



**2025  
NORTH  
AMERICA  
COMMUNITY  
MEETING**

2025  
NORTH  
AMERICA  
COMMUNITY  
MEETING

# The Future of Governance:

Leveraging Automation to Enhance Security



# James Huang

CISA, PCIP, ISA

Director - GCC

Salesforce



# Learning Objectives

- Learning Objective #1: Challenge: Alphabet Soup of Compliance
- Learning Objective #2: Common Controls Framework: Overview
- Learning Objective #3: Reducing Engineering Toil: Distributed Control Model
- Learning Objective #4: Security Stack: Enhancing Compliance via Automation

# Alphabet Soup of Compliance

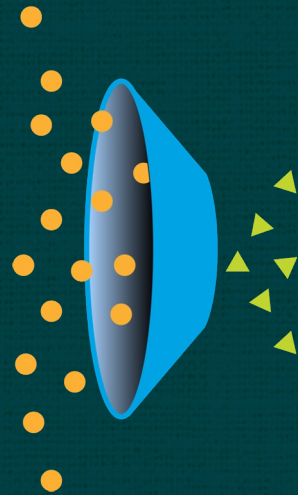


# The Common Control Advantage

## 10000+ Controls

### Applicable Industry Standards, Frameworks and Control Requirements

- AICPA Trust Service Principles - Service Organization Controls (SOC: S/A/C)
- ISO 27001 and 27002
- PCI DSS
- ISO 27017/27018/27701/22301
- IRAP
- ISMAP
- Spanish ENS (Basic)
- BSI C5



## Future State (350 controls)

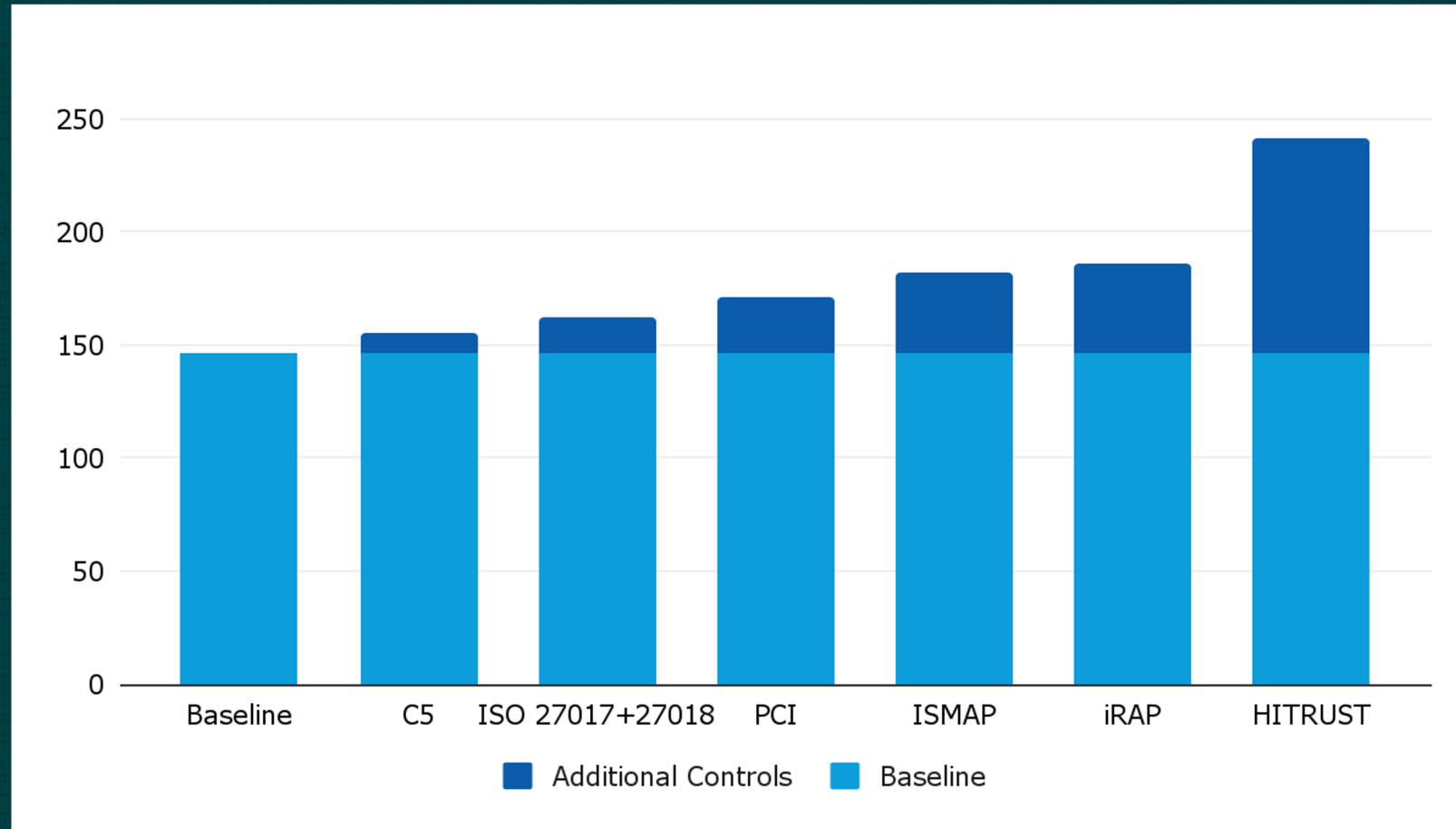
### The CCF Families and Control Requirements

