



Federal Information Assurance Management and FISMA Compliance with RSA Archer

Chris Hoover,
CISA, CISSP

Thursday, July 18th
11:00 AM/EST

U.S./Canada Toll-Free
1-877-748-4008 PIN: 8875

International Toll
Dial 001-503-295-8000, then enter
877-748-4008 and PIN: 8875

Or listen via your computer speakers:
Under the Voice & Video tab
select “Join Audio”

Disclaimer – Safe Harbor Statement

- This presentation is for informational purposes only. This document contains certain statements that may be deemed “forward-looking statements” within the meaning of the Private Securities Litigation Reform Act of 1995.
- Forward-looking statements are based on assumptions and assessments made by us in light of our experience and perception of historical trends, current conditions and expected future developments. Actual results and timing of events may differ materially from those contemplated by the forward-looking statements due to a number of factors, including regional, national or global political, economic, business, competitive, market and regulatory conditions.
- Any reproduction, retransmission, or republication of all or part of this document is expressly prohibited without the permission of RSA.

Introduction

- Chris Hoover, RSA Archer Federal Solution Manager
- 15 years in federal IA
- Equal mix of military, intelligence, and civilian experience
- Pentagon, Baghdad Embassy, NGA HQ, Los Alamos Labs, Joint Analysis Center UK
- SME driving federal solution offerings for RSA Archer

Agenda

- Federal IA challenges
- How Archer can help
- Demo
- Questions

Federal IA Challenges

Challenges – Learn & Implement New Requirements

- Continuous Monitoring
 - New controls
 - New family (Privacy)
 - Overlays?
- DoD switching to NIST / CNSSI 1253 / (DIARMF)
- FedRAMP



