PCI Compliance in Oracle E-Business Suite

April 2, 2014

Mike Miller
Chief Security Officer
Integrigy Corporation

David Kilgallon
Oracle Integration Manager
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.

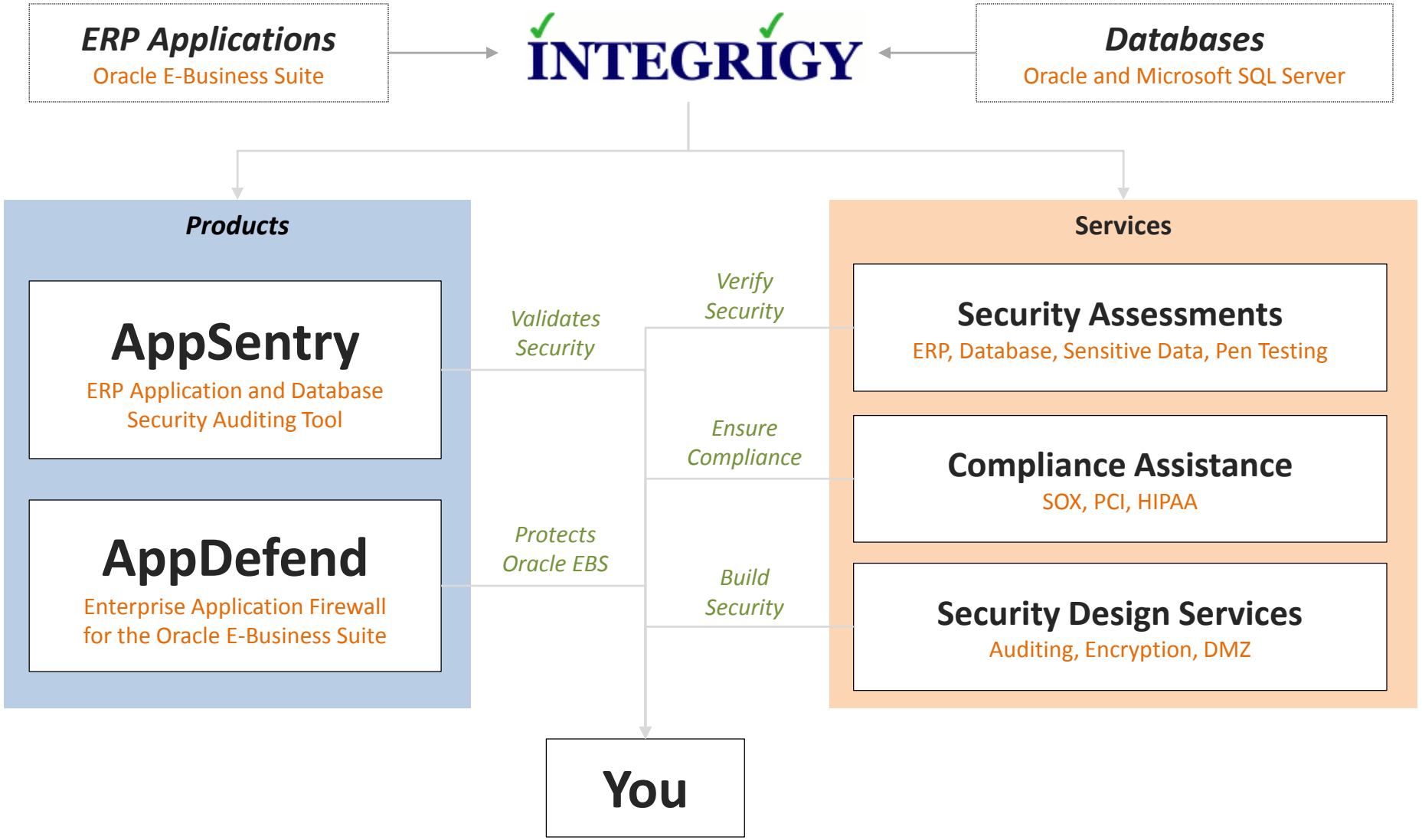
David Kilgallon

David Kilgallon, ISA, PCIP is Director of Integration Services at CardConnect and has 25 years of experience in the IT/Application Development, Deployment, and Support fields. David has worked in positions of leadership at Oracle and Johnson & Johnson and supported numerous Fortune 500 companies.