- ▲ Vulnerability Management
- ▲ Supply Chain & Vendor Security
- ▲ Secure Software Development & Build Environment Security
- ▲ On-Premise Asset & Cloud Accounts
- ▲ Network Security
- ▲ Logging, Monitoring & Incident Response
- ▲ Identity & Access Management
- ▲ Detection and Response
- ▲ Data Governance and Protection
- ▲ Cryptography, Encryption, & Key Management
- ▲ Application and OS Security

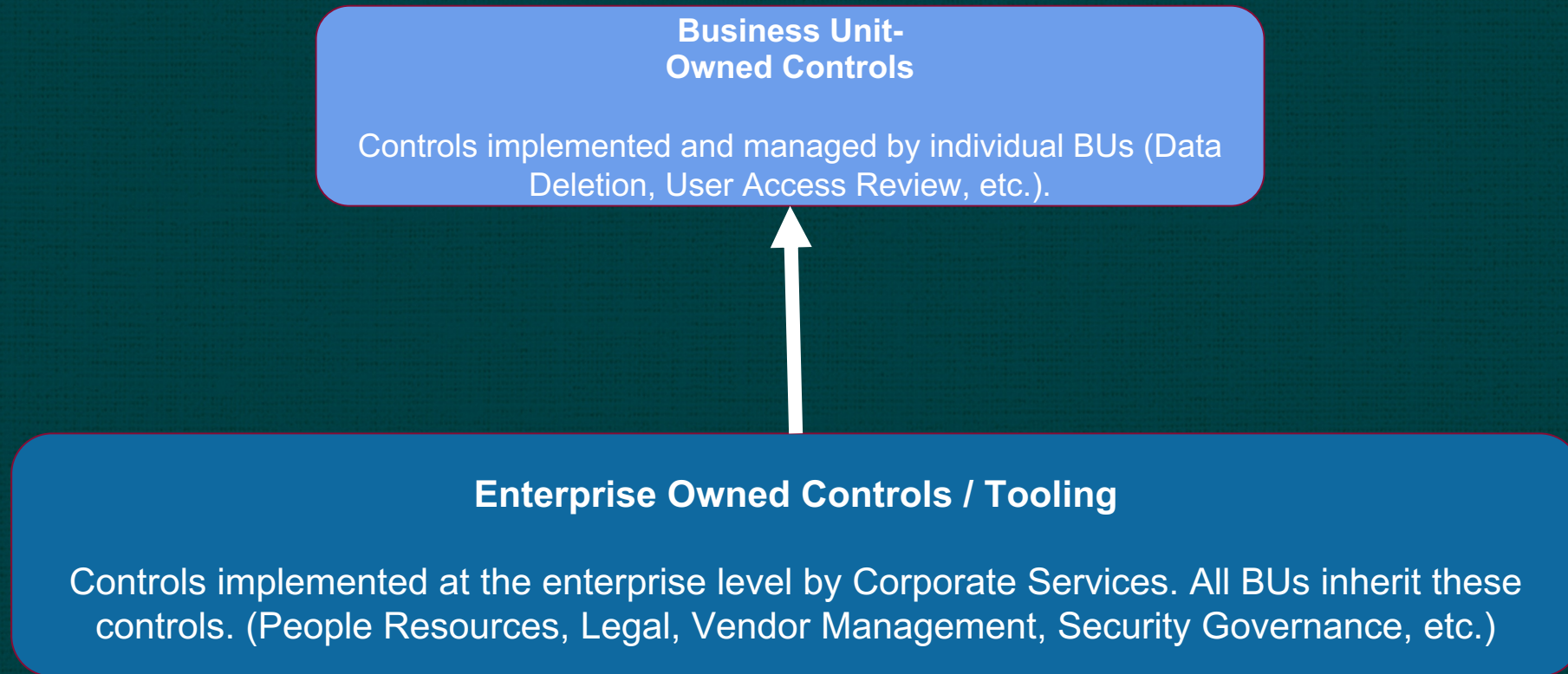
Total Control Count

~350

# CCF - A Stair Step Approach



# Reducing Engineering Toil: Distributed Control Model



# Security Stack: Enhancing Compliance via Automation



## Embedded Compliance

Shift compliance requirements to where engineers work, enabling simpler and faster adoption of compliance and CCF requirements



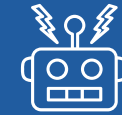
## Zero-Touch Audits

Develop necessary Agentforce functionality to execute audits with zero-to-minimal engineering and/or compliance personnel involvement.



