

Compliance in The Agentic World

Learning Objectives

1. Overview:Agentic AI Architecture
2. AI in Compliance
3. Balancing Progress & Risk via Governance
    a. Challenges to Agentic AI Adoption in Security
4. Enhancing Security through Agentic AI Use Cases

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

Marcos Marcal

Product Compliance, Senior Manager
Salesforce.com



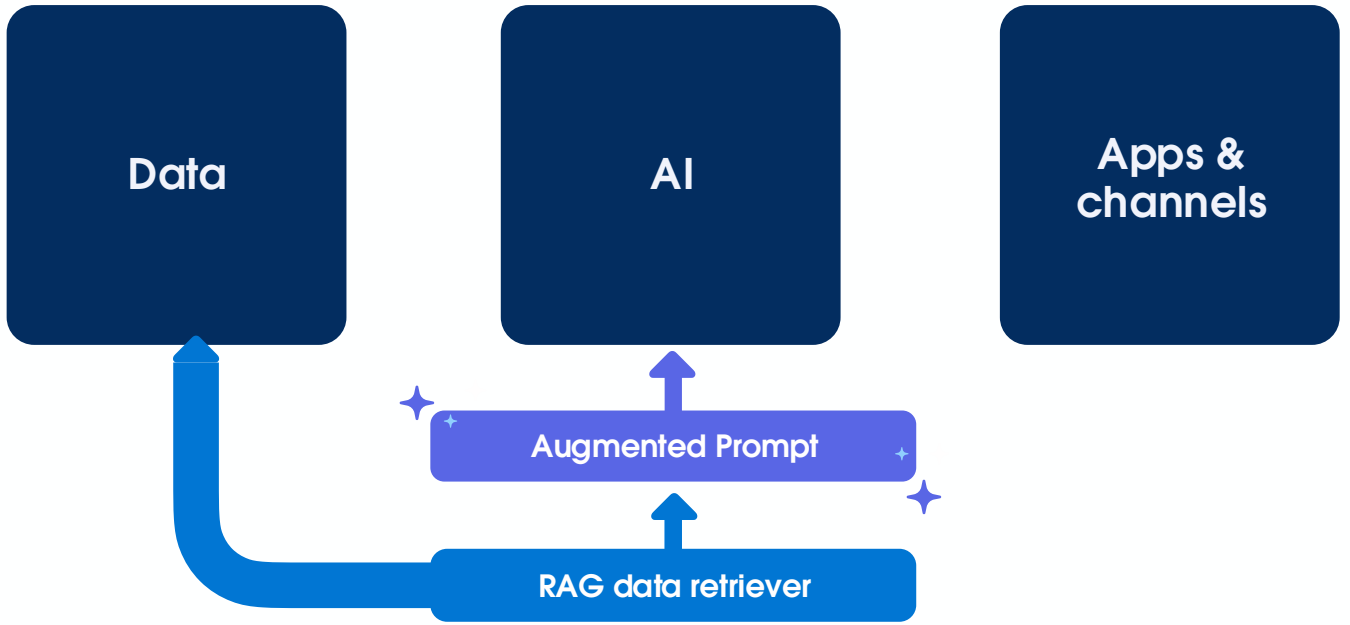
Humans + AI



Agentic Architecture Primer

Iterative and Adaptable Automation

1. Perception and Data Collection
2. Decision Making
3. Action Execution
4. Learning and Adaptation

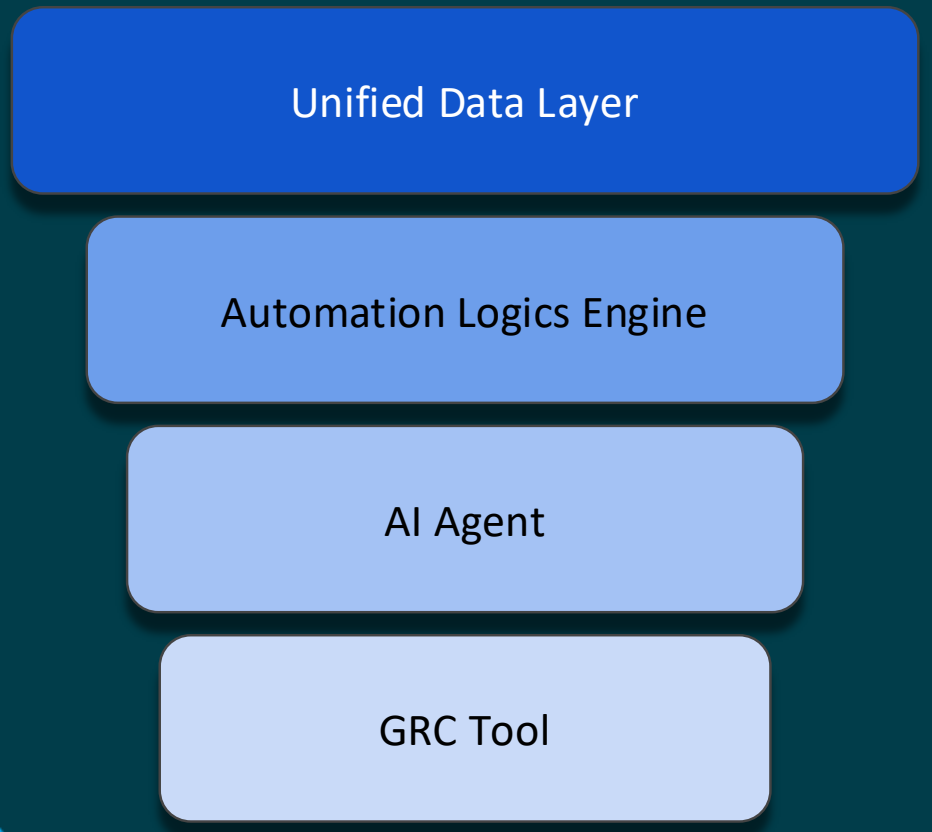


salesforce
20 YEARS OF SECURING PAYMENT DATA PCI

Automation Vision

Implementing compliance efficiencies

Automation Data Flow



