TIBCO™

Application Security Use Case:

PCI Compliance

Jaime D’Anna
Sr Dir of Product Strategy, TIBCO Software

LogLogic | AGENDA

- PCI Overview
- App Security in Context
- Essential Steps to Compliance
- Q & A

- What is PCI?
  - Consists 6 Categories with 12 Requirements designed to protect card holder data
  - Each Requirement Contains Multiple Sub-Components.
  - Compliance may be audited by a Qualified Security Assessor (QSA) or by Self-Assessment Questionnaire (SAQ)

- Who does it apply to?
  - Any organization that conducts business via payment cards

LogLogic | Application Security in the PCI Context

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	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
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

LogLogic | Essential Steps to PCI Compliance

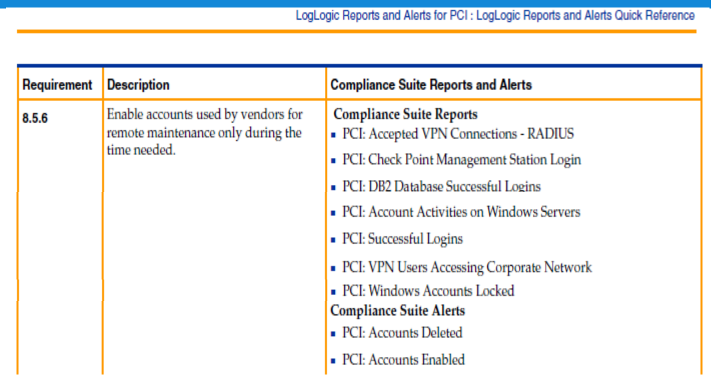
10 Essential Steps for a Successful Compliance program

- Understand the requirements
- Understand the IT controls that affect your business
- Define the compliance processes and success criteria
- Identify all in-scope IT components
- Collect fine-grain user and system activities
- Store all logs centrally for the required time period
- Implement regular tasks
- Implement and verify continuous monitoring
- Demonstrate compliance status to auditors
- Substantiate reports and alerts

7 out of 10 steps at some point will either involve a report or alert derived from Log Activity
Followed by an Auditor asking to validate the process

LogLogic | Log Management – The Critical Path to PCI Compliance

- **TIBCO Loglogic Compliance Manager & PCI Suite**
  - Consists of 371 Reports, 137 Alerts and a Guide book mapping each to a specific Sub-Requirement
- **Matching Reports and Alerts to the PCI Requirements**
- ***Requirement 8: Assign a unique ID to each person with computer access***
  - **PCI DSS Requirement. - 8.5.6** – Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.
- **Testing Procedures**
  - **8.5.6.a** - Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.
  - **8.5.6.b** - Verify that vendor remote access accounts are monitored while being used.



LogLogic Reports and Alerts for PCI : LogLogic Reports and Alerts Quick Reference

Requirement	Description	Compliance Suite Reports and Alerts
8.5.6	Enable accounts used by vendors for remote maintenance only during the time needed.	**Compliance Suite Reports** ▪ PCI: Accepted VPN Connections - RADIUS ▪ PCI: Check Point Management Station Login ▪ PCI: DB2 Database Successful Logins ▪ PCI: Account Activities on Windows Servers ▪ PCI: Successful Logins ▪ PCI: VPN Users Accessing Corporate Network ▪ PCI: Windows Accounts Locked **Compliance Suite Alerts** ▪ PCI: Accounts Deleted ▪ PCI: Accounts Enabled

LogLogic | The Value of LogLogic Compliance Manager

Strategic

Compliance without Complexity

Monitor enterprise activity and manage risk, as well as, manage and review network policies according to mandates and regulation..

Strengthen Policy Lifecycle

Manage the complete lifecycle of internal/external policies and their exceptions, develop workflow stages that model your organizations processes, and automatically notify users when their tasks require action.

Operational

Flexibility and Scalability

Establish repeatable processes for compliance management. Create reviewer processes, SLAs, assign reviewers and define reporting schedules with pre-packaged alerts and reports.

Automate Policy Management

Establish Automated workflows and IT data management processes for responding to alerts and reviewing reports concerning internal business policies or industry mandates.

TIBCO

LogLogic | Customer Case Study: US Retailer >$1BN

Requirements

- Ensure compliance is met with all data is in a single data store for reporting and forensics
- Infrastructure Simplicity
  - Single image rollout to POS
  - Centrally Managed and Supported
- Isolated PCI Solution
  - Centralized "PCI Only" Logging
  - Centralized PCI Reporting
- Hardware Appliance Solution
  - Single Vendor Solution
  - Separate "PCI Only" Appliance
  - Separate "Non-PCI" Appliance
- Flexible Log Collection
  - Scriptable Deployment
  - Support for Remote Collection

TIBCO LogLogic Solution

- Enterprise-Grade Appliances
- Universal Collector for all log files/types
- PCI Templates based on best-practices
- WW Support

Tangible Results

- Saved One FTE
- Consistently Pass Audits
- PCI Compliant for
  - 1,100 Retail Stores
  - 1,100 Routers
  - 3 Firewalls
  - 5 Domain Controllers
  - 2 AIX Application Servers

LogLogic | Resources to Get you started

➡ www.tibco.com/loglogic

- Demos
- Whitepapers
- Datasheets
- Testimonials

➡ **Join us at the RSA Show Feb 2014 in San Francisco, CA**

LogLogic | Questions?

Thank you!

Jaime D’Anna
jdanna@tibco.com
www.tibco.com/loglogic