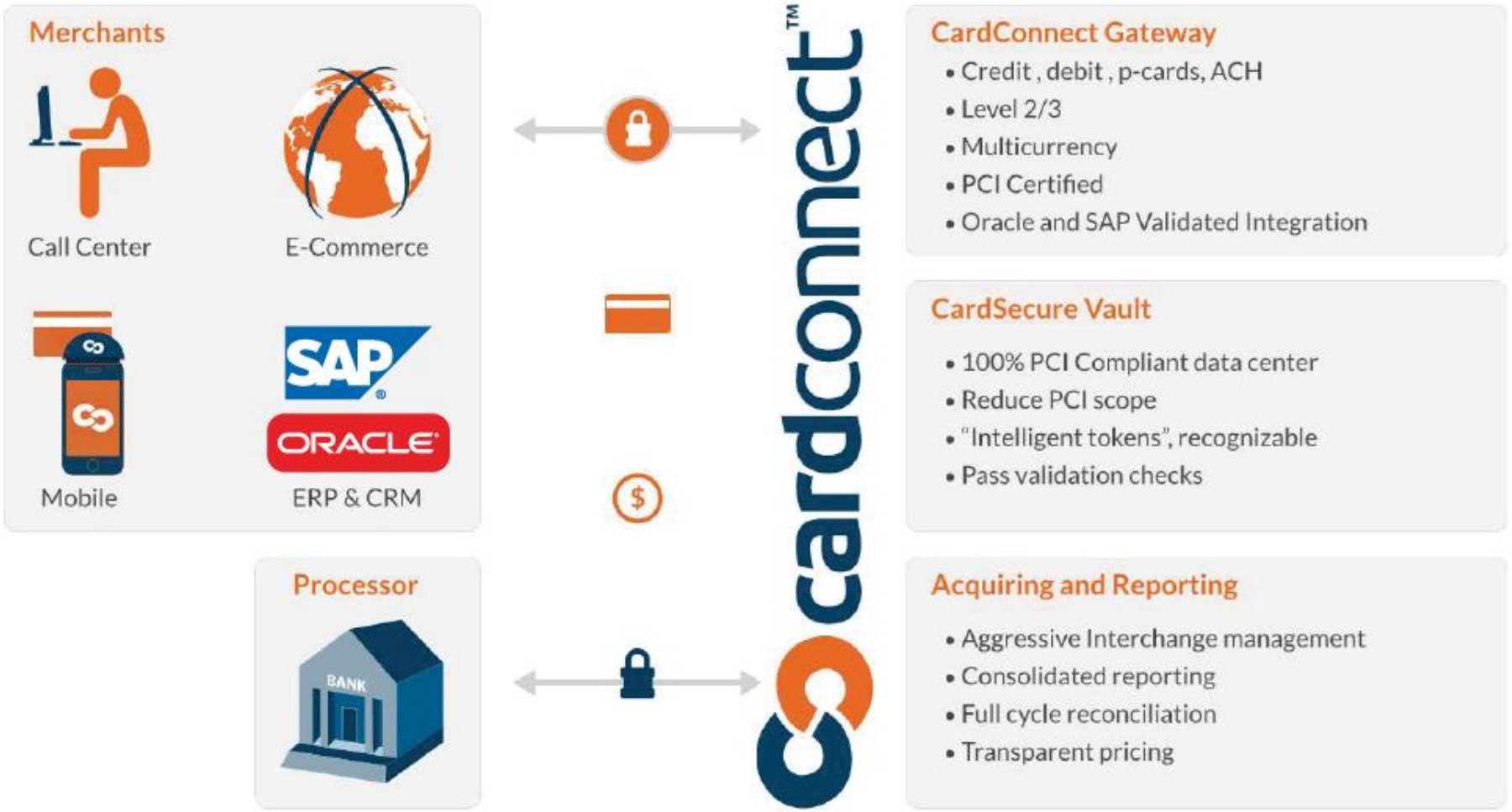
cardconnect™

INTEGRIGY

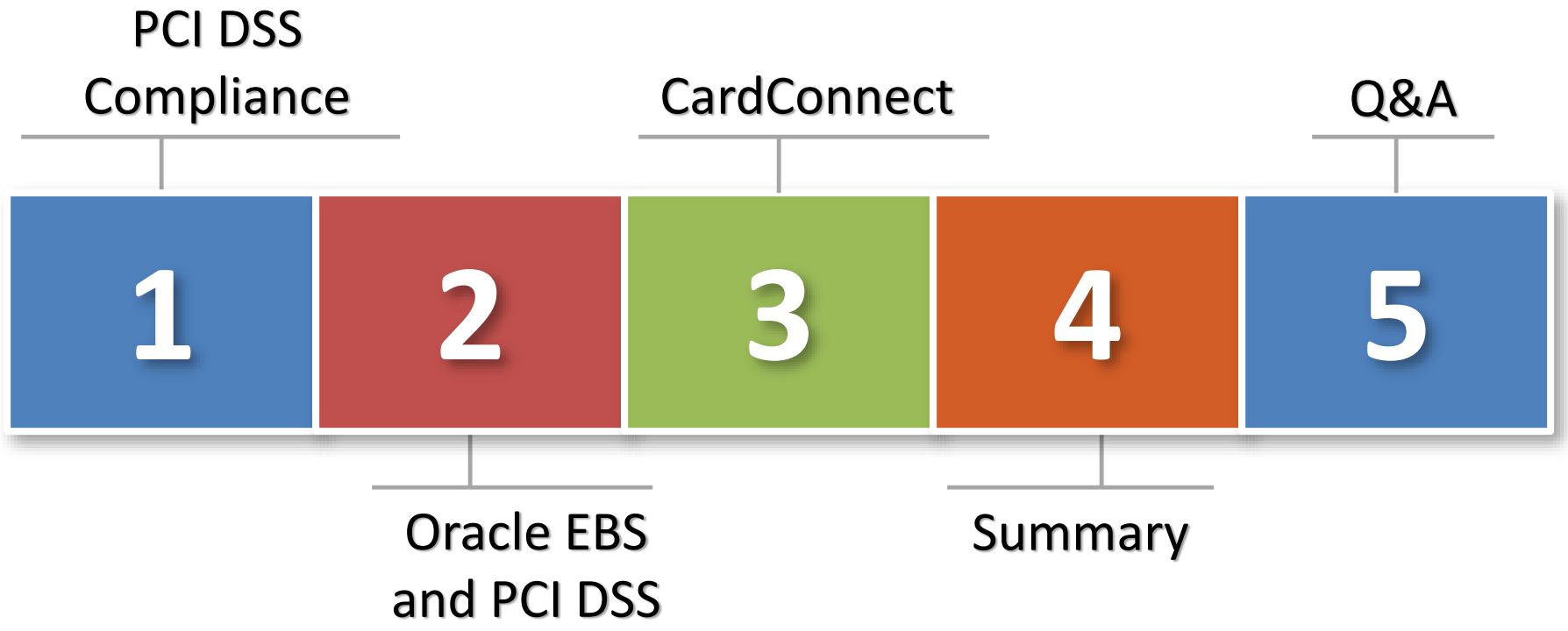
About Integrigy



About CardConnect



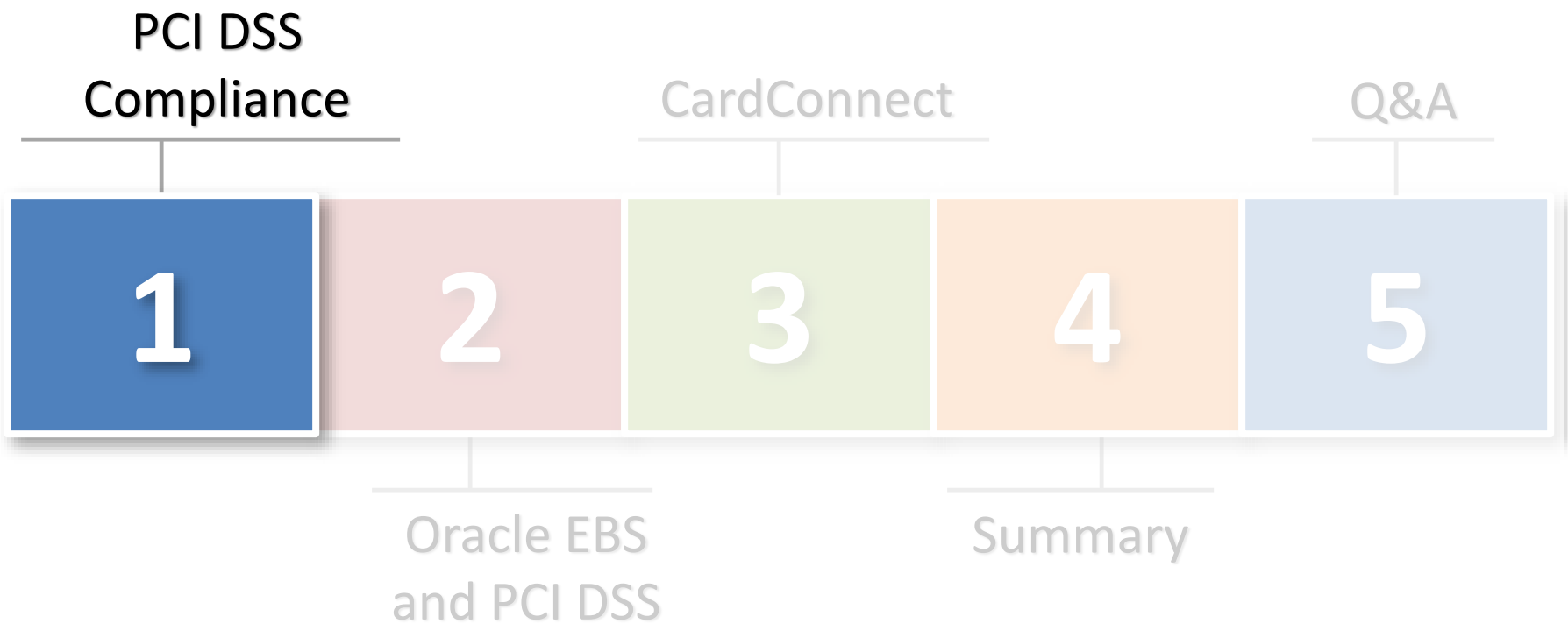
Agenda



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.