- Data lake to store all log data and more
- Automation Logic Engine performs compliance checks on data fetched from a unified data layer
- AI Agent to digest the results from logic layer and feed into GRC tool in desired state (e.g. creating test papers based on test results)
- GRC tool to record audit results and display compliance posture dashboard

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

AI in Compliance

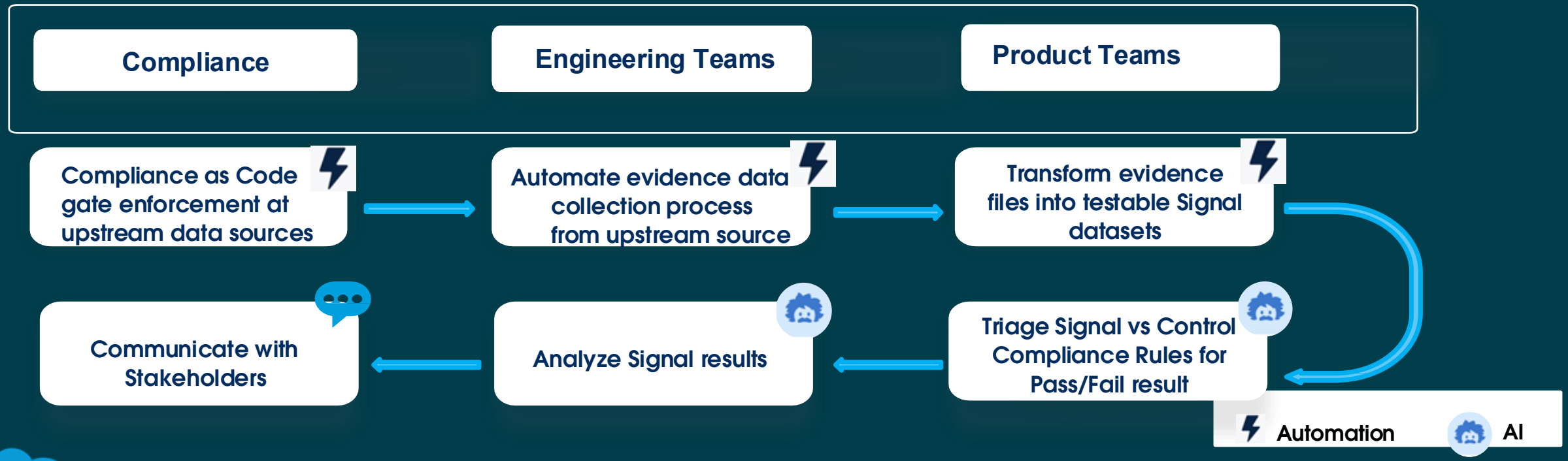


salesforce

The Compliance Function & Challenges

The challenge is to implement a **scalable security program** that provides on-demand guidance from **trusted** intelligent sources to reduce the burden of manual processes and ensure the creation of consistent, audit-ready documentation.

