Continuous Compliance in DevSecOps - The Resolution Life US Story

October 3, 2023

Resolution Life

CN202314_0918

CN202314_0918

Agenda for today

1. Software delivery changes in the Insurance industry
2. Benefits/Opportunities of automation
3. Resolution Life US Problem Statement Overview
4. What is Continuous Compliance?
5. What did we do?
6. Demo: Gathr Continuous Compliance Solution

Sensitivity - Restricted

Your presenters

Mittal Bhiogade
Chief Architect,
Resolution Life US

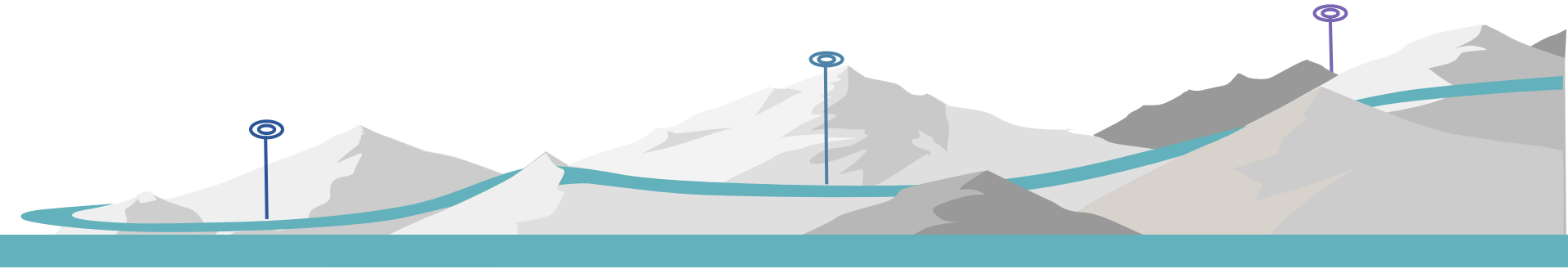
Matthew Bonser
Director,
PricewaterhouseCoopers

Bhavin Shah
SVP - Sales and Customer Success, Gathr

Sensitivity - Restricted

Key challenges for insurance industry for change management

- Disparate, complex tools and processes
- Uncorrelatable data
- Manual requests / responses for data
- Delays in visibility of current state
- Iterative manual audit and remediation
- Hard to trace source of issues quickly



Sensitivity - Restricted

Opportunities to improve the overall change management process

01 Consistent & Repeatable Processes

02 Integrated tools and technologies

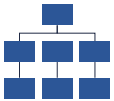
03 Traceable and auditable change flow

04 Alternative change management processes

05 Continuous automated monitoring

Sensitivity - Restricted

What is Continuous Compliance?

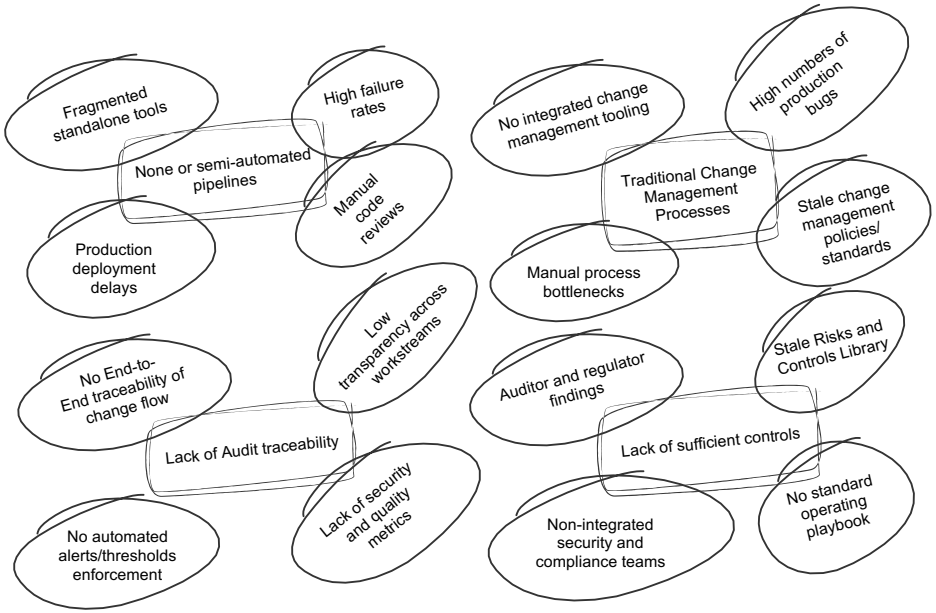
1	2	3	4	5
				
Culture Shift	**Dynamic Policy Adjustments**	**Integrated Systems**	**Automated Alerts and Notifications**	**Real-Time Monitoring**
Encourage a culture of accountability and responsibility to foster awareness of compliance requirements	Adapt policies and controls based on changing regulatory requirements	Ensure new code changes and updates comply with regulations while embracing DevOps and Agile methodologies	Trigger alerts to relevant stakeholders when compliance deviations are identified	Continuously monitor activities for any deviation from established compliance parameters

