

Being Audit Ready, Not Reactive – Automation What!

Team Governance, Risk and Compliance (GRC)

Global Cybersecurity, Liberty Mutual Insurance





Denise Miller

Manager, Global Cybersecurity
Governance, Risk and Compliance



Leah Mongeon

Solution Specialist, Cybersecurity
Governance, Risk and Compliance



Sheri LaCarbonara

Solution Specialist, Cybersecurity
Governance, Risk and Compliance



WARNING!



PROCEED WITH CAUTION



Agenda

Session Goals

Our Journey

- Keeping pace
- Moving to audit ready
- Automating today and tomorrow

**Session
takeaway**

5 areas to automate in your world

Session Goals

What You Can Expect To Learn Today

**How to keep
pace with
ever-growing
requirements**

**How to go
from audit
reactive to
audit ready**

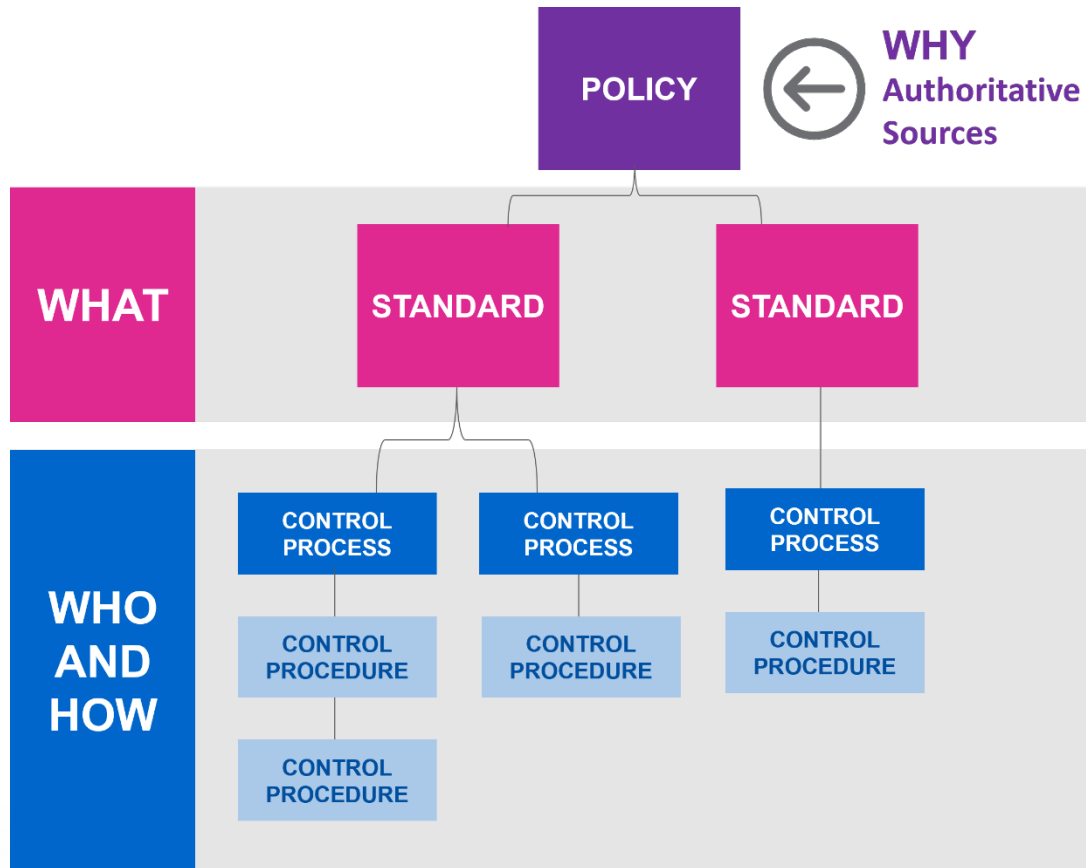
**How to
begin your
automation
journey**

Poll

- **How many regulations, contractual requirements or frameworks does your company leverage to drive your assurance programs?**
- **Polling response options**
 - **Less than 5**
 - **5 - 10**
 - **More than 10**



Keeping Pace



BUILDING: Control Library

- Authoritative sources support the "why"
- Organized by policy, standards inform the tool agnostic or the "what" to satisfy authoritative sources
- Controls inform the "who" and "how" for adhering to the standard
- Control teams understand what controls apply and alignment

Keeping Pace

ENABLING: Reuse and Automation

- Harmonizing controls across authoritative sources
- Collecting data and artifacts
- Building in automation; automating manual

Control Owner's Validation of Control Procedures

Email Notification

CyberGRC Archer <cybergcarcher@libertymutual.com>
To: Campbell, Ashley

Retention Policy Deleted Items (90 days)

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Expires: 1/14/2024

Control Design Consulting & Review

See the **My Tasks** section of the CyberGRC home page to view all tasks currently assigned to you.

