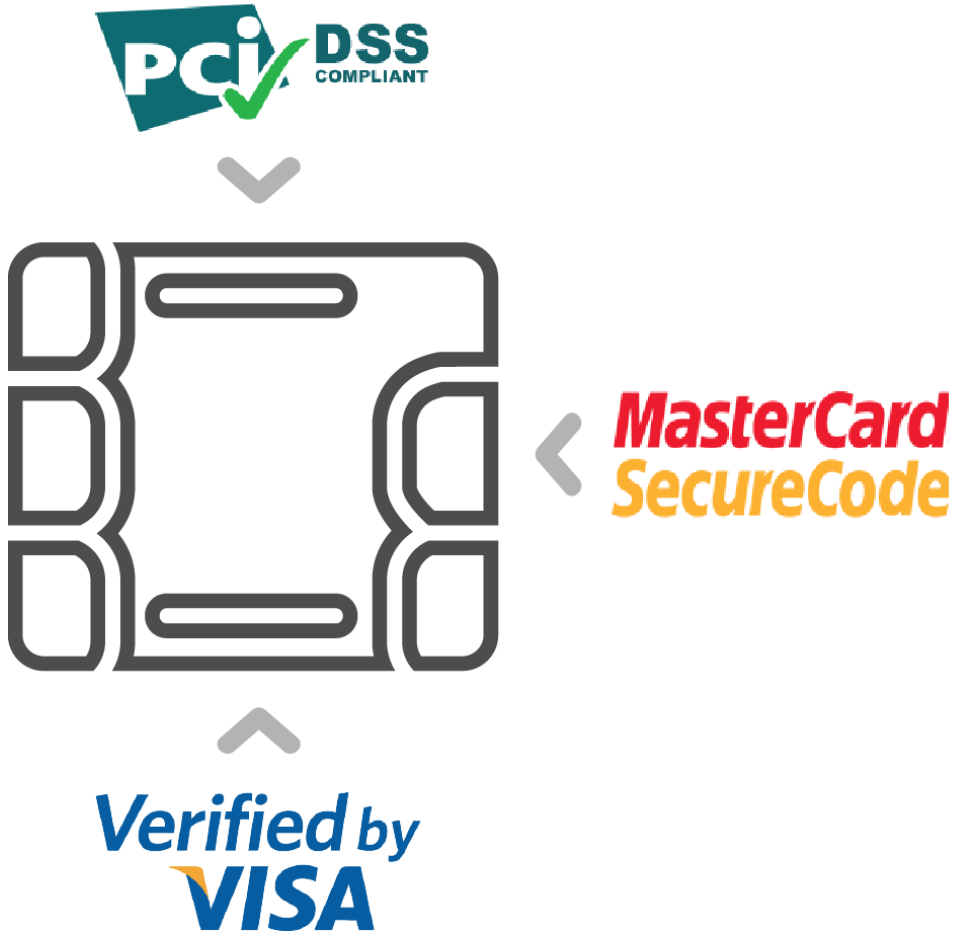
PCI 3.0

> EMV Mandate

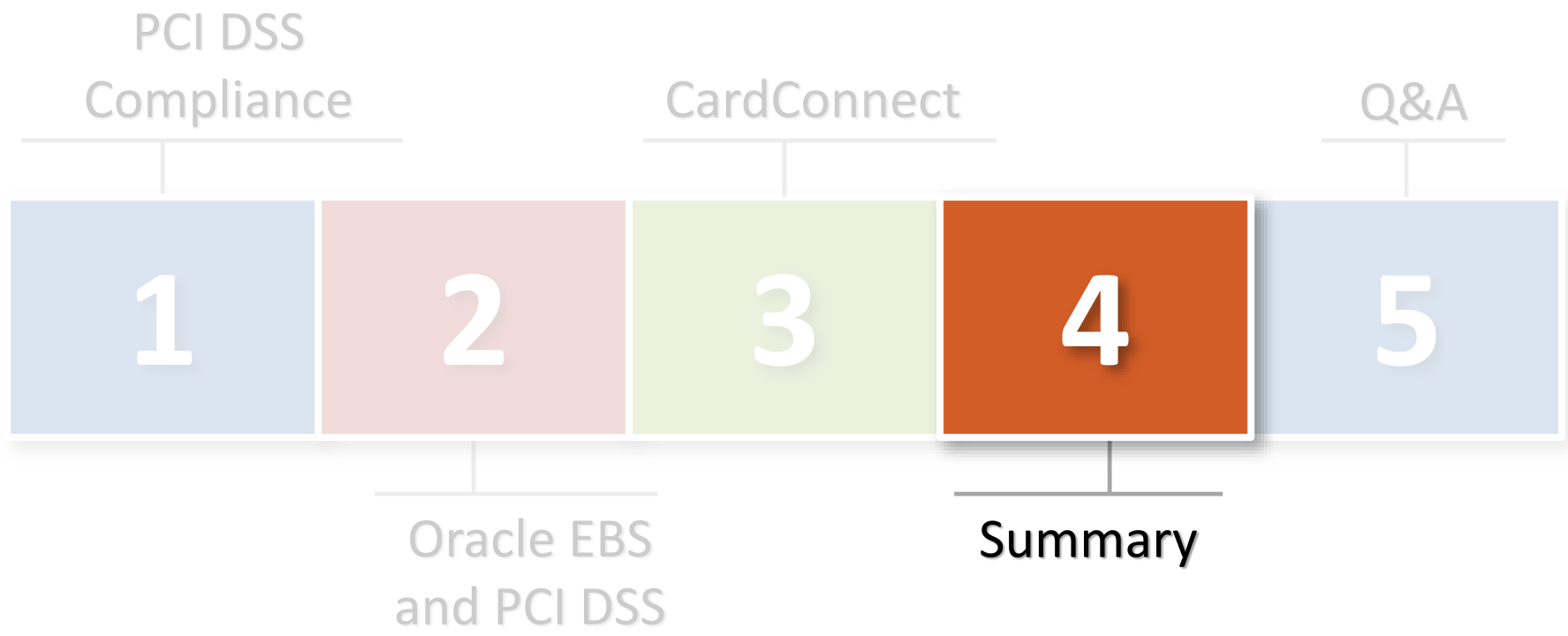
> PCI-certified P2PE

What's Next

> 3-D Secure



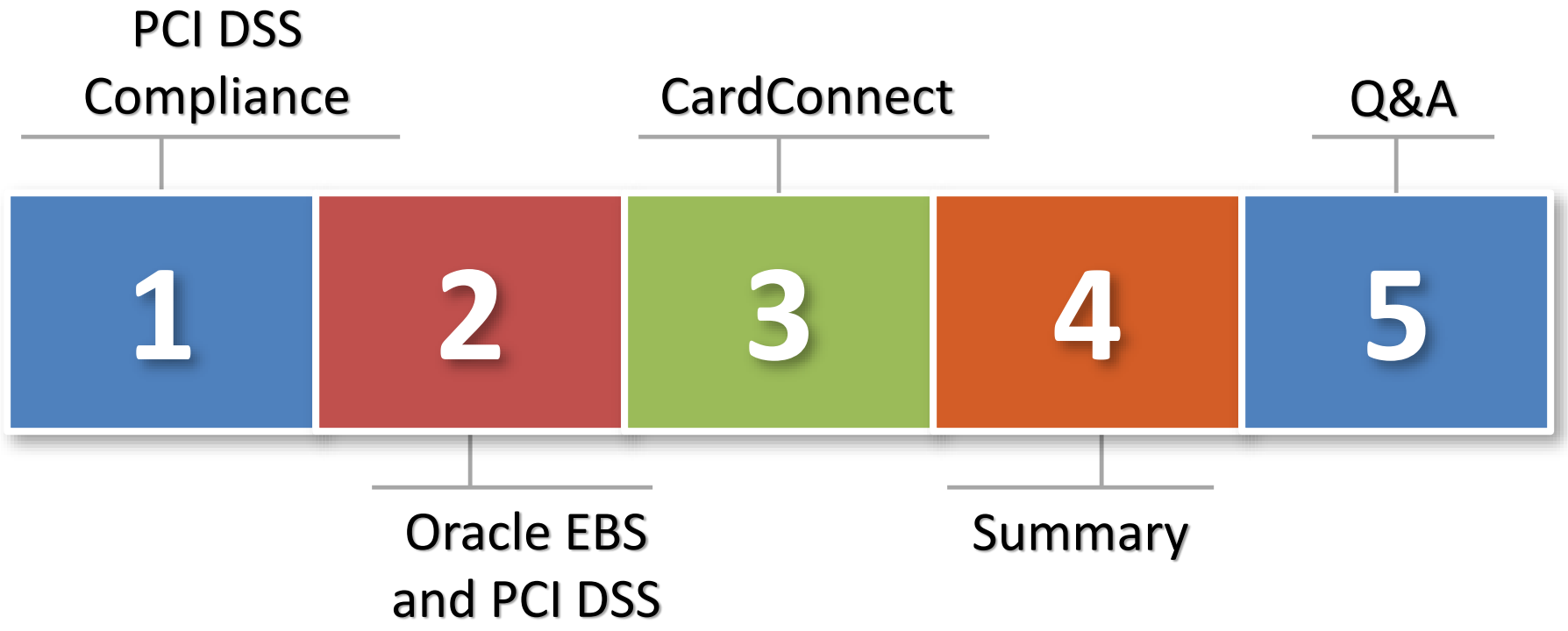