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					✓

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

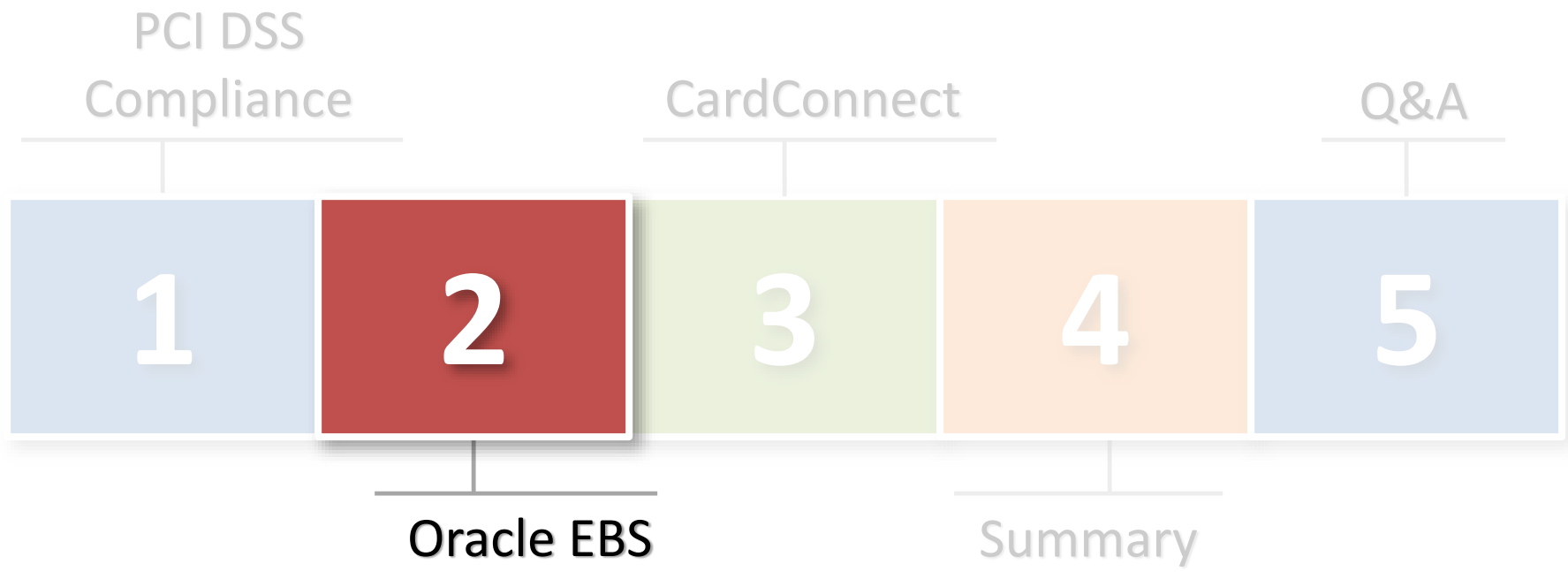
Oracle E-Business Suite and PCI Compliance

- **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

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

Agenda



cardconnect™

INTEGRIGY

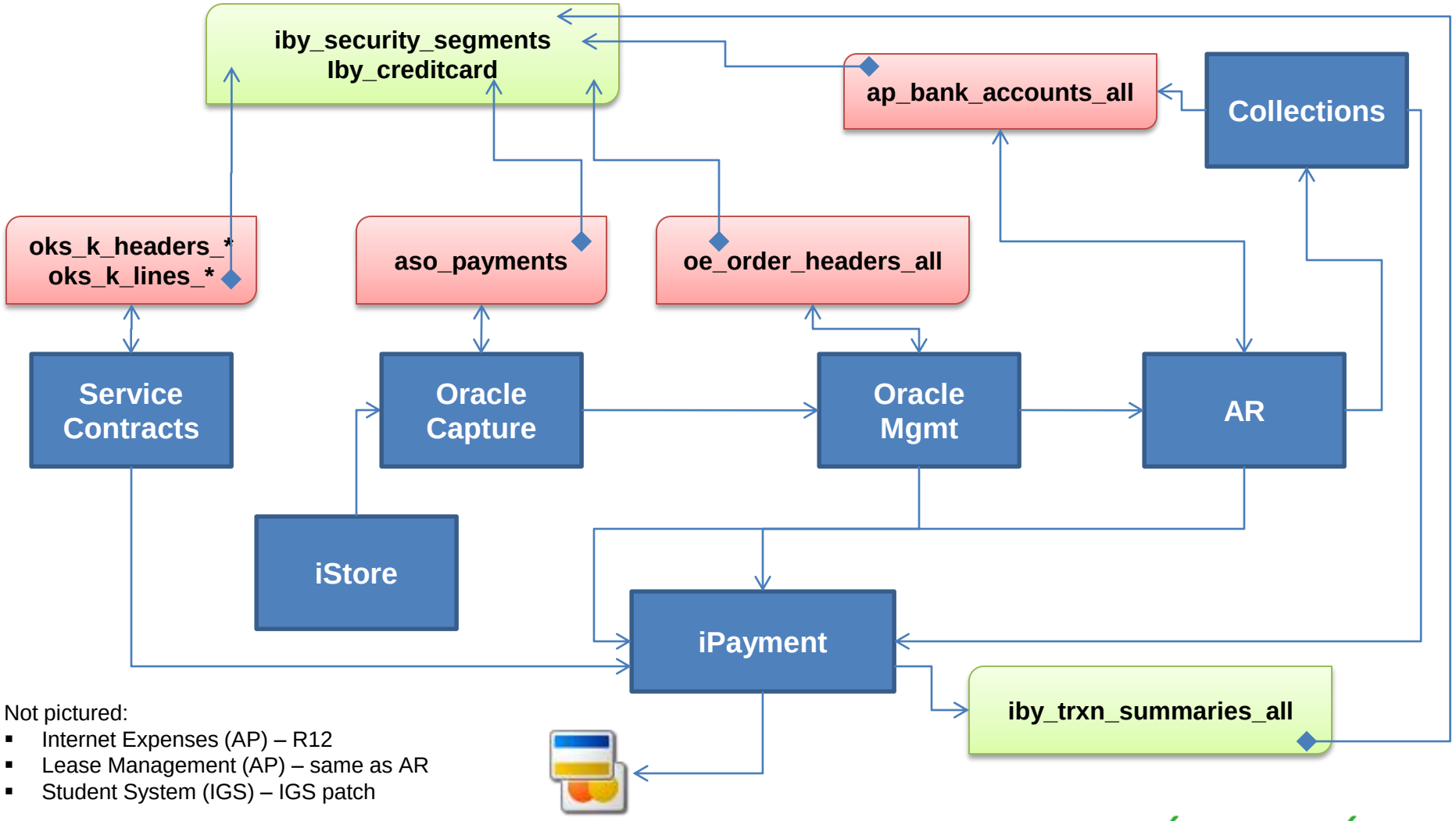
R12 Oracle Payments

- **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	

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

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

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)