Across compliance value streams with **automation and agentic products** that increase consistency and reduce cycle times…

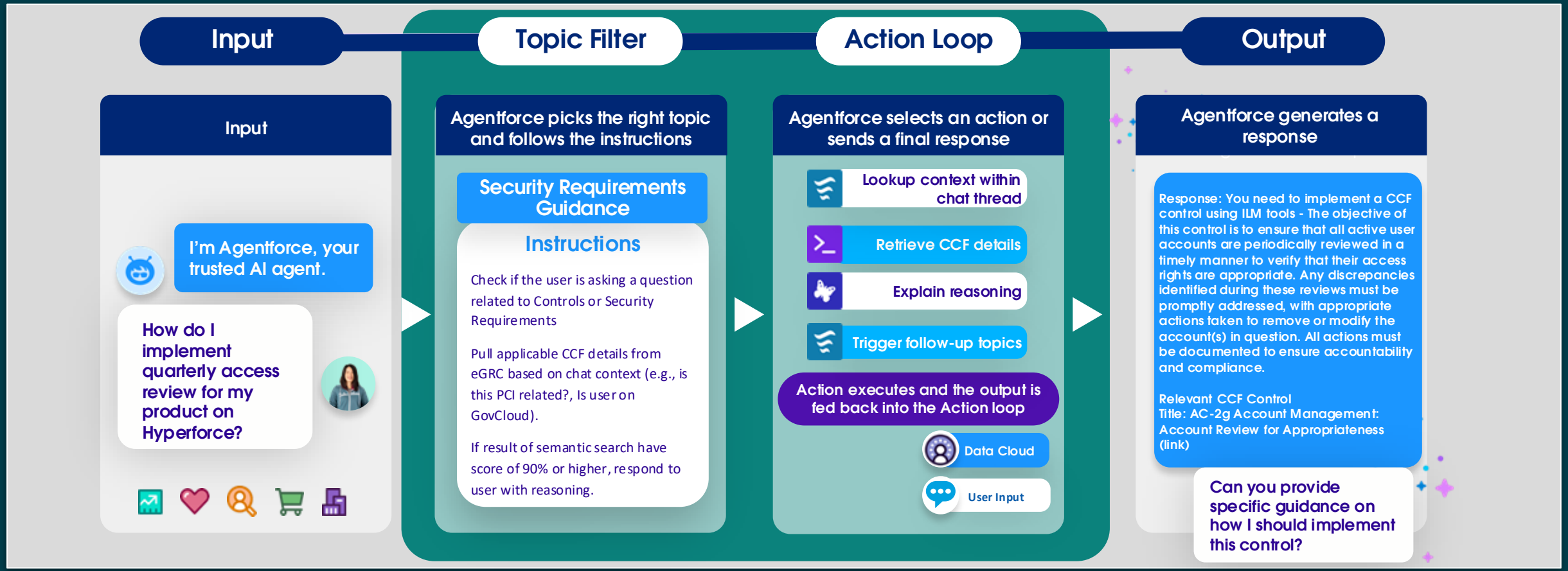


salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

Using Agents to Enhance Compliance

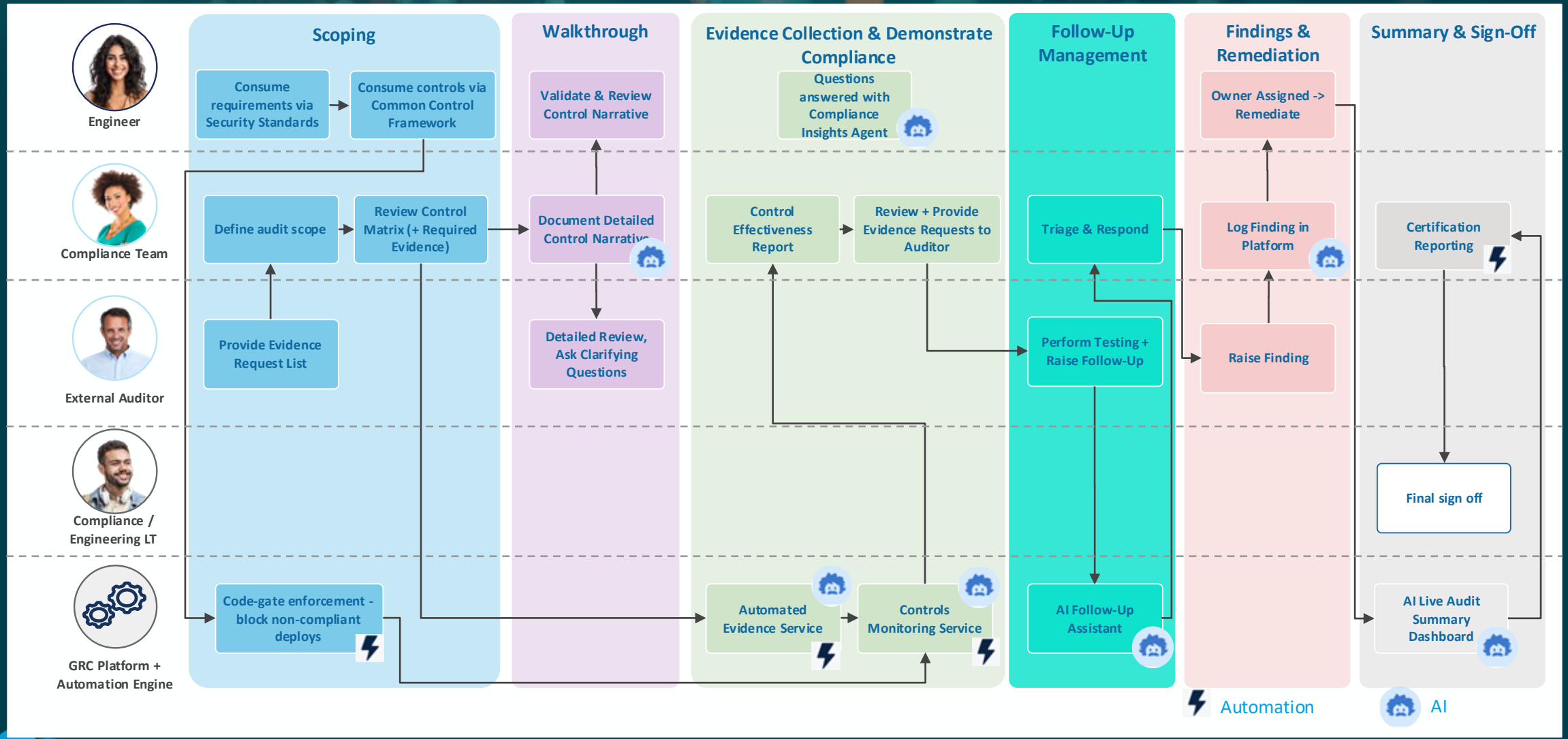
Streamlining Processes to Improve Customer Experience



salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

The Ideal Compliance Journey w/ AI



salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

Securing AI Through Effective Governance



salesforce

Securing AI - Common Risks & Mitigation Action

Balancing Security and Innovation

Common AI Risks

Confidentiality: Sensitive data exposure through prompt injection

Integrity: Hallucinations, factually inaccurate data

Security: Expanded 3PP attack surface

Mitigation Actions

Strong policy guidance

Investing in the right tools

Expanded monitoring & alerting

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

Practical AI Governance

Best Practices



Challenge of AI Governance

Invest in the Right Tools

Implement Monitoring & Alerting

Strong Policy Guidance

Drive toward clarity and a unified vision of agentic AI into your organization

Accelerate Innovation

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

Enhancing Security and Governance Functions with Agentic AI



salesforce

Key Operational Areas in Security

With Intensive Manual Processes

- Operations
- Product Security
- Customer Trust
- Security Bug Discovery
- Security Standards
- Security Compliance

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

