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
<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a <a href="#">firewall</a> configuration to protect cardholder data</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>2. Do not use vendor-supplied defaults for system <a href="#">passwords</a> and other security parameters</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td></td>
<td>5. Use and regularly update anti-virus software on all systems commonly affected by malware</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td></td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td></td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>

© Copyright 2000-2014 TIBCO Software Inc.
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
• **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.
Compliance without Complexity
Monitor enterprise activity and manage risk, as well as, manage and review network policies according to mandates and regulation.

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.

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.

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.
Requirements

- Ensure compliance is met with all data 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

© Copyright 2000-2014 TIBCO Software Inc.
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
Thank you!

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