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)

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`

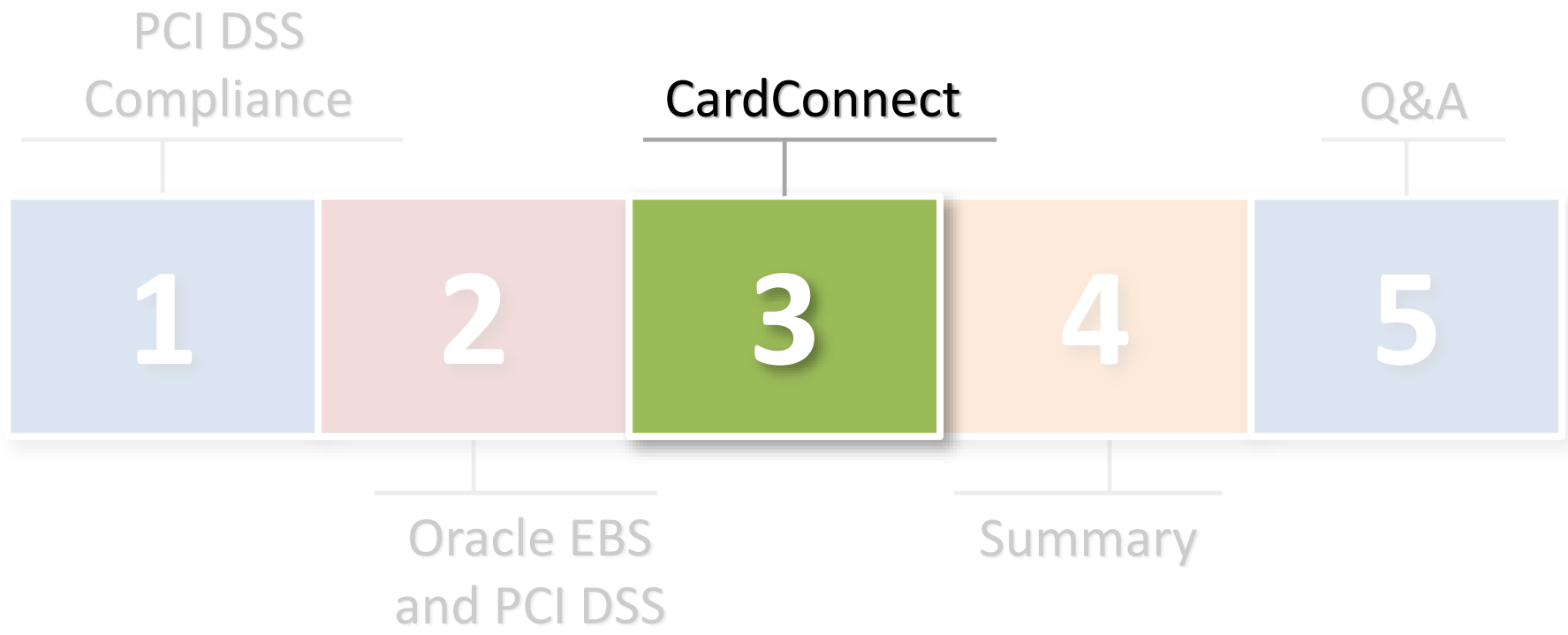
Bank Account Number	`ap_checks_all`
	`ap_invoice_payments_all`
	`ap_selected_invoice_checks_all`

