www.botzandassociates.com
E-mail: botz@botzandassociates.com

BŌTZ
& associates, inc.
solving information security problems

How Can i Do PCI?

Solving Information Security Problems

Agenda

- Objectives
- Context & Overview
- Matching OS function to PCI Requirements

BŌTZ
& associates, inc.
solving information security problems

Objectives

Objectives

- Brief overview of PCI DSS
- Describe which OS provided functions address which PCI requirements
- Identify PCI requirements that need to be Add'l Toolsd to effectively manage
- Identify PCI requirements for which additional tools/products (beyond OS provided function) are suggested or strongly recommended and the reasons why

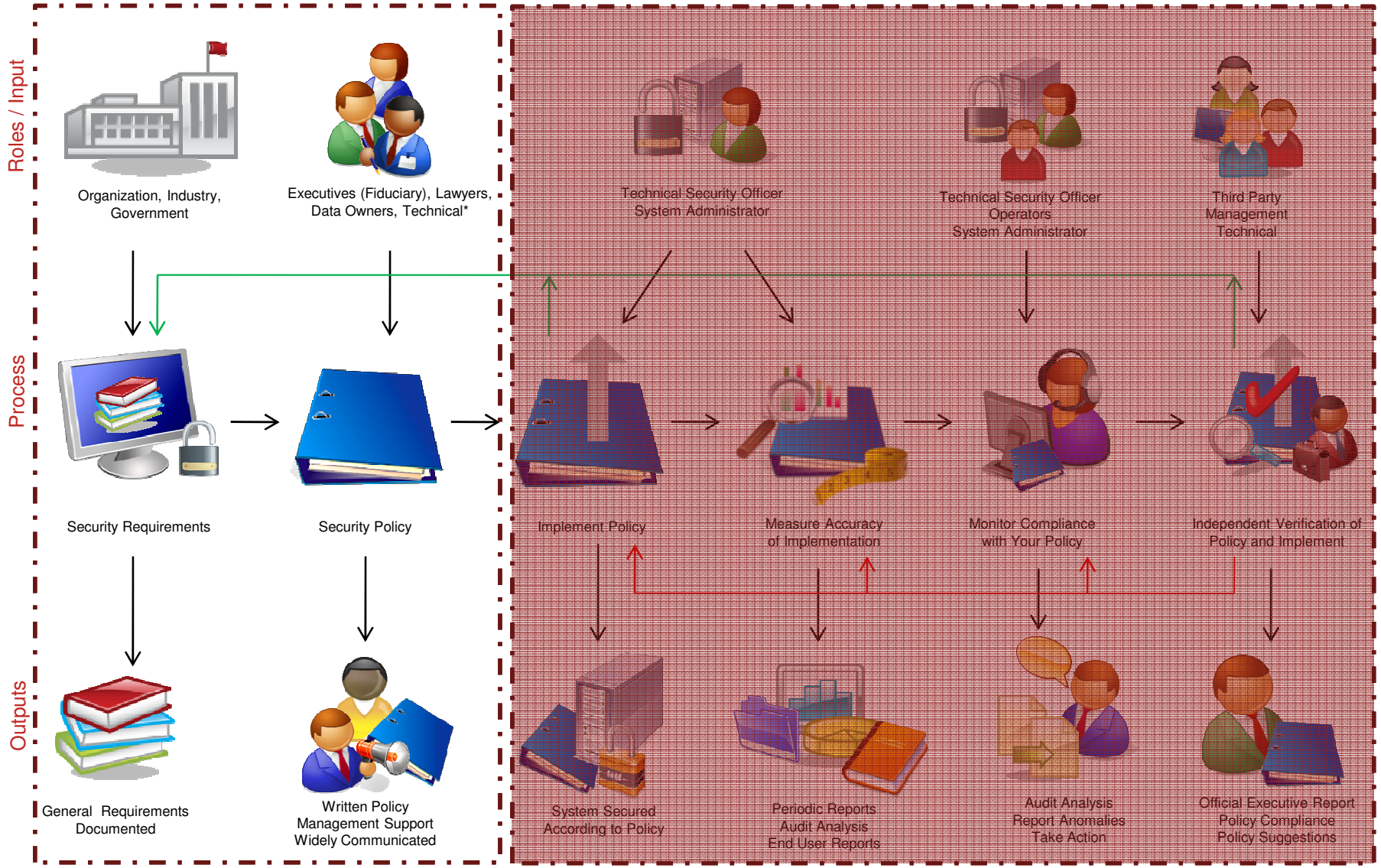
Context & Overview

Context & Overview

PCI DSS

- Payment Card Industry (PCI)
- Data Security Standard (DSS)
- Mixture of **policy** and **procedure**
  - Policy describes required **behavior**
  - Procedure defines how to **enforce** behavior
  - Unlike Sarbanes/Oxley which is entirely policy
- Focus of presentation is on **behavior**