Sensitivity - Restricted

Compliance by Design in IT change management

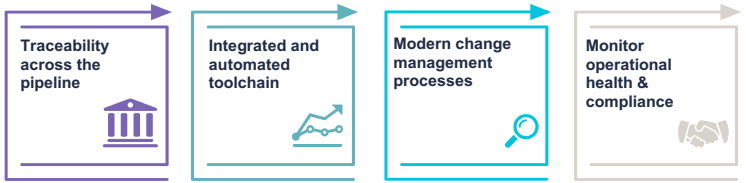
Automate compliance in the technology change management process to both strengthen the environment and enhance the developer experience

Disparate, Complex Processes



Target Tech Enabled Model

Continuous compliance and monitoring through the technology change cycle



Policies, Standards & Procedures

Standard Pipeline Tools and Configurations

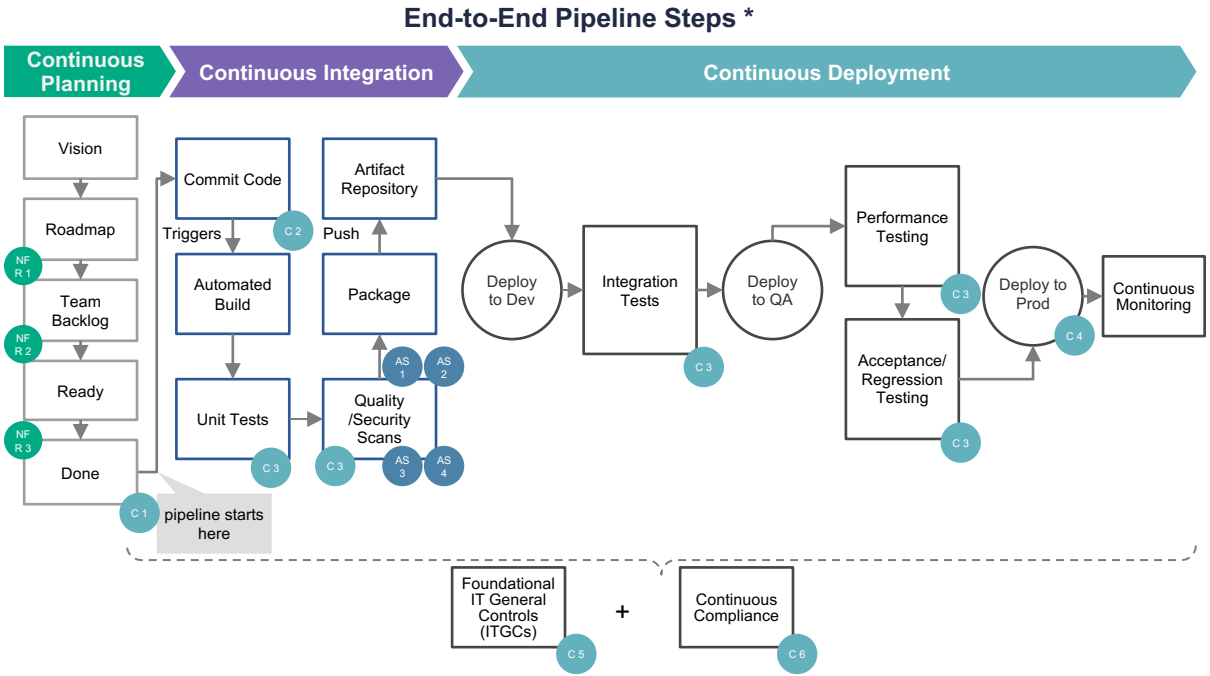
Operating Playbooks and Guardrails

Continuous Compliance Monitoring Tools

Sensitivity - Restricted

Integrating Compliance tools with DevOps toolchain

Achieving Compliance and Controls through DevSecOps



* Through necessity of showing a flow, this is shown as a single, linear process. In reality, certain capabilities persist throughout & the steps involved iteration