Challenges – Learn & Respond to New Threats

- New threats
- How to react:
 - New methods
 - New processes
 - New tools



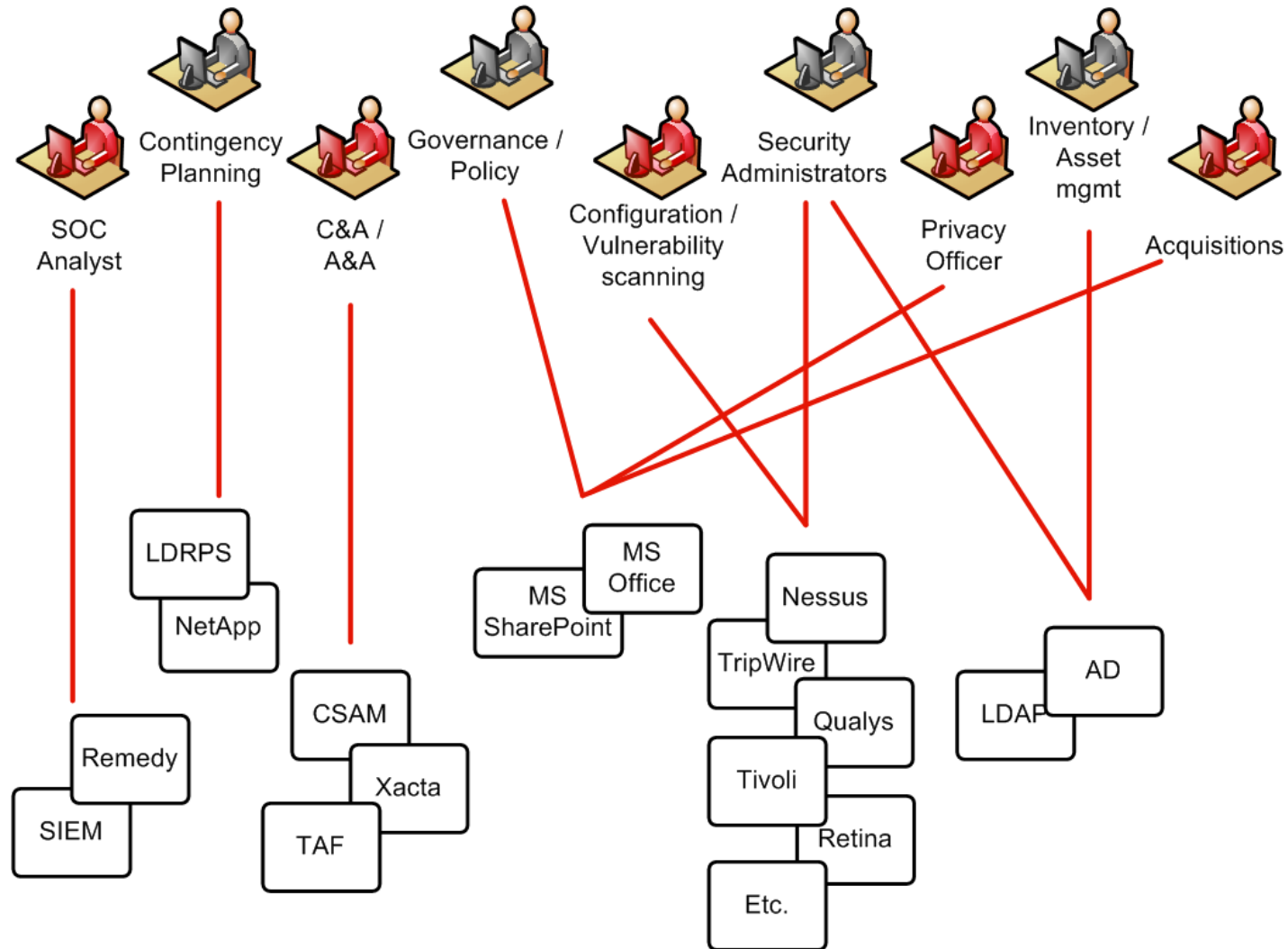
Challenges – Stovepipes / Silos

- Disparity and redundancy occur in:
 - Tools
 - Processes
 - Standards
 - Data
 - Language



Different people, different tools

- Where are they getting data ?
- Where are they putting it?



Why is this a bad scenario?

- Duplicate work
- Conflicting records
- Common format / interoperability
- Cost of licenses
- Training
- Logging in / out, account management

Challenges – Resources

- C&A required by FISMA cost \$1.3 billion per year
- Compliance auditing required another \$1 billion per year
- Since enactment of FISMA in 2002, federal government has spent over \$40 billion.



Challenges – Resources

- Annual security reports mandated by the FISMA cost \$1,400 per page to produce, totaling over \$500 million each year
- Huge amounts spent on third-party assessors and support contractors



Challenges – Resources

- Continuous Monitoring means assessing and monitoring more controls, more often, with same staff
- Budget and hiring constraints make every IA task more challenging (CR/Sequester)



Challenges – Risk Insight

- Risk decisions made without full risk picture
- Not knowing which findings/deficiencies to fix first