Integrated Enterprise-Wide Security Management Process



BOTZ & associates, inc.
solving information security problems

Policy

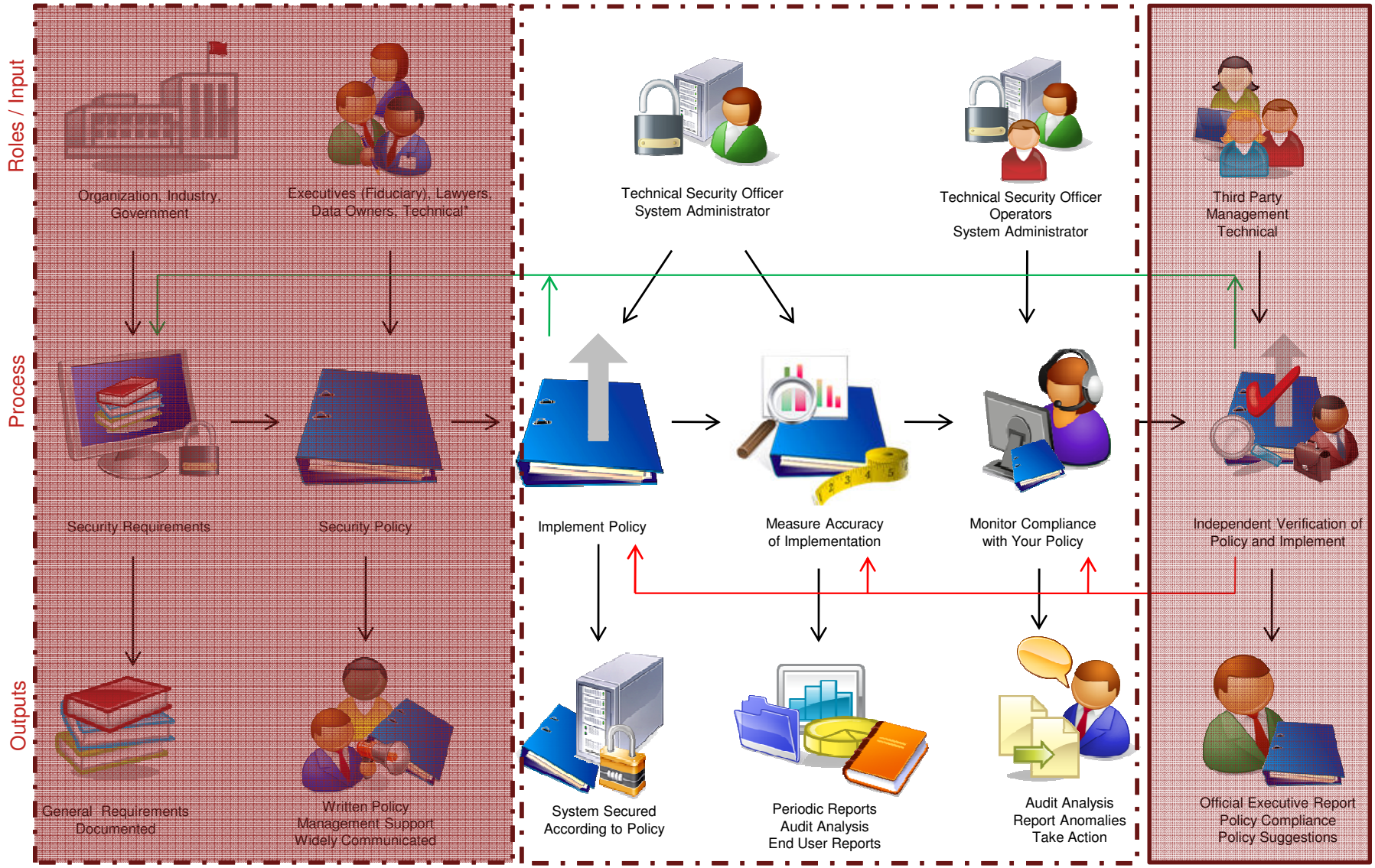
Defining Policy

1. Gather appropriate people from the entire organization

2. Identify and define the organization's security requirement and objectives

3. Translate requirements and objectives into required behaviors

Integrated Enterprise-Wide Security Management Process



BOTZ & associates, inc.
solving information security problems

Defining Procedures

1. Gather the appropriate IT people

2. Translate policies into specific processes and/or technical tools/configuration necessary to:
   - enforce and monitor adherence to,
   - or to detect circumvention of,

   those policies

12 PCI Sections

Section	Article Description
1	Install and maintain a firewall configuration to protect cardholder data
2	Do not use vendor-supplied defaults for system passwords and other security parameters
3	Protect stored cardholder data
4	Encrypt transmission of cardholder data across open, public networks
5	Use and regularly update anti-virus software
6	Develop and maintain secure systems and applications

12 PCI Sections cont...

Section	Section Description
7	Restrict access to cardholder data by business need-to-know
8	Assign a unique ID to each person with computer access
9	Protect stored cardholder data
10	Track and monitor all access to network resources and cardholder data
11	Regularly test security systems and processes
12	Maintain an information security policy

Policy vs. Procedure

- Section heading stated as policy
- Sub-sections of most sections define procedures
- Some sections do not pertain to behaviors enforceable at the OS level
  - These are outside the scope of this presentation
- Some sub-sections outside the scope of this presentation