Non-functional Requirements (Compliance, Control, Audit, Privacy and Information Security Teams)

- NF R 1 — Quarterly product roadmap review
- NF R 2 — Add non-functional requirements as user stories with detailed acceptance criteria and DoD
- NF R 3 — Confirm security, privacy and controls related objectives

Application Security Validation Controls

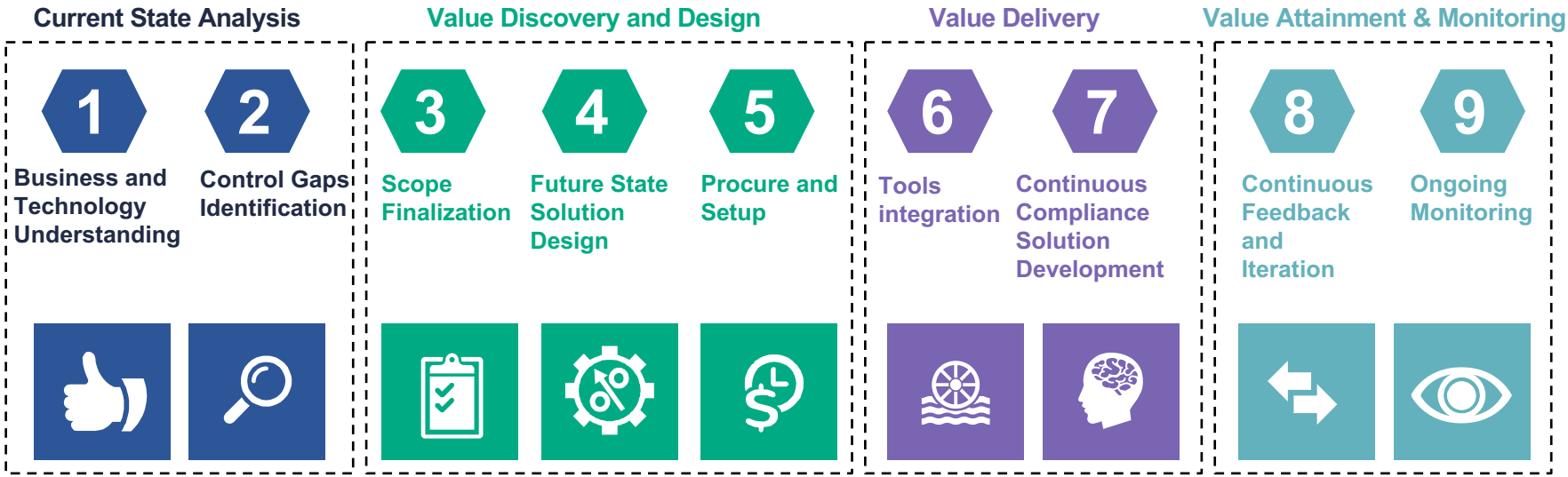
- AS 1 — Software Composition Analysis (SCA)
- AS 2 — Static Application Security Testing (SAST)
- AS 3 — Dynamic Application Security Testing (DAST)
- AS 4 — Interactive Application Security Testing (IAST)

Other IT General Controls

- C 1 — Changes are authorized by Product Owner
- C 2 — Code is reviewed by peers for quality and validity
- C 3 — Changes are tested and meet exit criteria
- C 4 — Validate deployed code has met quality standards and controls
- C 5 — All tools in the pipeline have ITGCs (change control, role-based access controls, segregation of duties)
- C 6 — The control environment is continuously monitored and violations trigger remediation protocols

Sensitivity - Restricted

What did we do?



Sensitivity - Restricted

But why is all of this important, though?

Develop End-to-End Traceability

Establish a traceable end-to-end audit trail to track code changes, infrastructure changes, configurations to demonstrate compliance at any point

Reduce Cost of Audit

Reduce your cost and effort in executing cumbersome and manual audits by establishing automated monitoring and tracking of the development lifecycle

Establish Compliant Processes and Tools

Enforce automated validation and reporting of control points defined across the pipeline to ensure your systems remain compliant and in alignment with regulatory requirements

Enable Low Touch Change Flow

Introduce an alternative to traditional change management process, with end-to-end automation where possible

Sensitivity - Restricted

Continuous Compliance Solution Demo

Gathr Demo

Sensitivity - Restricted

Thank you