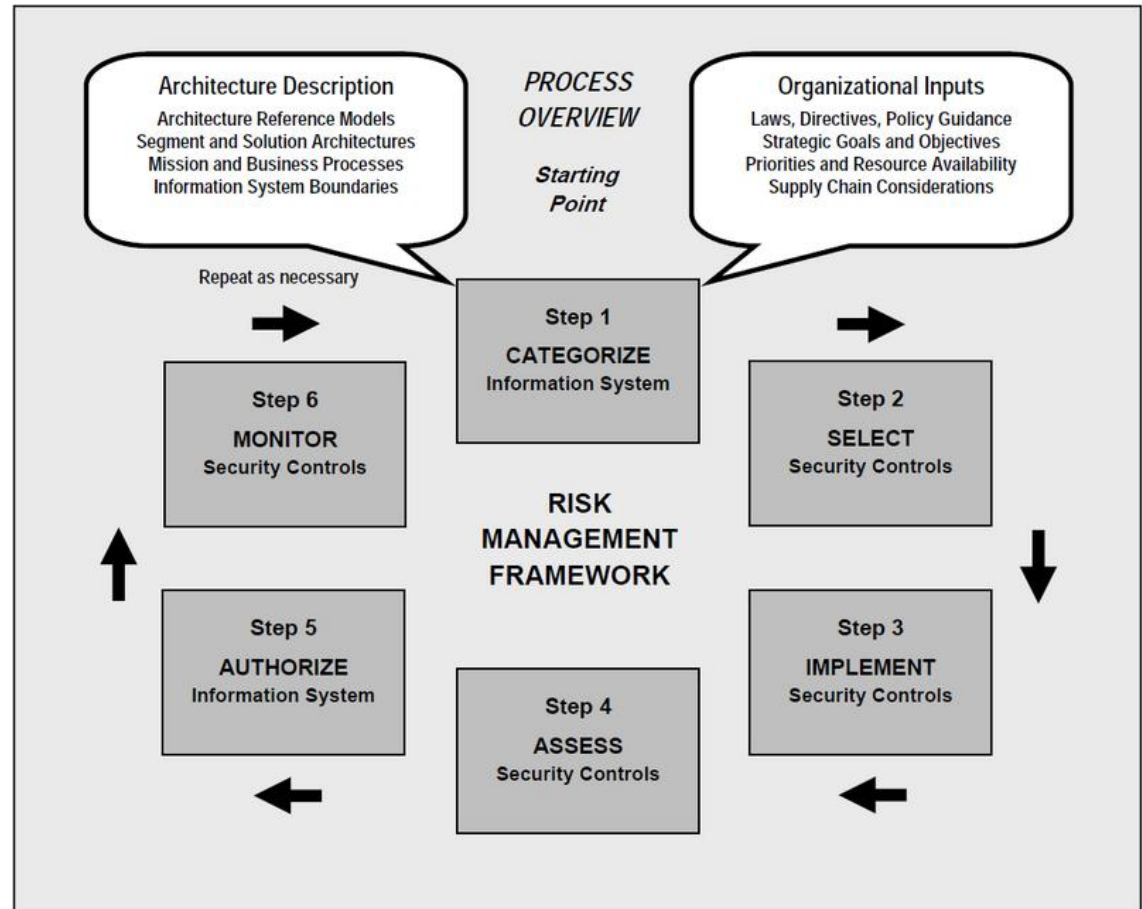
How Archer Can Help

RSA Archer Assessment & Authorization (A&A) and Continuous Monitoring (CM) solutions

- Comply with FISMA
- Integrate operational security data into compliance activities
- Actually improve your security posture

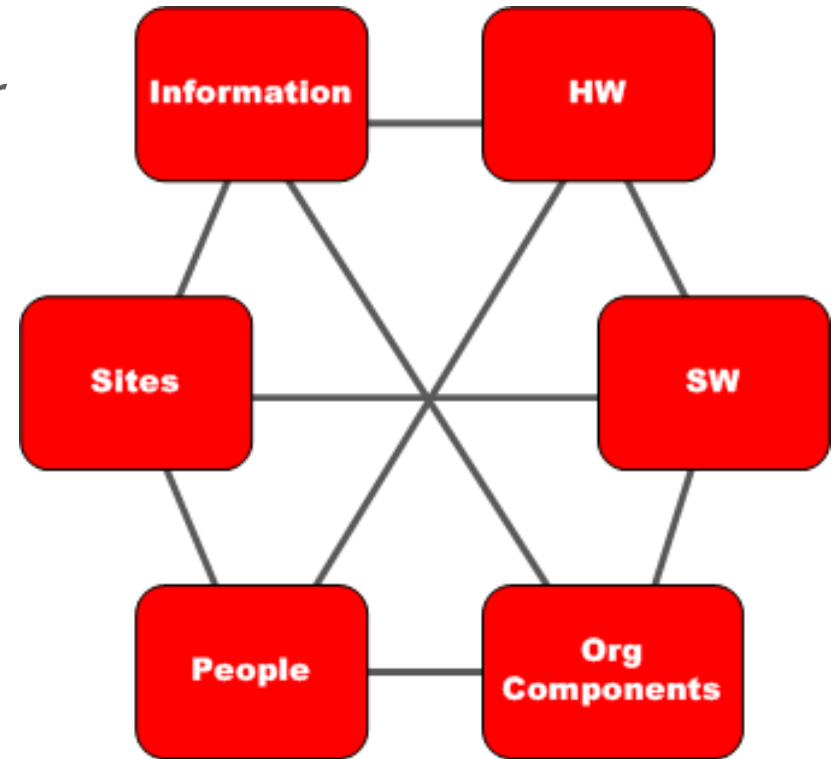
Assessment & Authorization (A&A)