Reading the tables

Table headings:

- Section
  PCI DSS section or sub-section number

- Description
  Short description of section or sub-section

- In Scope
  Section is or is not within the scope of this presentation
  - ✓ = yes, **N** = no

Reading the tables cont...

Table headings:

- Native OS

  Operating system does/not provide function necessary to meet the requirements of (i.e. comply with) this section or sub-section
  - ✓ = does provide

- Add'l Tools

  Additional tools needed to reasonably implement or manage the implementation of the section or sub-section
  - **Y** = additional tools are recommended to enforce or manage the enforcement of required behavior

Reading the tables cont…

Table headings:

- Prdcts/Srvcs (3rd Party Products or Services)

  Products = ISV/LPP solutions, consulting services, or tools/utilities, typically license plus yearly maintenance, some available on a “software as a service” basis

  Services = Tools/utilities = 3rd-party, no-charge or one-time charge, typically include source code, often provided by consultants

  - ✓ = available
  - **S** = strongly suggested
  - **?** = availability of products unknown, services/consulting is available

OS Function & PCI Requirements

PCI Section 1

Section	Description	In Scope
1	**Install and maintain a firewall configuration to protect cardholder data**	**N**

- Section 1 applies to network traffic control firewalls
- IBM i not typically used as a standalone firewall

PCI Section 2

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✓	✓	Y	✓
2.2	Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts				?
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function)				?
2.2.3	Configure system security parameters to prevent misuse				S
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access				✓

PCI Section 2 cont...

