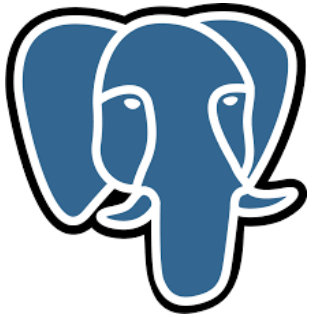
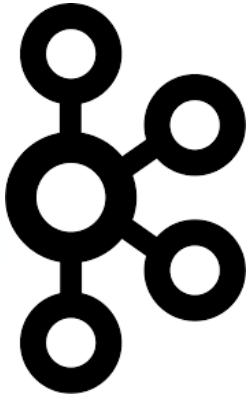
Developing Compliant Patterns for Modern Technologies



Stephen Podobinski
Lead Information Security Analyst
Target

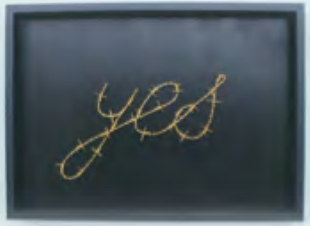
Goal & Take-Aways

- Understand the process
  - 6 steps
  - Appreciate its repeatability

p

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

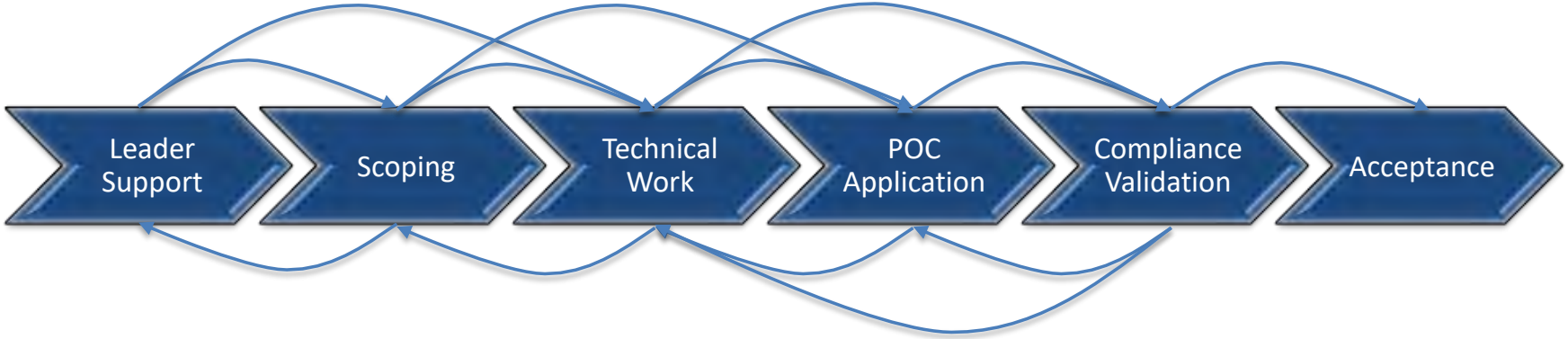


What's driving this desire?

- Typically, entities want to reduce licensing costs
- Other potential drivers:
  - Using open source technologies
  - More control over the environment
  - Be awesome

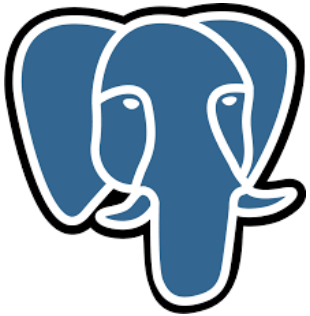
The Repeatable Process ·

- 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

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

Follow-up Items:

- I've agreed to send communication and set up a meeting with the 5 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 SCML 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 ~12/1) include:
  - Additional screenshot 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

Status Summary:

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

Next Steps:

- See 'Follow-up Items' above

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

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 constituency 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/Mdse+Transfer+-+Design – Architecture diagram we're working with the FIN team to understand

Control Standard (SOX Specific)	Technically Complete	Application Validation	Compliance Acceptance	Next Steps
CS-1557076 – Access Provisioning	Complete	Not Started	Not Started	Completed work on LDAP integration
CS-1557079 – Access Reviews	Complete	Not Started	Not Started	Completed work on LDAP integration
CS-1557077 – Change in or Termination Role/Responsibilities	Complete	Not Started	Not Started	Completed work on LDAP integration
CS-1557122 – Configuration Scanning	In Progress	Not Started	Not Started	Target India working the SCML baseline
CS-1557160 – Data Backup and Storage Requirements	Blocked	Not Started	Not Started	Technical and Compliance teams are at an impasse
CS-1557074 – Identity and Access Management Configuration	Complete	Not Started	Not Started	Completed work on LDAP integration
CS-1557075 – Least Privileged Access Control	Complete	Not Started	In Progress	PADD is completed and reviewed; review by SOX team needed
CS-1557119 – Monitoring and Resolving Processing Errors	Blocked	Not Started	Not Started	Technical and Compliance teams are at an impasse
CS-1557150 – System Activity Logging	In Progress	Not Started	Not Started	Completed integration with T-Falcon->Kafka->Kibana pattern for logging
Automated Schema Change Pipeline	In Progress	Not Started	Not Started	Team working on automating via GHE

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

Take-Aways

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