
# Federal Contingency Planning with RSA Archer Business Continuity Management

Patrick Potter & Chris Hoover
GRC Strategists, RSA
February 6, 2014

# 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

- Patrick Potter, GRC Strategist
  - 20 years as BCM practitioner and consultant
- Chris Hoover, GRC Strategist
  - 15 years in federal Information Assurance
  - SME driving federal solution offerings for RSA Archer

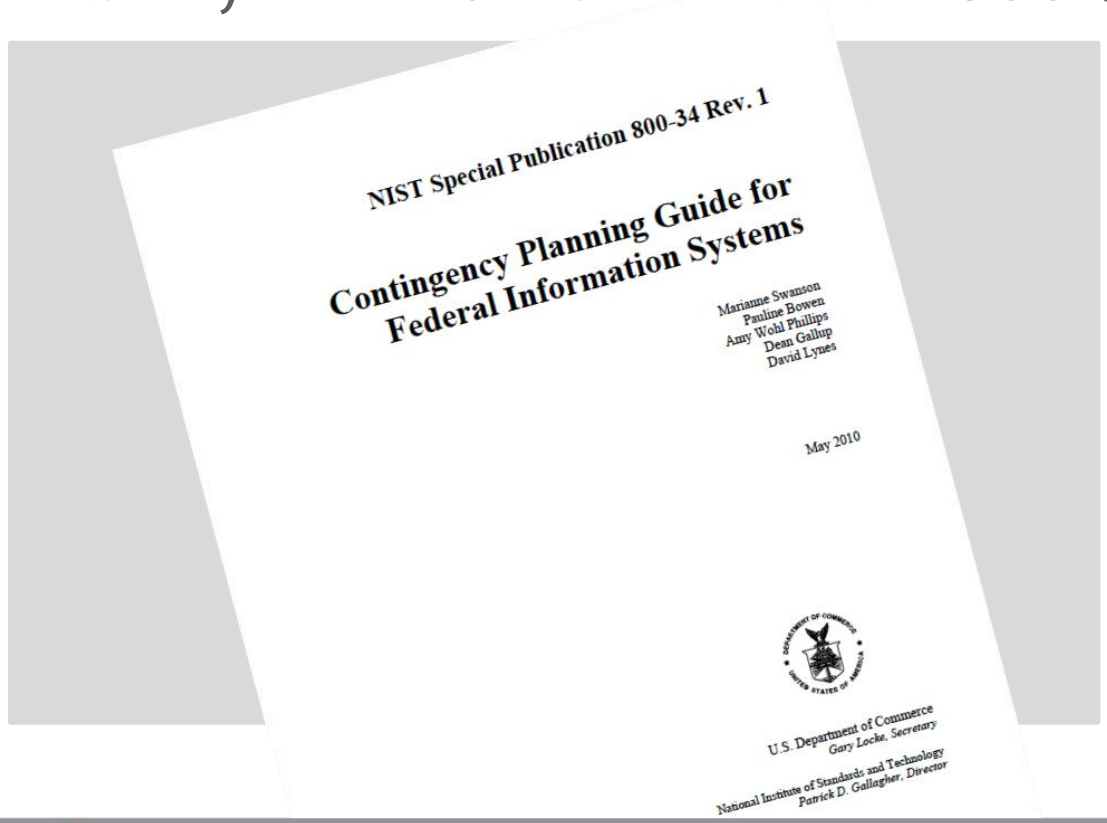
# Contingency Planning

Coordinated strategy involving plans, procedures, and measures to enable the recovery of information systems, to continue or resume operations and data after a disruption. May include:

- Restoring information systems using alternate equipment
- Performing some/all of the affected business processes using alternate processing (manual) means (typically for short-term disruptions)
- Recovering information systems operations at an alternate location (for long–term disruptions)
- Implementing of appropriate contingency planning controls based on the information system's security impact level

# Contingency Planning

- Primary CP guidance: NIST SP 800-34
- CP family of controls in NIST SP 800-53




| Control Number | Control Name |
|---|---|
| CP-1 | Contingency Planning Policy and Procedures |
| CP-2 | Contingency Plan |
| CP-3 | Contingency Training |
| CP-4 | Contingency Plan Testing |
| CP-5 | Withdrawn |
| CP-6 | Alternate Storage Site |
| CP-7 | Alternate Processing Site |
| CP-8 | Telecommunications Services |
| CP-9 | Information System Backup |
| CP-10 | Information System Recovery and Reconstitution |
| CP-11 | Alternate Communications Protocols |
| CP-12 | Safe Mode |
| CP-13 | Alternative Security Mechanisms |