- Additional tools are suggested to automate the on-going enforcement of non-default settings you choose
- Build or Buy
- Look for solutions that:
  1. Automate setting your selected values
  2. Prevent (or immediately reset) changes to your selected settings

PCI Section 3

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
3	**Protect stored cardholder data – the encrypt data at rest provision**	✓	✓	Y	S

- Encryption Easy – Key Management **HARD**
- IBM i provides basic tools to do both
  - Key management support analogous to giving an end user a keyboard to do SQL queries
  - They could do what they needed with the keyboard, but it would be much more efficient (and safe) to give them a canned ODBC program instead
- ISV solution strongly suggested
  - You'll still have some work, but you only have to understand your applications
  - You won't have to become a cryptography expert

BŌTZ & associates, inc.
solving information security problems

PCI Section 4

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
4	**Encrypt transmission of cardholder data across open, public networks**	✓	✓	Y	S

- IBM i provides basic encryption and key management support
- If doing credit card transaction verification, use 3rd party credit card transaction processing
- If transferring data from POS to back-end server, consider VPN, SSH, SSL/TLS
  - Otherwise, find ISV Key management solution

PCI Section 5

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
5	Use and regularly update anti-virus software	✓			
5.1	Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers)		✓	Y	S *

- QSYS (/qsys.lib) file system
  - IBM i provides CHKOBJITG
  - Need a tool to automate the execution of it
- Root file system ("/", other than /qsys.lib)
  - For protecting stream files used with Windows
  - Strongly recommend ISV product/solution

PCI Section 6

Section	Description	In Scope	Native OS	Add'l Tools	Prdcts/Srvcs
6.0	Develop and maintain secure systems and applications	✓			
6.3.2	Separate development/test and production environments		✓		✓
6.3.3	Separation of duties between development/test and production environments		✓	Y	S
6.3.4	Production data (live PANs) are not used for testing or development		✓	Y	S
6.3.5	Removal of test data and accounts before production systems become active		✓	Y	✓
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers		✓	Y	?
6.4	Follow change control procedures for all changes to system components.		✓	Y	S
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks		N	Y	S

PCI Section 6 cont...

- Software management product strongly suggested for most organizations
- Use a different system for development!
  - Using the same system makes it difficult and expensive to meet all the requirements in this section of PCI DSS
  - Virtual system perfectly acceptable
- Consider automating the removal of test accounts, default passwords (i.e. 6.3.6) using CL commands/scripts
- 3rd party solutions/services available for testing Web application security remotely

PCI Section 7

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
7	Restrict access to cardholder data by business need to know	✓	✓	Y	
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access				✓
7.2.3	Default “deny-all” setting				S

PCI Section 7 cont…

- Default deny all
  - Makes it easier and cheaper to meet most other PCI DSS requirements!
  - Services available to make it very cheap and easy for most customers to change default allow systems to default deny!
    - Tools and utilities make this easier to implement
- Recommend solutions that maintain enforcement of access control settings once set correctly

BŌTZ
& associates, inc.
solving information security problems

PCI Section 8

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
8	Assign a unique ID to each person with computer access	✓	✓		✓
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: Password or passphrase; Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)				
8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.				
8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography				

PCI Section 8 cont…

- ISV/LPP solutions available for userID management
- Sections 8.2/8.3 Biometric authentication available for IBM i
  - **Transparency**: Speaker also employed by biometric solution provider
- Section 8.4 handled by OS for system user profiles
  - Application level passwords cannot be stored in stream files or databases w/o hashing or encrypting them
  - Typically hashing (avoids key mgmt issues) is all that is needed

PCI Section 8 cont...

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	✓	✓	Y	✓
8.5.2	Verify user identity before performing password resets.				
8.5.3	Set first-time passwords to a unique value for each user and change immediately after the first use.				
8.5.4	Immediately revoke access for any terminated users				
8.5.5	Remove/disable inactive user accounts at least every 90 days				
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed				

BŌTZ
& associates, inc.
solving information security problems

PCI Section 8 cont…

- ISV user management solutions available

PCI Section 8 cont...

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
8.5.7	Communicate password procedures and policies to all users who have access to cardholder data	✓	✓		✓
8.5.8	Do not use group, shared, or generic accounts and passwords	✓	✓		✓
8.5.9	Change user passwords at least every 90 days	✓	✓		
8.5.10	Require a minimum password length of at least seven characters	✓	✓		
8.5.11	Use passwords containing both numeric and alphabetic characters	✓	✓		
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used	✓	✓		

PCI Section 8 cont...