- Manages all phases of NIST RMF with high integrity and rigid, role-based access enforcement



Assessment & Authorization (A&A)

- Defines assets and information systems
- Serves as the system of record for all hardware, software, and information assets
- Assets are uniquely tied to information system boundaries for A&A (formerly known as Certification & Accreditation (C&A)).
- Relationships are easily built between assets and the stakeholders and organizational components that own the assets

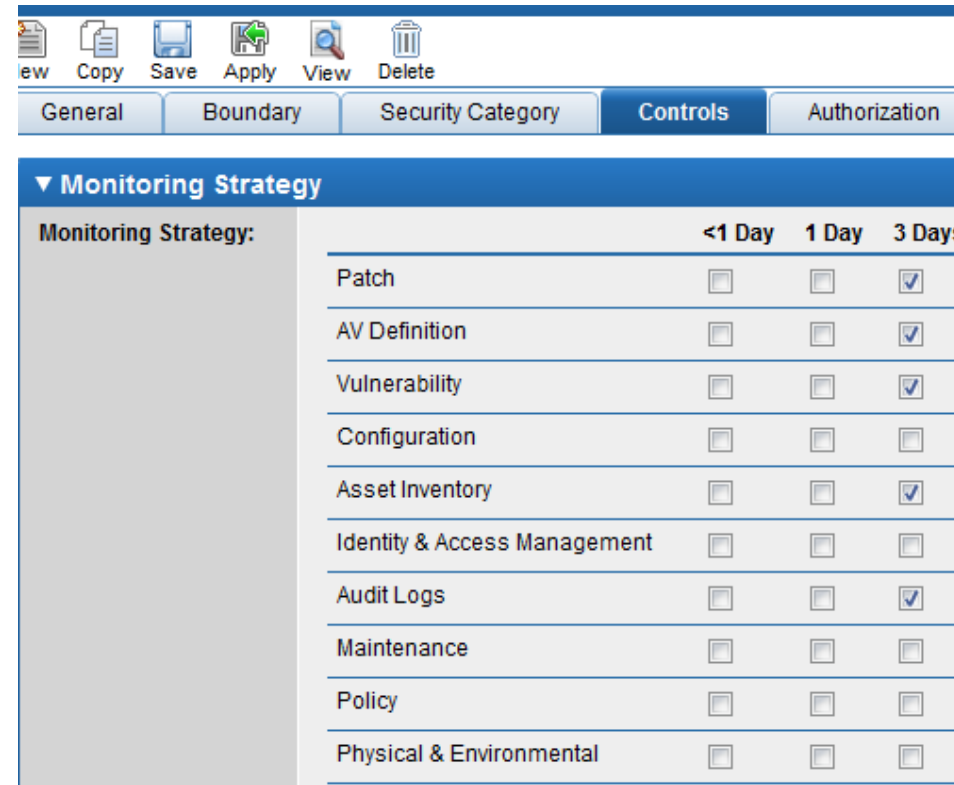


Assessment & Authorization (A&A)