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

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

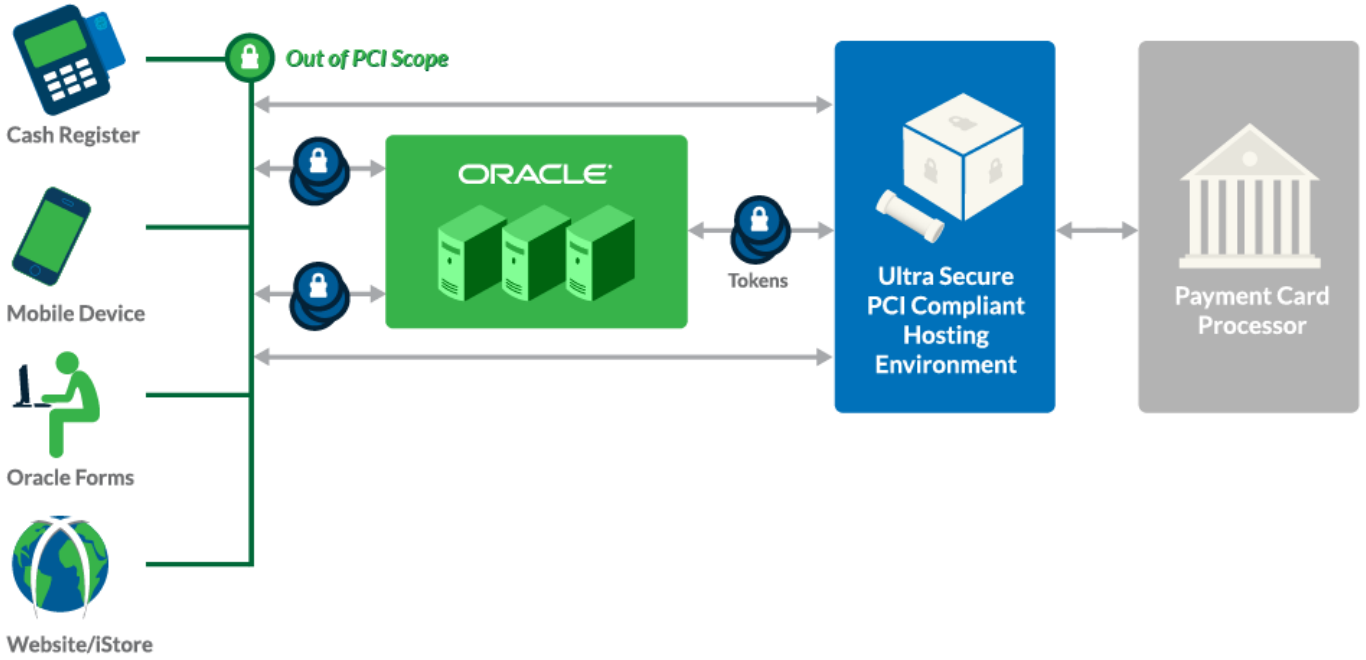
Agenda



cardconnect™

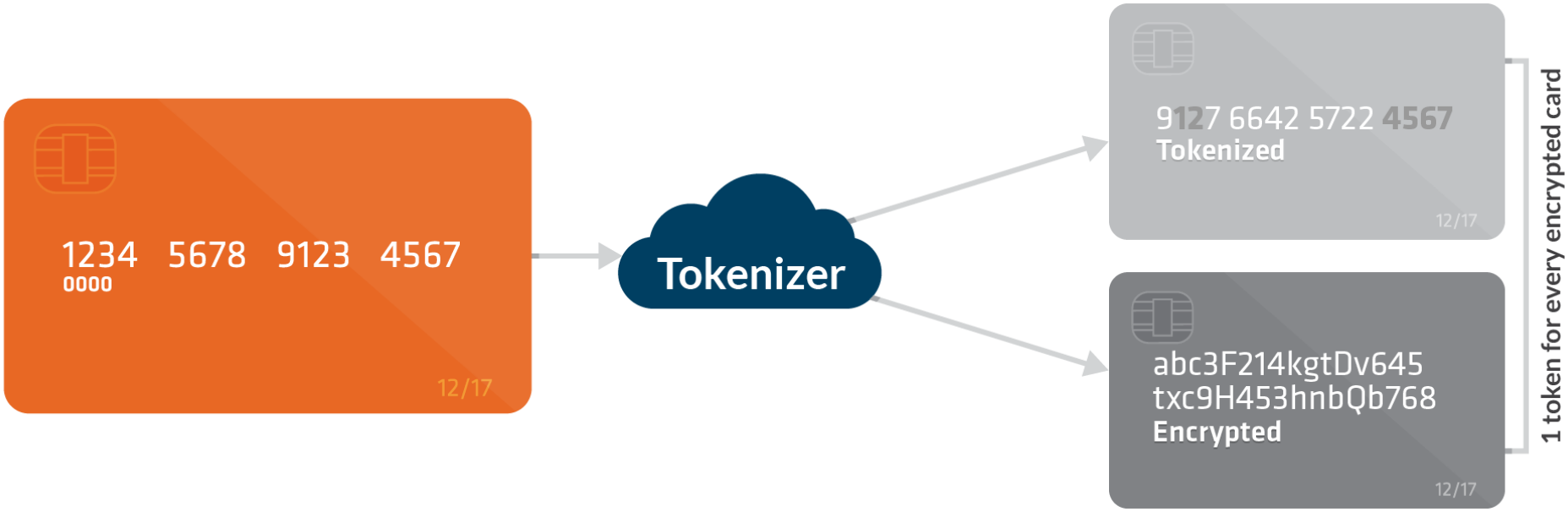
INTEGRIGY

Why Tokenize?



- If scrambling and purging card data makes Oracle EBS PCI compliant, why spend more for tokenization?
- Tokenization removes sensitive payment data from your Oracle EBS entirely – reduces PCI scope and ultimately reduces cost.