- Section 8.5.9 thru 8.5.12
  - Standard password composition rules
  - IBM i provides necessary flexibility for enforcing requirements
- Consider solutions or utilities that prevent changing these rules on production systems except under tight management control
- Password change management products and utilities available

PCI Section 9

Section	Description	In Scope
9	Restrict physical access to cardholder data	N

PCI Section 10

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
10	Track and monitor all access to network resources and cardholder data	✓	✓	Y	S

- System auditing provides all capability necessary to **CAPTURE** required data
- Strongly recommend tools or solutions that automate the **ANALYSIS** of the data

PCI Section 11

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
11	Regularly test security systems and processes	✓		Y	S
11.3.2	Application-layer penetration Tests				
11.5	Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly				

- Automate as much as possible
  - Build or buy

BŌTZ
& associates, inc.
solving information security problems

PCI Section 12

Section	Description	In Scope	Native OS	Add'l Tools	Prdct/Srvcs
12	Maintain an information security policy	✓		Y	✓
12.1.1	Addresses all PCI DSS requirements				
12.1.2	Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment				
12.1.3	Includes a review at least once a year and updates when the environment changes				
12.2	Develop daily operational security procedures that are consistent with requirements in this specification				
12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach				

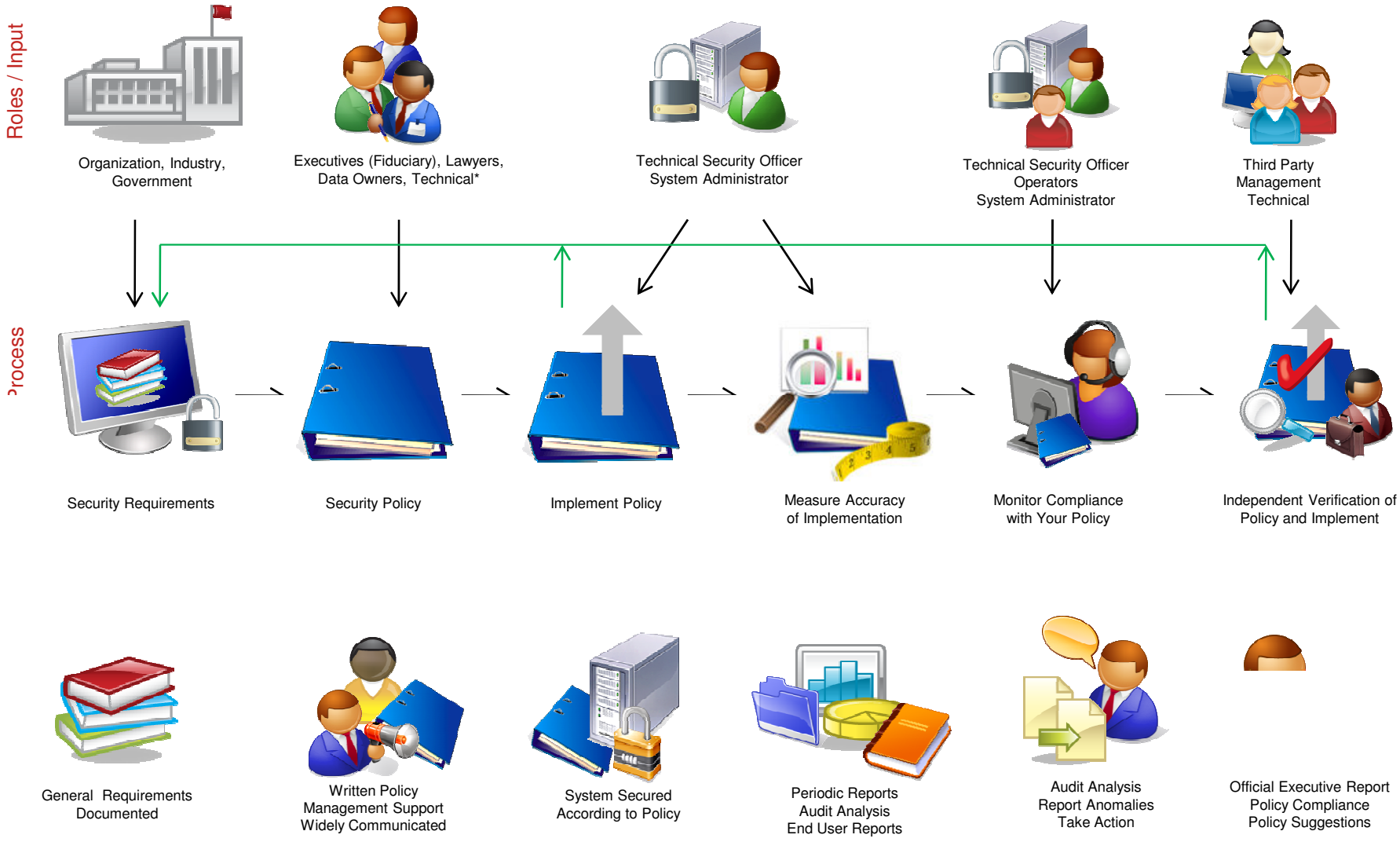
PCI Section 12 cont…

- Most of this section describes required behavior (i.e. policy)
  - e.g. “annual process”, “daily operational procedures”, “incidence response plan”
- IBM’s Secure Perspective LPP helps you define, manage, and **IMPLEMENT** security policy
- Other products available to define and manage security police

BŌTZ
& associates, inc.
solving information security problems

Summary

Integrated Enterprise-Wide Security Management Process



BOTZ & associates, inc.
solving information security problems

More Information

- https://www.pcisecuritystandards.org/
- https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf
- https://www.pcisecuritystandards.org/security_standards/supporting_documents.shtml
- Download the PCI DSS specification at : https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

THANK YOU!

BŌTZ
& associates, inc.
solving information security problems

P.O. Box 7498
Rochester, MN 55903