- Easily allocate the appropriate baseline of controls and tailor the final control set
- Manage common controls (inheritance) through a two-way “handshake” to prevent abuse
- Manage control assessments and compliance

Assessment & Authorization (A&A)

- Streamlines assessments through Monitoring Strategy application and notifications which aid in building assessment plans and with manual continuous assessments



Monitoring Strategy:	<1 Day	1 Day	3 Day
Patch	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AV Definition	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vulnerability	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Configuration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Asset Inventory	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Identity & Access Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Audit Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Maintenance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical & Environmental	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Assessment & Authorization (A&A)

- More powerful and configurable dashboards and reports than other A&A tools
- Integrates with other RSA Archer solutions focused on operational security (Incident Management, Vendor Management, and Contingency Planning)
- Provides deep risk insight and metrics can be rolled up from end user through each component level to department and federal levels

Continuous Monitoring (CM)

- Provides near real-time insight into the security posture of every device in the enterprise.
- Manage with risk-based approach by prioritizing security risk data and focusing on “worst first”
- Automate control assessments, for other controls that are not completely automatable, the solution can provide valuable insights to control assessors to make informed assessment decisions.

Continuous Monitoring (CM)

- Leverage existing scanners and sensors and integrate new tools, including those which are Security Content Automation Protocol (SCAP)-enabled (also via XML, API, RSS, and data imports)
- Report aggregate metrics and report at any level of the organization

Archer Solutions – Learn & Implement New Requirements

- Enables Continuous Monitoring
- Accepts multiple format feeds for automated control assessment
- Allows definition of monitoring strategy
- Sends notifications to assessors for manual control assessments



Archer Solutions – Learn & Implement New Requirements

- Ongoing content development process
- 800-53 Rev 4 integrated
- Since A&A solution is based on NIST RMF, easy to adapt for:
 - FedRAMP systems
 - CNSSI 1253 /DIARMF support



Archer Solutions – Learn & Respond to New Threats

- Archer has a mature Threat management system
- Accepts live threat feeds from multiple sources
- “Speaks” multiple SCAP specifications
- Ranks threats by severity