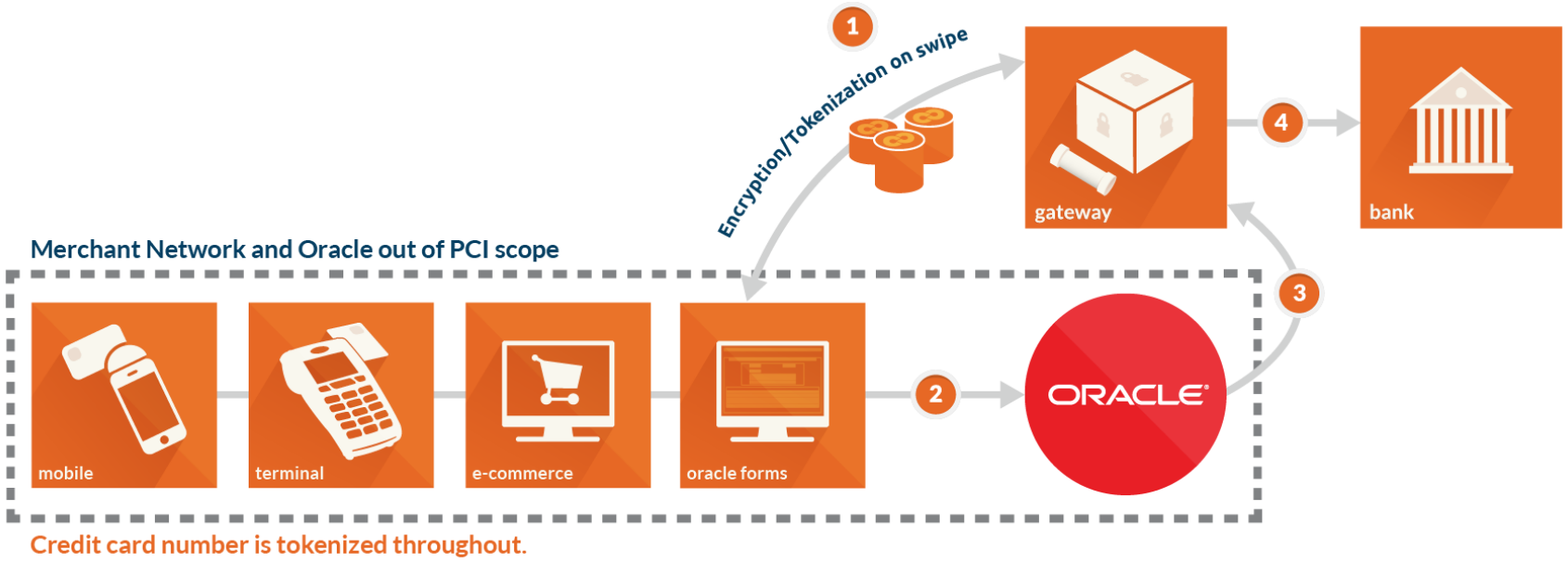
Secure Existing Data



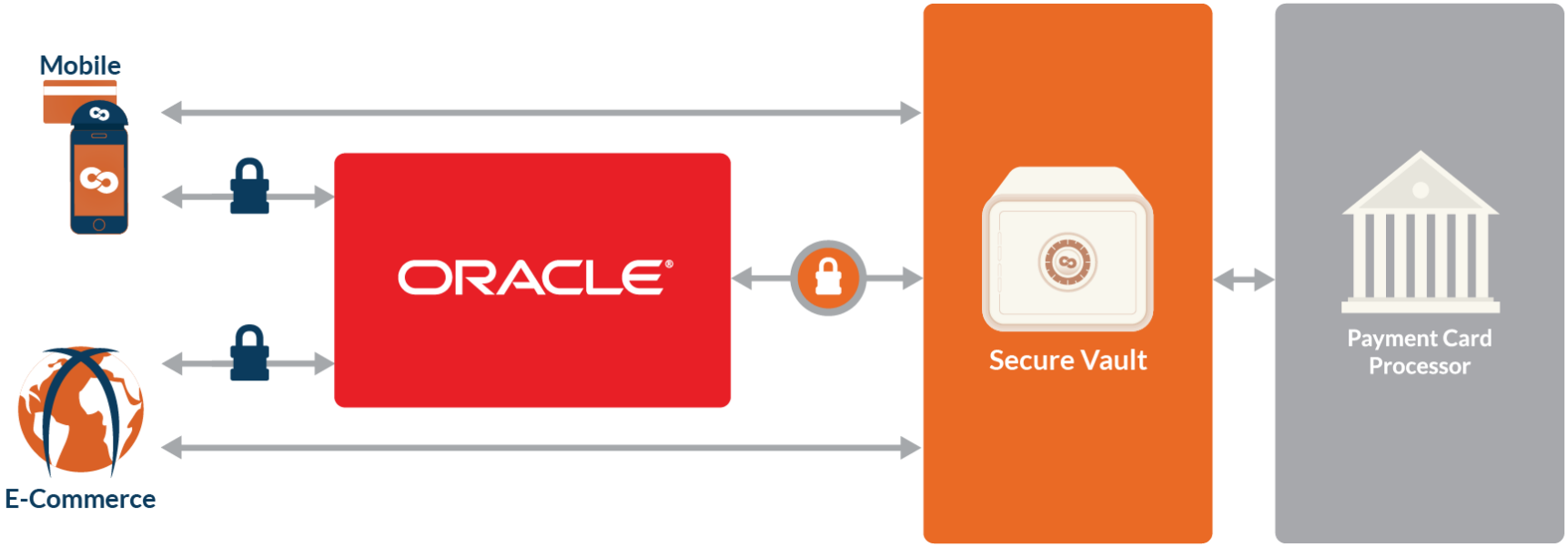
- Remove historical payment card data from Oracle EBS via batch tokenization
- Implement encryption and tokenization for all new transactions

Secure Future Transactions

- Apply to existing sales channels
  - Oracle Forms, iStore, integrations
  - POS, Mobile, e-commerce, and more
- Oracle-to-Gateway integration



Security: Tokenization

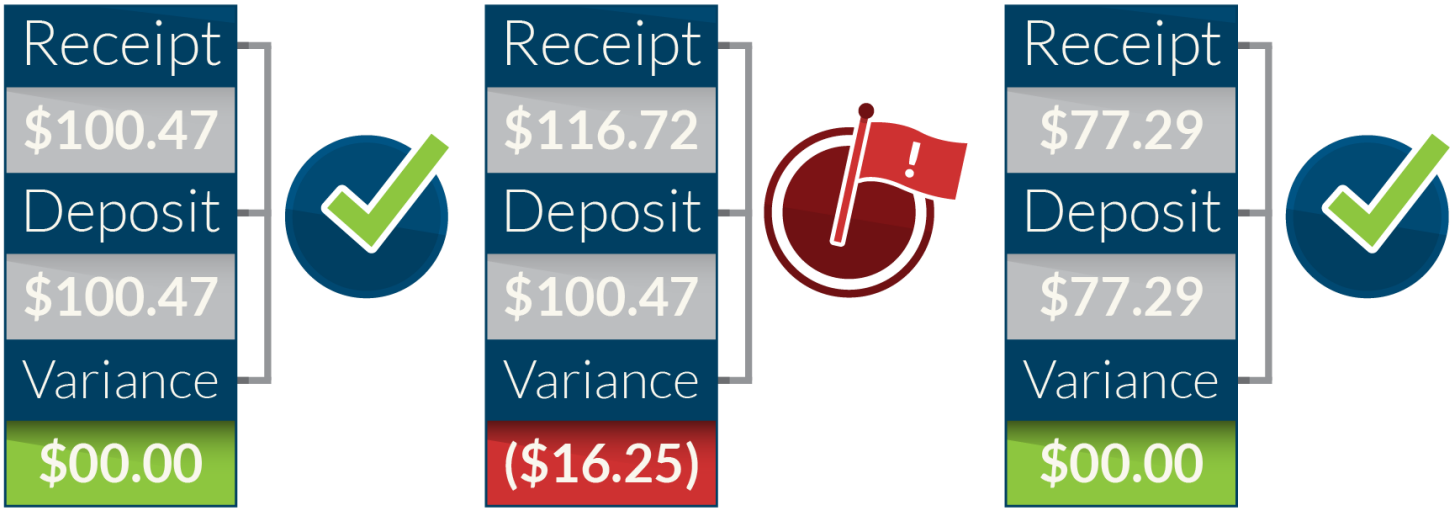


- CardConnect's method of encryption and patented tokenization
  - Irreversible tokens
  - Single-use vs. Multi-use Tokens

Security: Vaulted Hosting

- Hosted off-site payment vault
  - Is it in the *cloud*?
  - Security Requirements

Additional Benefits



- Modifications to Oracle E-Business – **None**
- Enhanced Automatic Reconciliation
  - Settle matched transactions instantly
  - Discrepant transactions are marked with a red flag for review
  - Expedited settlement and automates fee posting

PCI Cost Components

Merchant Level	Initial Scope	Becoming Compliant	Annual PCI Cost
Level 1 Merchant *Over 6 million Visa transactions per year*	$250,000	$550,000-$1,000,000	$250,000
Level 2 Merchant *1M to 6M Visa transactions per year*	$125,000	$260,000-$500,000	$100,000
Level 3 and 4 Merchants *Up to 1M transactions per year*	$50,000	$75,000-$90,000	$35,000

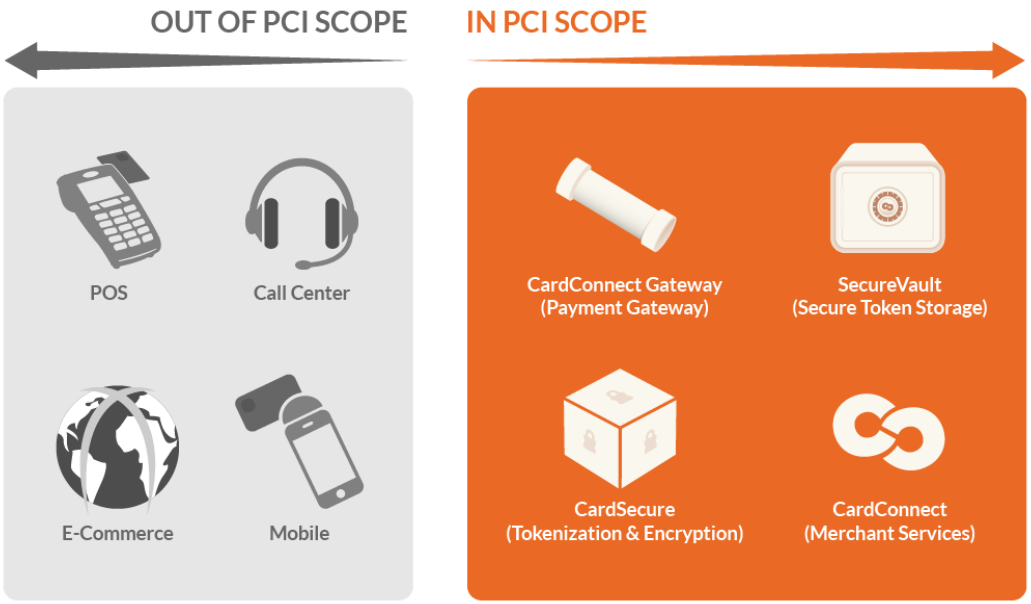
Source: PayPlum, http://www.payplum.com/#!pci-costs/c1ed1