Telephone: (507) 319-5206

www.botzandassociates.com

ABOUT Botz & Associates, Inc.

We specialize in helping customers understand and execute the business AND technical aspects of the security management process.

BŌTZ
& associates, inc.
solving information security problems

ABOUT THE SPEAKER

Patrick Botz is the founder and president of Botz & Associates, Inc.

Prior to starting Botz & Associates, Pat served as the Lead Security Architect and Team Leader for the IBM, working on some of the most widely used midrange servers is the business world with a focus on authentication, authorization, auditing, and ease of use. Following his work primary focus on helping customers meet various industry regulations such as SOX, PCI DSS, and SAS 70. He additionally worked to help customers improve the effectiveness and efficiency of their current security management processes, assisting them with moving to exclusionary access control models, eliminating passwords in various environments, managing User IDs, implementing encryption, and auditing on various platforms.

Pat is co-author of the book /Expert's Guide to OS/400 and i5/OS Security/, and has published numerous articles in the trade press and IBM magazines. He is also a noted worldwide security conference speaker, presenting at various conferences and in webcasts including COMMON, IBM Technical Conference, various user groups, St. Cloud State University Security conference, and IBM Business Partner conferences.

BŌTZ
& associates, inc.
solving information security problems

P.O. Box 7498 ▪ Rochester, MN 55903 ▪ Telephone: (507) 319-5206 ▪ www.botzandassociates.com

Trademark & Disclosure Statements

The following terms and marks are trademarks of Botz & Associates, Inc.:

security = f (cost, risk) is a trademark of Group8 Security, Inc.
Other company, brand and product names are trademarks or registered trademarks of their respective holders.

Information is provided “AS IS” without warranty of any kind. All examples described are presented as illustrations of how customers have used BAI recommendations, products or services and are the results they may have achieved. Actual results may vary by customer. Information concerning non-BAI products or services was obtained from a supplier of these products, published announcement materials, or other publicly available sources and does not constitute an endorsement of such products by BAI.

BŌTZ
& associates, inc.
solving information security problems

P.O. Box 7498 · Rochester, MN 55903 · Telephone: (507) 319-5206 · www.botzandassociates.com