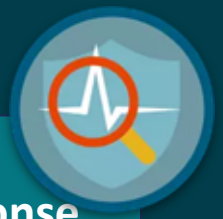
Agentic AI Use Cases in Security

Agentic AI deployments drive risk reduction at enterprise scale



Customer Inquiry Response

- Agents respond to customer security questionnaires
- 1,500+ questionnaires received per year
- Reduction in response time to 6-7 seconds



Detection & Response

- Automated triage
- Agentic AI-developed summaries streamline incident handover
- Annual time savings of 3,000+ hours



3PP Security Engineering

- Agents to pre-assess supplier requirements
- Summarizes Salesforce's questionnaires to suppliers and highlights potential risks
- 30% reduction in time spent on reviews

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI

Agentic AI in Governance, Risk & Compliance

Governance

- Standardize & rationalize Policies, Standards, and SOPs (PSSOP)
- Provide human-like PSSOP usage guidance to engineers
- Use CCF to provide compliance control implementation guidance to engineers/stakeholders
- Automated alignment of CCF to capture global regulatory requirements, and generate test & implementation plans

Risk

- Perform automated risk assessments of products based on the compliance framework (CCF)
- Auto-feed and update CCF based on the risk assessment



Compliance

- Automated evidence collection
- CCF-based compliance checks
- Work paper creation based on manual & automated testing
- Onboard new products/features or new certification requirements through automated gap assessments
- Track remediation efforts and guide engineers in real time

salesforce

20 YEARS OF SECURING PAYMENT DATA PCI