Risks of Non-Compliance

- If a merchant is found to be non-compliant, Visa and MasterCard may fine them up to $25,000 per month
  - **Merchants are liable if a breach occurs and the fines may be huge, even into the millions**
- Costs of a breach are estimated to be $100-$200 per compromised record

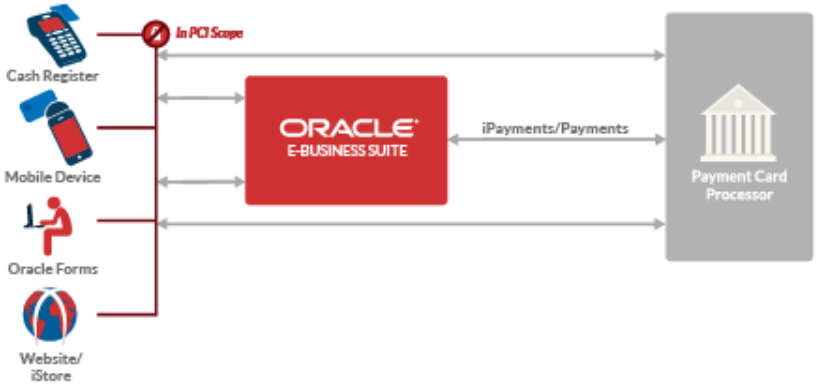
Source: PCI Standard, http://www.pcistandard.com/card-association-fines/; Ponemon Institute: 2013 Cost of Data Breach Study; PCI Compliance Guide, http://www.pcicomplianceguide.org/pcifaqs.php#11

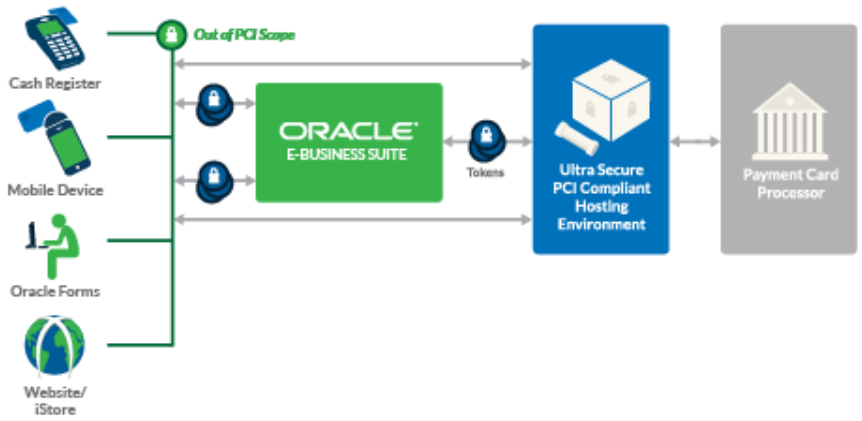
PCI Scope Reduction



Before	After
SAQ-D	SAQ-A/B
QSA Costs - $100,000+	Reduced Audit Requirements - $3,000
2 Full-Time Equivalents	1 Full-Time Equivalent

Standard vs. Integrated





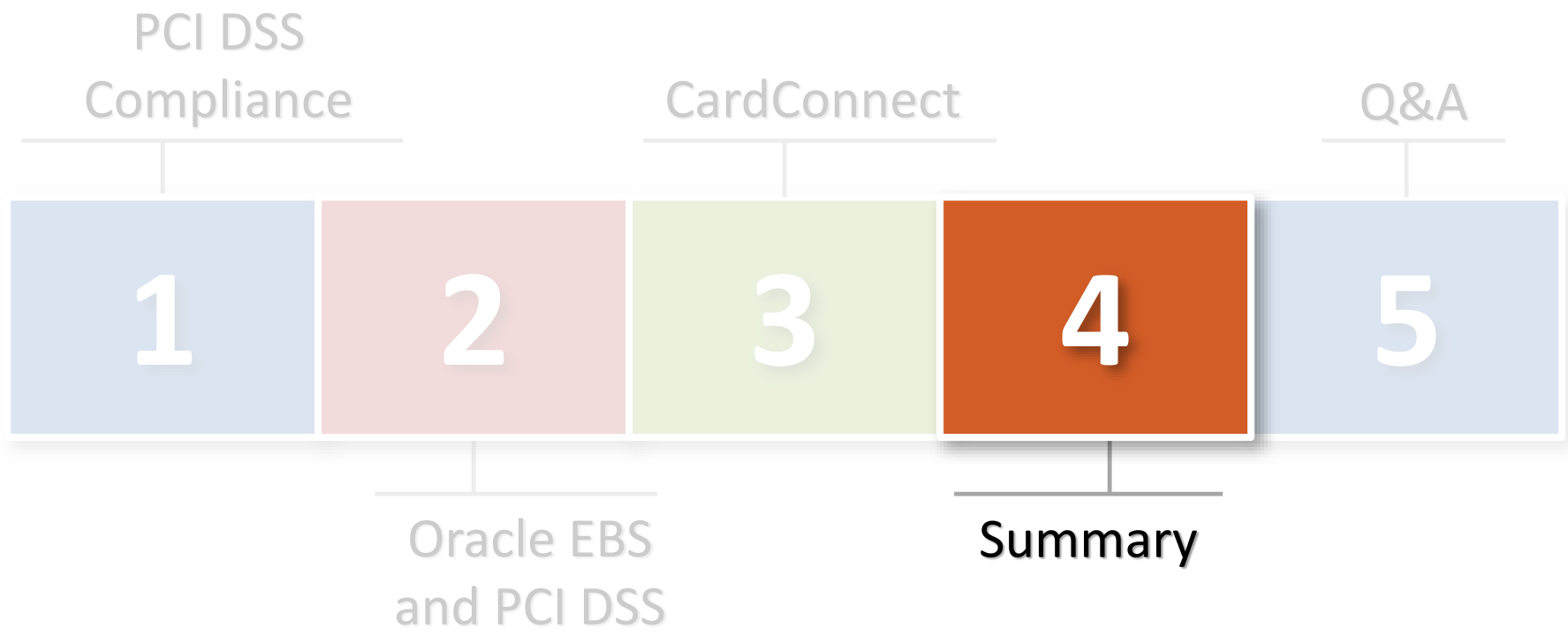
Areas of Concern

- **Card data stored and transmitted within your environment**
  Requires PCI questionnaire D and possibly not compliant
- **Data is only encrypted**
  Encryption greatly reduces risk, but does not guarantee that information is safe from a hack
- **No support for level 2 and 3 payment data**
  Results in higher interchange fees
- **Bank deposit information is not reported into Oracle**
  Creates reconciliation nightmares