# Resilience

- the ability to quickly adapt and recover from any known or unknown changes to the environment
- a resilient organization strives to continue mission essential functions at all times during any type of disruption

# Contingency Planning

- Develop the Contingency Planning Policy Statement
- Conduct the Business Impact Analysis (BIA)
  - Determine Business Processes and Recovery Criticality
  - Identify Resource Requirements
  - Identify System Resource Recovery Priorities
  - Identify Preventive Controls

# Create Contingency Plans

- Business Continuity Plan (BCP)
- Continuity of Operations (COOP) Plan
- Crisis Communications Plan
- Critical Infrastructure Protection (CIP) Plan
- Cyber Incident Response Plan
- Disaster Recovery Plan (DRP)
- Information System Contingency Plan (ISCP)
- Occupant Emergency Plan (OEP)

# Create Contingency Strategies

- Backup and Recovery
- Backup Methods and Offsite Storage
- Alternate Sites
- Equipment Replacement
- Cost Considerations
- Roles and Responsibilities

# Managing Plans

- Plan Testing, Training, and Exercises (TT&E)
  - Testing
  - Training
  - Exercises
  - TT&E Program Summary
- Plan Maintenance

# Activation and Notification

- Activation Criteria and Procedure
- Notification Procedures
- Outage Assessment

# Recovery and Reconstitution

- Sequence of Recovery Activities
- Recovery Procedures
- Recovery Escalation and Notification
- Reconstitution

# Other Tools

- Must buy separate modules for BIAs, Risk Assessments, BC plans, DR plans and Crisis Management
- Lacks reporting functions, must be tied to an external product like Crystal Reports
- The complexity of some reports' layout and data requirements can require a deep understanding of databases and Crystal Reports itself

# How RSA Archer Can Help

# Demo

# Integrating with Other Archer Solutions

# Integrating with Other Archer Solutions

- Assessment & Authorization (A&A)
  - A&A (C&A) team and Contingency team can share data on same platform and same DB
  - CP controls assessed and remediated here
  - Control assessor can see plans, test and exercise dates, other contingency details
  - Boundary defined in A&A allows CP activities by Information System

| Control Number | Control Name |
|---|---|
| CP-1 | Contingency Planning Policy and Procedures |
| CP-2 | Contingency Plan |
| CP-3 | Contingency Training |
| CP-4 | Contingency Plan Testing |
| CP-5 | Withdrawn |
| CP-6 | Alternate Storage Site |
| CP-7 | Alternate Processing Site |
| CP-8 | Telecommunications Services |
| CP-9 | Information System Backup |
| CP-10 | Information System Recovery and Reconstitution |
| CP-11 | Alternate Communications Protocols |
| CP-12 | Safe Mode |
| CP-13 | Alternative Security Mechanisms |

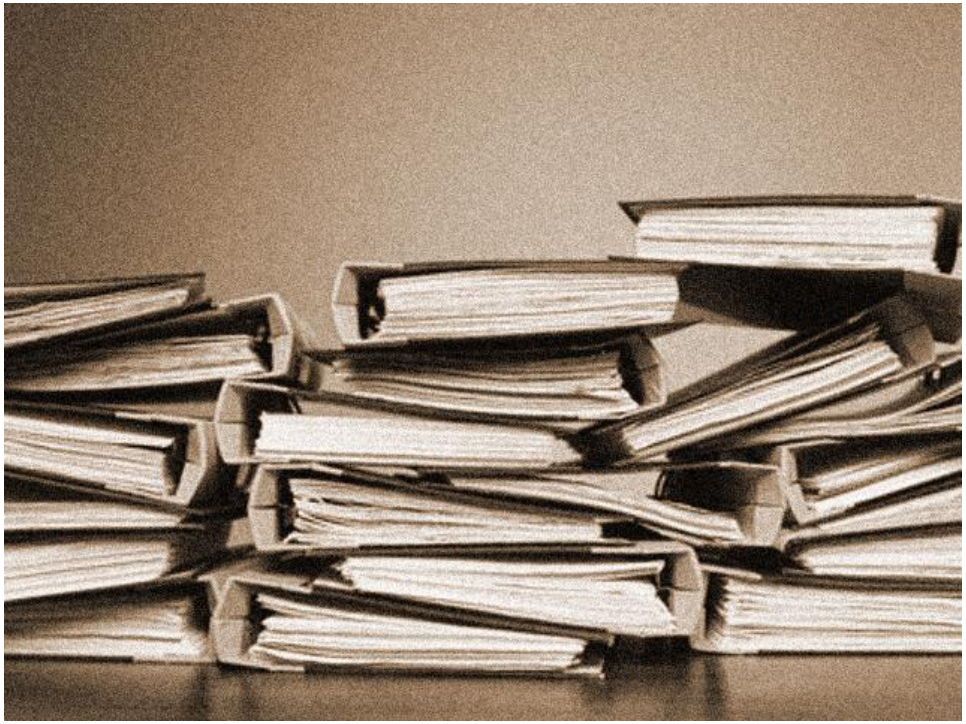
# Integrating with Other Archer Solutions