Summary



cardconnect®

INTEGRIGY

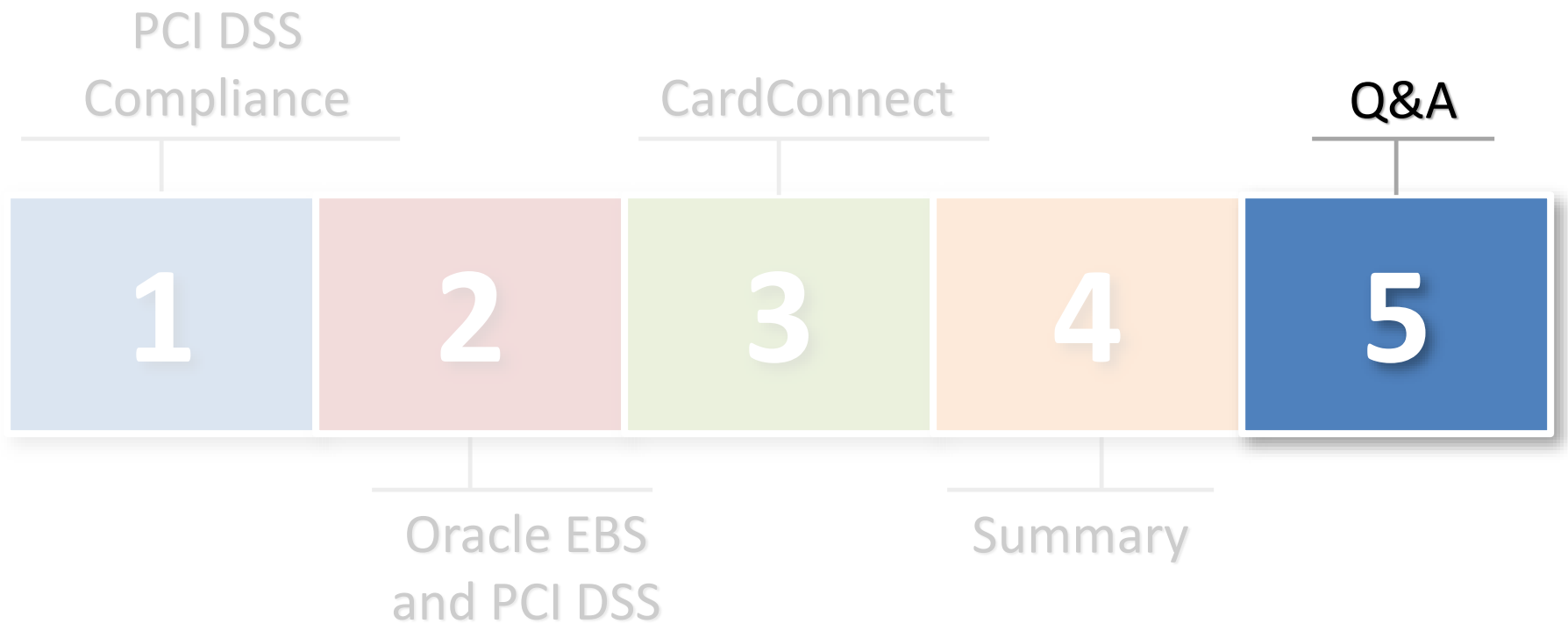
Summary



cardconnect®

INTEGRIGY

Q&A



cardconnect®

INTEGRIGY

For more information

Megan Kelly
Director of ERP Integrations
484-654-9660
mkelly@cardconnect.com

Mike Miller
Chief Security Officer
888-542-4802 x81
info@integrigy.com

cardconnect®

INTEGRIGY