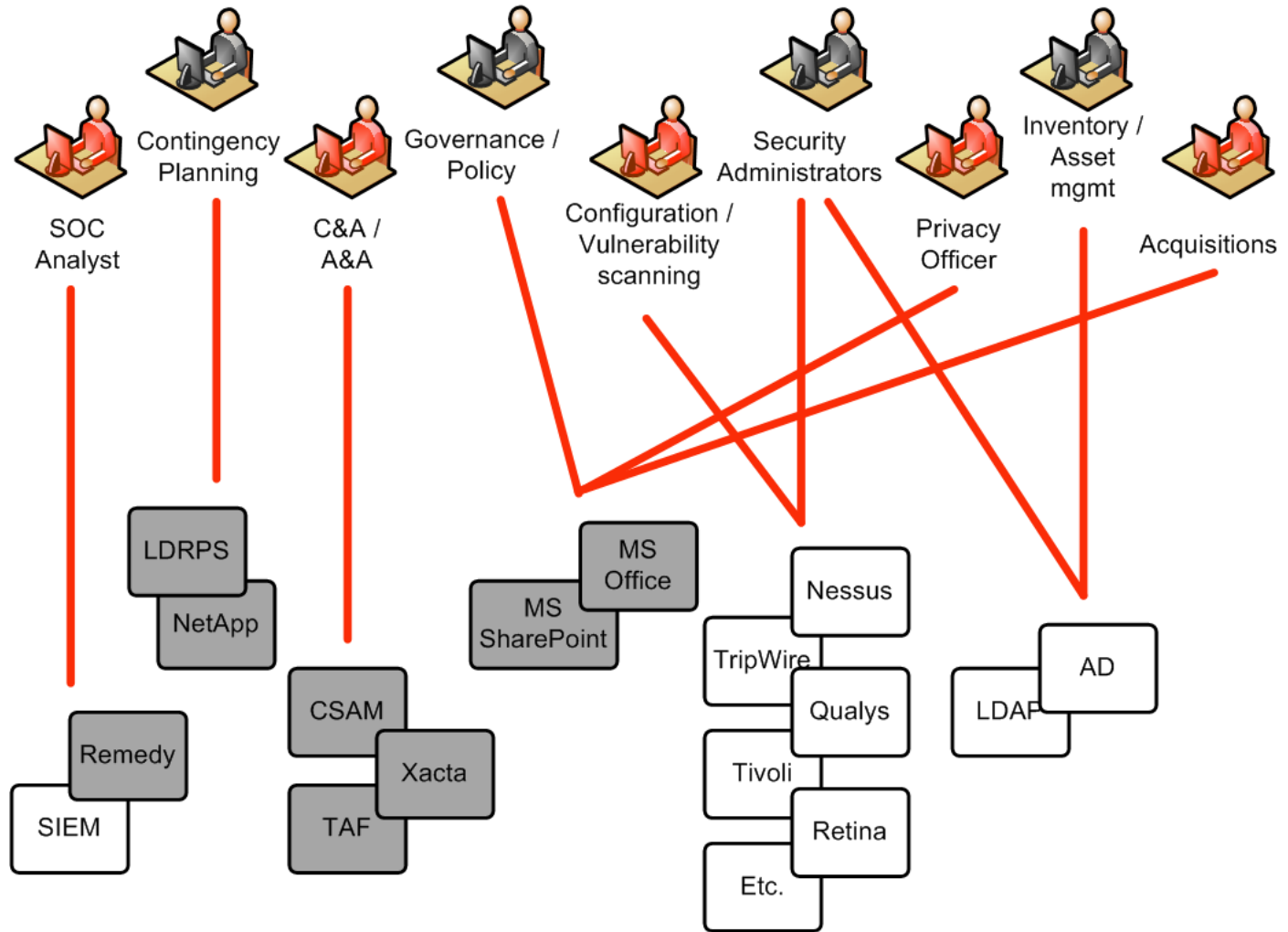
Archer Solutions– Stovepipes / Silos

- Archer can bridge & eliminate in several ways
- Can eliminate other tools through consolidation
- Policy and control mapping allows support for multiple methodologies / frameworks
- Common use of one tool fosters common language and forces single data set