- Incident – share incident, recovery, after-action data
- Vendor – weigh vendor agreements in recovery process, supply chain management

# In ye Olden Times…

COOP plans required

DR plans required

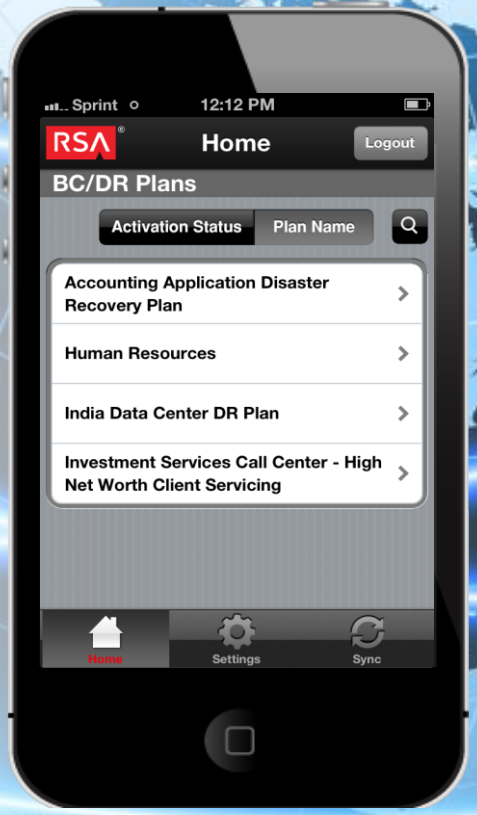


# Who Has the Binders? Protect the Binders!

# What if You Didn't Need the Binders?

# RSA Archer BCM Mobile

- BCM Mobile Application for iPhone and iPad enables users to view business continuity or disaster recovery plans and associated strategies, tasks, calling trees, and requirements
- Key technical features:
  - Secure authentication
  - Off-line availability of encrypted data
  - Click to call, email, and text functionality from the app
  - Regular data synchronization
  - URI convenience



# Summary

- All in one solution combines BC, DR and CM
- Use Archer to link your CP processes with other security activities
- One platform enables data integration, ease of reporting and Plan printing
- Leverage mobile technologies

# Questions?

patrick.potter@rsa.com
chris.hoover@rsa.com

# Come See Us at RSA Conference 2014

- Our entire GRC Strategist team will be present.
- Stop by and say “Hi”, we are in the center booth of the expo
- Details and registration at: www.rsaconference.com
- February 24-28, 2014
- Moscone Center – San Francisco, CA

# Come See Us at CPM East

- Patrick Potter will be speaking May 13
- RSA Archer will have a booth
- May 13 – 14
- Walter E Washington Convention Center – Washington DC

# Upcoming RSA Archer Events & Webcasts

- RSA Archer GRC Summit: June 10-12 in Phoenix, AZ
- 2/13 @ 11am EST: Third Party Supply Chain Risk Mgmt.
- Register on the RSA public website or Archer Community
  http://www.emc.com/campaign/global/rsa/rsa-webcast.htm
- Webcast **replays** are available on same public website

# THANK YOU

patrick.potter@rsa.com
chris.hoover@rsa.com