Control Owner's Validation of Control Procedures

You are receiving this notification because you are listed as a Control Owner on one (or more) Control Accuracy Validations in CyberGRC Archer. Your input is essential to validate that the control documentation is accurately stated. We realize these reviews are one of many competing priorities each year. Thank you for your time, effort, and partnership in making these reviews successful.

Please take a moment to review and validate the people, processes, tools and/or technologies within your aligned control procedures.

Use the Questionnaire ID link(s) below to access the control validations assigned to you. Alternatively, use the **Control**.

For questions about the process, visit the Control Accuracy Validation Workflow [link](#) or contact the GRC Reviewer. For

Questionnaire ID: 2534341
Control Procedure: Name of procedure
Validation Required By: 10/28/2023
GRC Reviewer: Name of employees that perform

List of more CPs to review

Control Design Consulting & Review
GCS | Governance, Risk & Compliance

The screenshot displays the CyberGRC Archer web application interface. The top navigation bar includes the Liberty Mutual logo and the text "CyberGRC Archer". Below the navigation bar, there are several tabs: "Issues Management", "IT Policy Management", "IT Controls Assurance", "IT Security Risk Management", "Issues Management", "SIG Customer Inquiry", and "Administrative Reporting". The main content area is divided into two panels. The left panel shows the "Control Accuracy Validation : 2534341" details, including a "REFINE BY" section with filters for "Assessment Year" (2022 (276), 2023 (127), 2021 (1)), "Request Status" (Completed (404)), and "Due Date" (August 2023 (3), April 2023 (1), March 2023 (36), February 2023 (87), October 2022 (20), September 2022 (29), August 2022 (7), May 2022 (2), April 2022 (117), January 2022 (107)). The right panel shows the "EVIDENCE REPOSITORY" with a table of search results. The table has columns for "Assessment Year", "Request Status", "Document ID", and "Due Date". The table contains 40 rows of data, showing various assessment years and request statuses. The bottom of the interface features the "PCI Security Standards Council" logo and the "RSA ARCHER SUITE" branding.

Poll

- How many of you are prepared prior to a regulator/auditor/assessor coming on site and have a package of materials ready to go for them (without a request list)?
- Polling response options
 - I am ready to go day 1
 - I need a request list and then we start to collect evidence and set up meetings
 - I am not sure



Control

Control
Validation
Reviews

Request

Request
once, apply
many

Evidence

Evidence
Repository

*“There’s a way to do
it better – find it.”*

Thomas Edison

Automating Today and Tomorrow

Current State

Control Testing

12 control tests automated for control areas in Change Management, Logical Access and Problem Incident Management

Testing runs in less than 1 minute; significant number of manual hours saved

External assessor buy-in; consideration for relying on automated testing for Internal and External GRC Compliance programs

Future Opportunities

Expansion

Control Testing automation for all GRC programs with possible expansion to business

Findings

Automated identification, notification and resolution

AI and Automation

Leverage AI in combination with automation to further digitalize current processes around data intel collection, summarization and mapping

Lessons Learned

Early Days for AI and Automation

Not widely embraced; may require heavy lifting to get teams and external assessors on board

- **Learning curve and slow adoption** of automated testing results and AI by both internally and externally
- **Vendor data validation** Information Provided by Entity (IPE) for all automation
- **Inconsistencies** in data sources and testing practices poses automation challenges

Our Journey

Continuous
Compliance &
Audit Ready
Data driven
insights into our
control state

Assessment Automation
Across multiple regulations,
frameworks and company
requirements

Control
Balance custom assessment
needs with enterprise standards

Policy/Standards
Manage these to meet or exceed level

Authoritative Sources
Frameworks and Risks

Session Takeaways – 5 Areas to Automate



Policy & Standard – Reviews & Approval



Process & Control Validations



Evidence Requests for Reuse



Program Scope Details



Controls with Data Insights

Thank You