Developing Compliant Patterns for Modern Technologies

Stephen Podobinski
Lead Information Security Analyst
Target
Goal & Take-Aways

• Understand the process
  – 6 steps
  – Appreciate its repeatability

• Take-Aways
  – Support – Partners & Leaders
  – Scope – Know the controls to be addressed
  – Adoption – An important, often overlooked step
You Can Do It!

- ANY enterprise or organization can implement modern technologies
  - Things to keep in mind:
    - Understand business drivers
    - Understand resources available
    - Drive scoping discussion
What’s driving this desire?

• Typically, entities want to reduce licensing costs
• Other potential drivers:
  – Using open source technologies
  – More control over the environment
  – Be awesome
The Repeatable Process ·

• NOT a linear, waterfall-like progression
PostgreSQL: SOX-Compliant Pattern

• First enterprise effort
  – Organizational challenge
  – Partnerships were new
  – Identity and Access Management
## Communication Tool – Nice Example

### Status Summary:
- Day 22 of 23 (ending 11/15): completed 1 day early!
- SOX Documentation deemed complete with appropriate evidence

### Follow-up Items:
- I've agreed to send communication and set up a meeting with the in-scope applications' key contacts, along with SOX and BISO partners, to discuss the compliant pattern and stress timely onboarding
  - Met MVP for CS-1557122 – Configuration Scanning – Security and Vulnerability Management
    - SVM team conducting analysis on Tenable/Postgres-scripts ability to meet configuration-scanning control requirements
    - Scripted SCIM scan results, sent to SVM for validation, will suffice in the interim (estimated to be through end of year, 2018)
  - Met MVP for CS-1557150 – System Activity Logging – Future improvements (estimated completion by 12/31) include:
    - Additional screenshoot of the 'postgres' user ID filter in T-Falcon upon development
    - Storage and automated monitoring of the logs integrated with CFC functionality—dependent upon .json efforts completed by Data Store team and ArcSight team onboarding

### Challenges:
- There may be resistance from the product teams regarding developer access to production

### Additional Links:
- Detailed Compliance Requirements Tracker
- Challenge Chartering
- CFC Requirements
- Applications Needing to be Onboarded 2018

### Control Standard (SOX Specific) | Technically Complete | Application Validation | Compliance Acceptance
---|---|---|---
CS-1557076 – Access Provisioning | Complete | Complete | Complete
CS-1557079 – Access Reviews | Complete | Complete | Complete
CS-1557077 – Change in or Termination Role/Responsibilities | Complete | Complete | Complete
CS-1557122 – Configuration Scanning | Complete | Complete | Complete
CS-1557160 – Data Backup and Storage Requirements | Complete | Complete | Complete
CS-1557074 – Identity and Access Management Configuration | Complete | Complete | Complete
CS-1557075 – Least Privileged Access Control | Complete | Complete | Complete
CS-1557119 – Monitoring and Resolving Processing Errors | Complete | Complete | Complete
CS-1557150 – System Activity Logging | Complete | Complete | Complete
Cassandra: SOX-Compliant Pattern

• Technically difficult
  – Instaclustr, scaling issues, Ecaudit, Gatek
  – Backups? Completeness and accuracy of the data
  – Hardened offering – part of a broader SOX compliant pattern
## Communication Tool – Hurdle Example

### Status Summary:
- Technical pattern AD integration is complete
- Database activity logs integrated with the T-Falcon tool; database activity monitoring (DAM) complete
- Continued challenge regarding need for database backups given the unique database distributed design

### Next Steps:
- FIN team committed to proving out the pattern once technical hurdles have been cleared—their partnership is secured
- Continued discussions regarding Data Backup and Processing Error requirements continue based on increasing knowledge of the architecture
- SOX team integration is integral to our efforts and will continue throughout
- Team to work automated deployment pipeline in GHE

### Challenges:
- Continued challenge given Cassandra's use case is to NOT be source of truth
  - Challenge database backup requirements given technology's use case
  - Challenge monitoring and resolving processing errors given technology's use case
  - Need help understanding proper constituencies to agree on a way to move forward
- Timeline is a significant issue given the represented need to have a compliant pattern by end of April

### Additional Links:
- Privileged Access Design Document
  - [https://confluence.target.com/display/FIT/Maker+Transfer+-+Design](https://confluence.target.com/display/FIT/Maker+Transfer+-+Design) – Architecture diagram we're working with the FIN team to understand

### Exhibit Standard (SOX Specific)

<table>
<thead>
<tr>
<th>Exhibit Standard (SOX Specific)</th>
<th>Technical Completeness</th>
<th>Valuation</th>
<th>Compliance</th>
<th>Acceptance</th>
<th>Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-3557076 – Access Provisioning</td>
<td>Complete</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Completed work on LDAP integration</td>
<td></td>
</tr>
<tr>
<td>CS-3557078 – Access Reviews</td>
<td>Complete</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Completed work on LDAP integration</td>
<td></td>
</tr>
<tr>
<td>CS-3557077 – Change in or Termination Role/Responsibilities</td>
<td>Complete</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Completed work on LDAP integration</td>
<td></td>
</tr>
<tr>
<td>CS-3557122 – Configuration Scanning</td>
<td>In Progress</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Target India working the SCML baseline</td>
<td></td>
</tr>
<tr>
<td>CS-3557160 – Data Backup and Storage Requirements</td>
<td>Blocked</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Technical and Compliance teams are at an impasse</td>
<td></td>
</tr>
<tr>
<td>CS-3557074 – Identity and Access Management Configuration</td>
<td>Complete</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Completed work on LDAP integration</td>
<td></td>
</tr>
<tr>
<td>CS-3557075 – Least Privileged Access Control</td>
<td>Complete</td>
<td>Not Started</td>
<td>In Progress</td>
<td>PAAD is completed and reviewed; review by SOX team needed</td>
<td></td>
</tr>
<tr>
<td>CS-3557119 – Monitoring and Resolving Processing Errors</td>
<td>Blocked</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Technical and Compliance teams are at an impasse</td>
<td></td>
</tr>
<tr>
<td>CS-3557139 – System Activity Logging</td>
<td>In Progress</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Completed integration with T-Falcon→Kafka→Kibana pattern for logging</td>
<td></td>
</tr>
<tr>
<td>Automated Schema Change Pipeline</td>
<td>In Progress</td>
<td>Not Started</td>
<td>Not Started</td>
<td>Team working on automating via GHE</td>
<td></td>
</tr>
</tbody>
</table>
PostgreSQL: PCI-Compliant Pattern

• An Entirely Different Beast
  – Additional/different requirements
  – All non-cardholder data supported
  – Enables multi-million dollar savings
What’s Next?

• Mongo – SOX pattern
  – Currently in proof-of-concept
  – Currently being reviewed by internal partners
  – Q1 2020

• Kafka – SOX pattern
  – Believed to be close to finished
Take-Aways

- **Support** - Partners & Leaders
- **Scope** - Know the controls to be addressed
- **Adoption** - An important, often overlooked step