## Realtime Control Monitoring

Establish real-time visibility into control health, and develop the necessary tools, programs, and/or processes to rapidly remediate any known findings or control failures.



## Compliance Agents

Identify key processes and employee functions that can be autonomous. Develop, deploy, and maintain agents that perform these tasks, enabling a better experience for our stakeholders and freeing up personnel time for other critical initiatives.

# How Does Agentforce Enhance Compliance?

Input

Topic Filter

Action Loop

Output

Input



I'm Agentforce, your trusted AI agent.

How do I implement quarterly access review for my product on Hyperforce?



Agentforce picks the right topic and follows the instructions

Security Requirements Guidance

Instructions

Check if the user is asking a question related to Controls or Security Requirements

Pull applicable CCF details based on chat context (e.g., is this PCI DSS related?, Is user on GovCloud).

If result of semantic search have score of 90% or higher, respond to user with reasoning.

Agentforce selects an action or sends a final response



Lookup context within chat thread



Retrieve CCF details



Explain reasoning



Trigger follow-up topics

Action executes and the output is fed back into the Action loop



Data Cloud



User Input

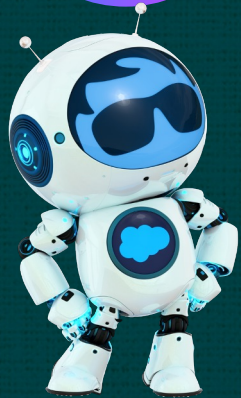
Agentforce generates a response

Response: You need to implement a CCF control using ILM tools - The objective of this control is to ensure that all active user accounts are periodically reviewed in a timely manner to verify that their access rights are appropriate. Any discrepancies identified during these reviews must be promptly addressed, with appropriate actions taken to remove or modify the account(s) in question. All actions must be documented to ensure accountability and compliance.

Relevant CCF Control  
Title: AC-2g Account Management: Account Review for Appropriateness (link)

Can you provide specific guidance on how I should implement this control?

# Agentforce Example



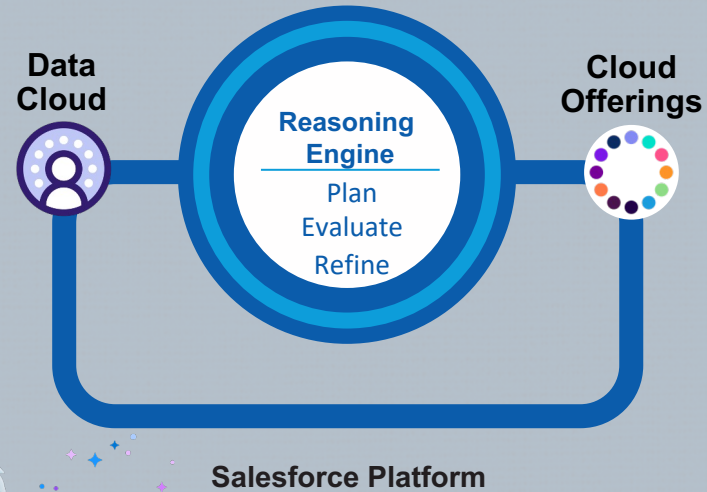
## Agents Become Teammates



### Agentforce in Slack

- Easily Discover
- Message Directly
- Deploy in Channel
- Enable with Slack Skills & Actions
- Proactive Assistants

## Permissioned Conversations feed Atlas

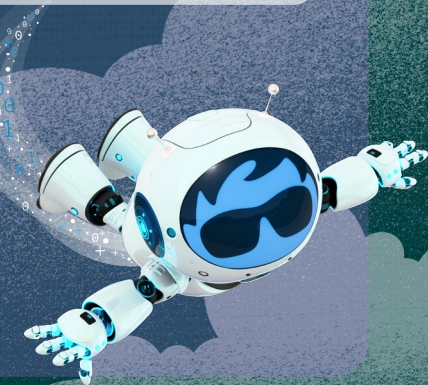


## Real-Time Outcomes

Improved Reasoning

More Accurate Recommendations

Smarter Actions



# Market Access Benefits: Business & Innovation Uplift

Increased Efficiency  
Faster GTM timelines

*Shorter development & deployment cycles*

*Facilitates business growth with sales & engineering*

Rapid Cert Onboarding  
Drive regional & vertical sales

Proactive Approach  
Reduces risk & costs

*Automated compliance issue detection & remediation*

*Agentforce for regulatory and compliance use cases*

Industry Leadership  
Pioneer agentic AI compliance adaptation



**Please come find me during a Networking  
Break if you have any questions!**



2025  
NORTH  
AMERICA  
COMMUNITY  
MEETING