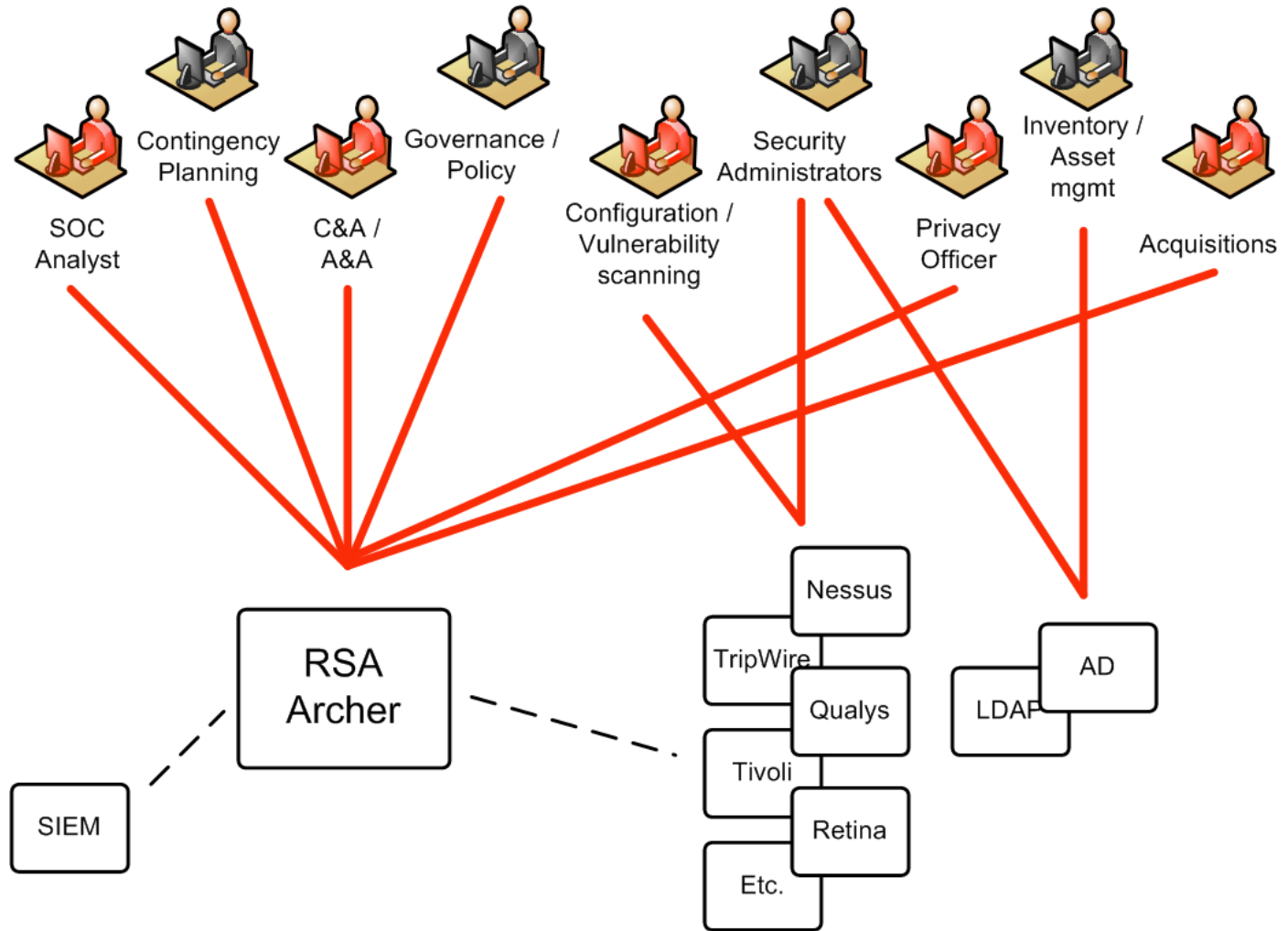
Different people, different tools

- Where are they getting data ?
- Where are they putting it?



Different people, different tools

- Where are they getting data ?
- Where are they putting it?



Archer Solutions – Resources

- Leverage more, duplicate less
- Work from a common set of data, enforce data integrity
- Guaranteed common format / interoperability



Archer Solutions – Resources

- Reduce cost/number of licenses
- Reduce training cost and burden
- Fewer accounts to manage, less attack surface
- Modular nature means buy as you need / can afford



Archer Solutions – Resources

- Streamlining A&A workflow and consolidating data and processes in one tool translates to fewer labor hours
- This allows for Continuous Monitoring assessment of more controls, more often, with same staff (in light of budget and hiring constraints/ CR /Sequester)



Archer Solutions – Risk Insight

- Correlates multiple risk scores and risk factors across enterprise and IA Program for comprehensive risk picture
- Highlights which hosts and which failed controls introduce most risk for rapid, “worst first” resolution



Demo: A&A and CM Solutions

Questions?

chris.hoover@rsa.com

Upcoming RSA Events

- **RSA Roundtable Series: Defend with Confidence Against Advanced Threats**

Register Now & View 9-City Event Schedule

<https://community.emc.com/docs/DOC-21675>

- **RSA Archer GRC Summit 2013 – Washington, D.C., June 12-14**

Register Now:

<https://community.emc.com/docs/DOC-21919>



THANK YOU

chris.hoover@rsa.com