Benefits of Integrating Secure Payment Acceptance

- **Greatly reduce compliance efforts**
  Survey decreases from SAQ D to SAQ B for Card-present environments; SAQ D to SAQ A for Card-Not-Present Environments
- **Reduce costs**
  Lower interchange rates and encryption costs
- **Eliminate risk**
  Maintain brand reputation and customer loyalty; mitigate threats of financial penalties and lawsuits
- **Increase efficiency**
  Take advantage of automated bank deposit level reconciliation

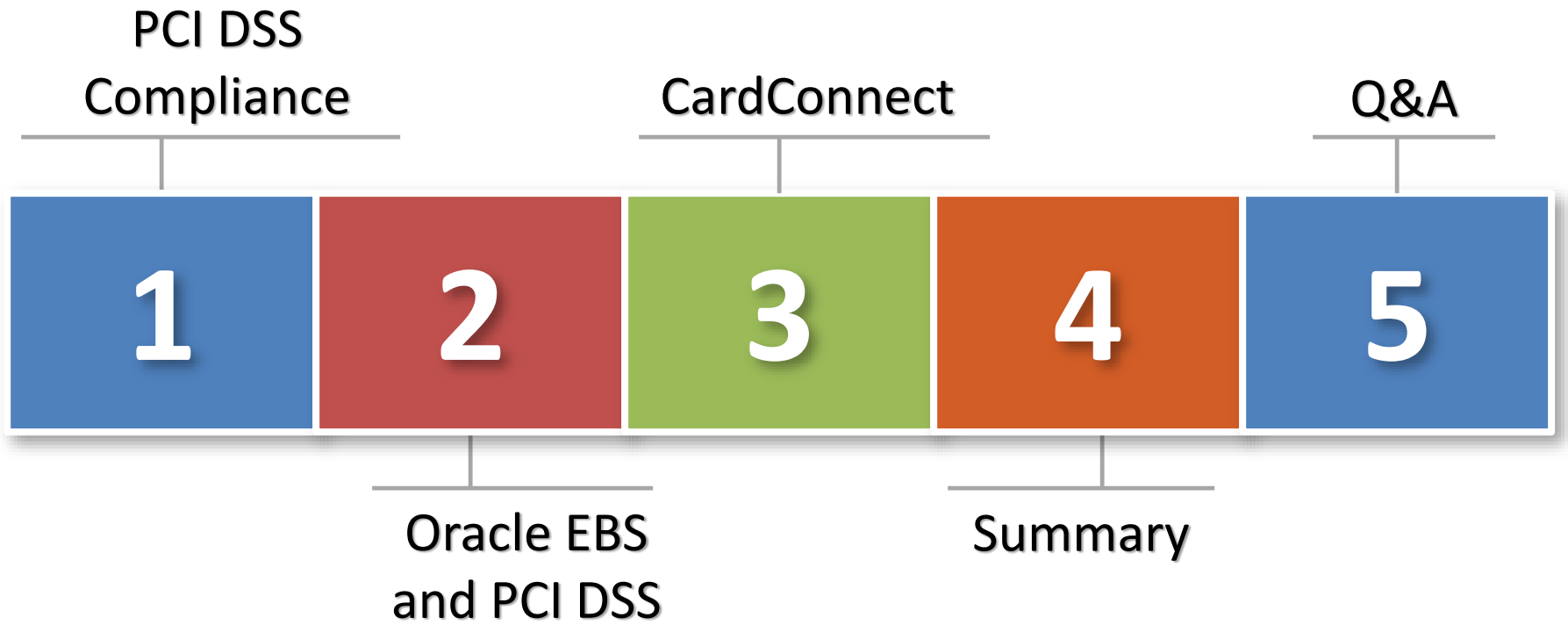
Summary



cardconnect™

INTEGRIGY

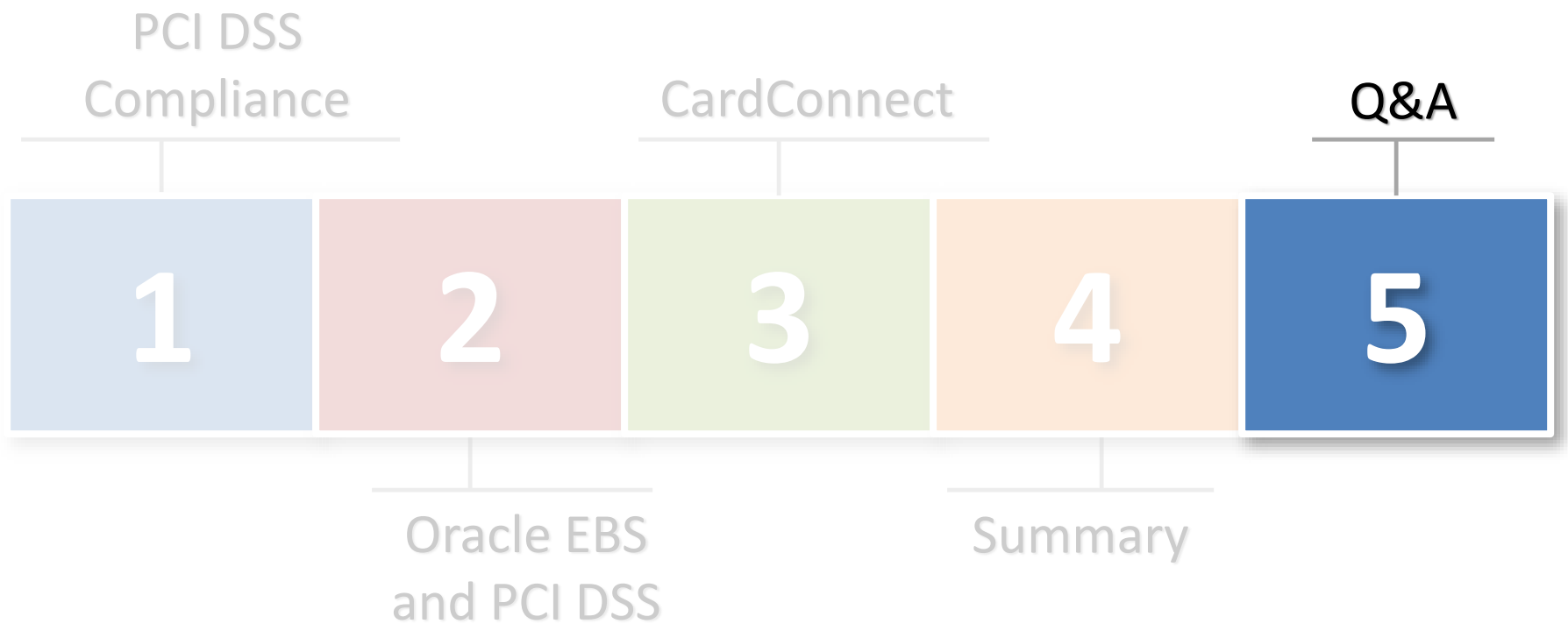
Summary



cardconnect™

INTEGRIGY

Q&A



cardconnect™

INTEGRIGY

Thank you!

Mike Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**

cardconnect™

INTEGRIGY