



RSA Archer Compliance Management 5.2 Webcast

Marshall Toburen

eGRC Risk Solutions Manager – RSA Archer

Agenda

- Introductory Comments
- 5.2 Enhancements Overview
- RSA Archer approach to Compliance Management
- Positive Outcomes
- Demonstration
- Q&A

Introductory Comments

- Newest version of Compliance Management solution became available on February 2 along with enhanced versions of Audit, Risk and Enterprise Management solutions
 - Existing, licensed customers can obtain the packages and install guides directly from the Archer Exchange
 - Upgrades will also be reflected in the 5.2 solution master
 - Updated Compliance Management Practitioner's Guide on the Exchange
- To fully benefit from Compliance Management solution, we recommend that you also utilize the Enterprise, Risk, and Policy Management solutions
- Consider requesting demonstration(s) around specific use cases

5.2 Enhancements Overview

- Enhanced configuration of the Control Procedures application to enable enhanced categorization and testing of internal controls
- Introduced cost to control
- Financial Close Management Checklist
- Developed Quarterly Financial Certification Questionnaires targeting the Business Hierarchy in the Enterprise Management solution
- Enabled Key Control Indicator Monitoring via Risk Management Solution
- Established a mechanism to capture relevant, point in time, compliance information to build and report on historical compliance data
- Various cosmetic changes

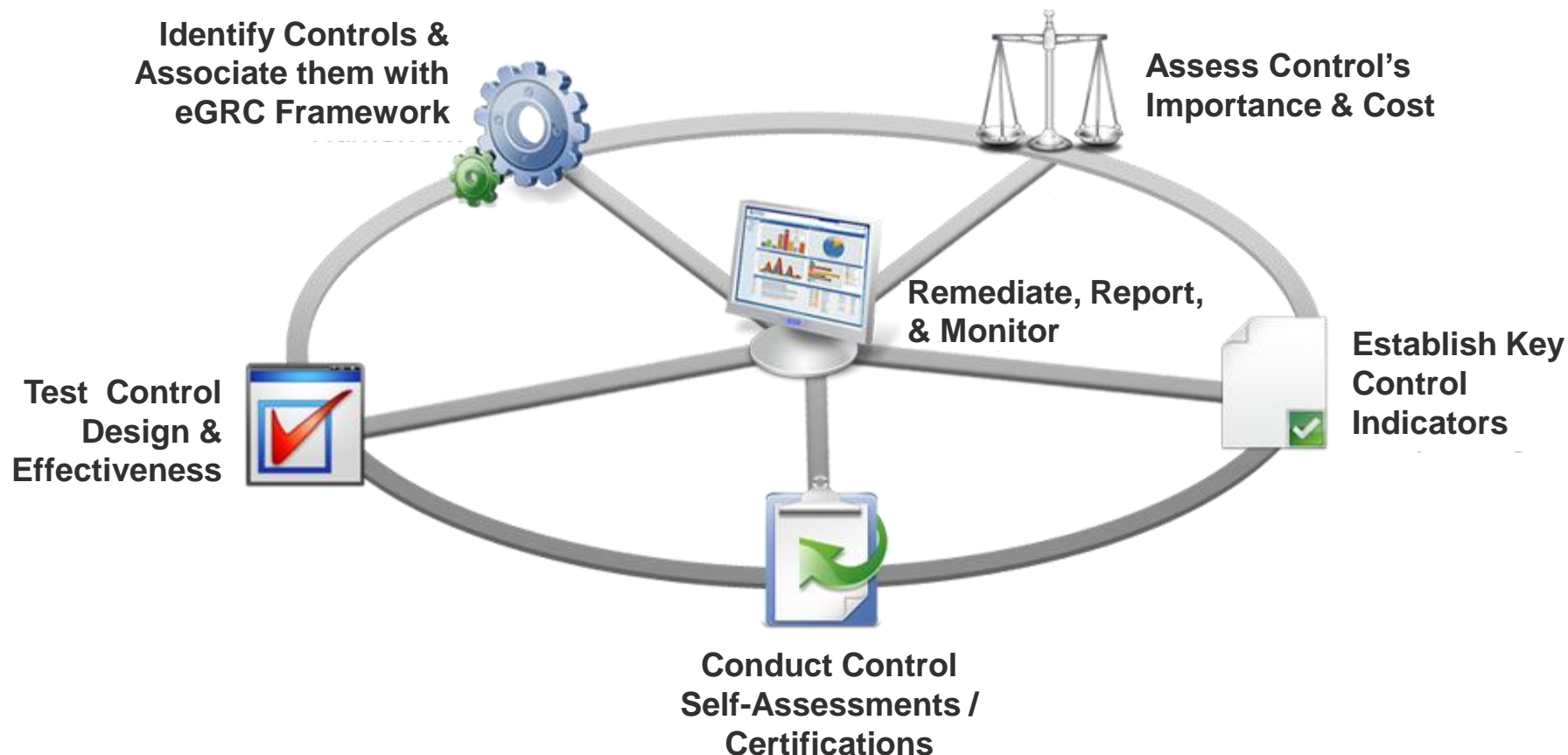
Controls & Compliance

- Internal Control – it's about managing risk to achieve objectives
 - Fines & sanctions from regulatory non-compliance
 - Litigation from product liability, human resources, and business operations
 - Losses from errors & fraud associated with people, process, technology
 - Brand reputation
 - Losses from extending credit or losing assets managed by 3rd parties
 - Insufficient liquidity to meet obligations
 - Charges from adverse change in markets and interest rates
 - Risk of not executing on strategy
- By compliance we mean control assurance, and compliance with policy, procedure, and authoritative sources
- Common Use Cases: Demonstrating Compliance with Specific Regulations, Financial Reporting Obligations, ERM / Performance Management

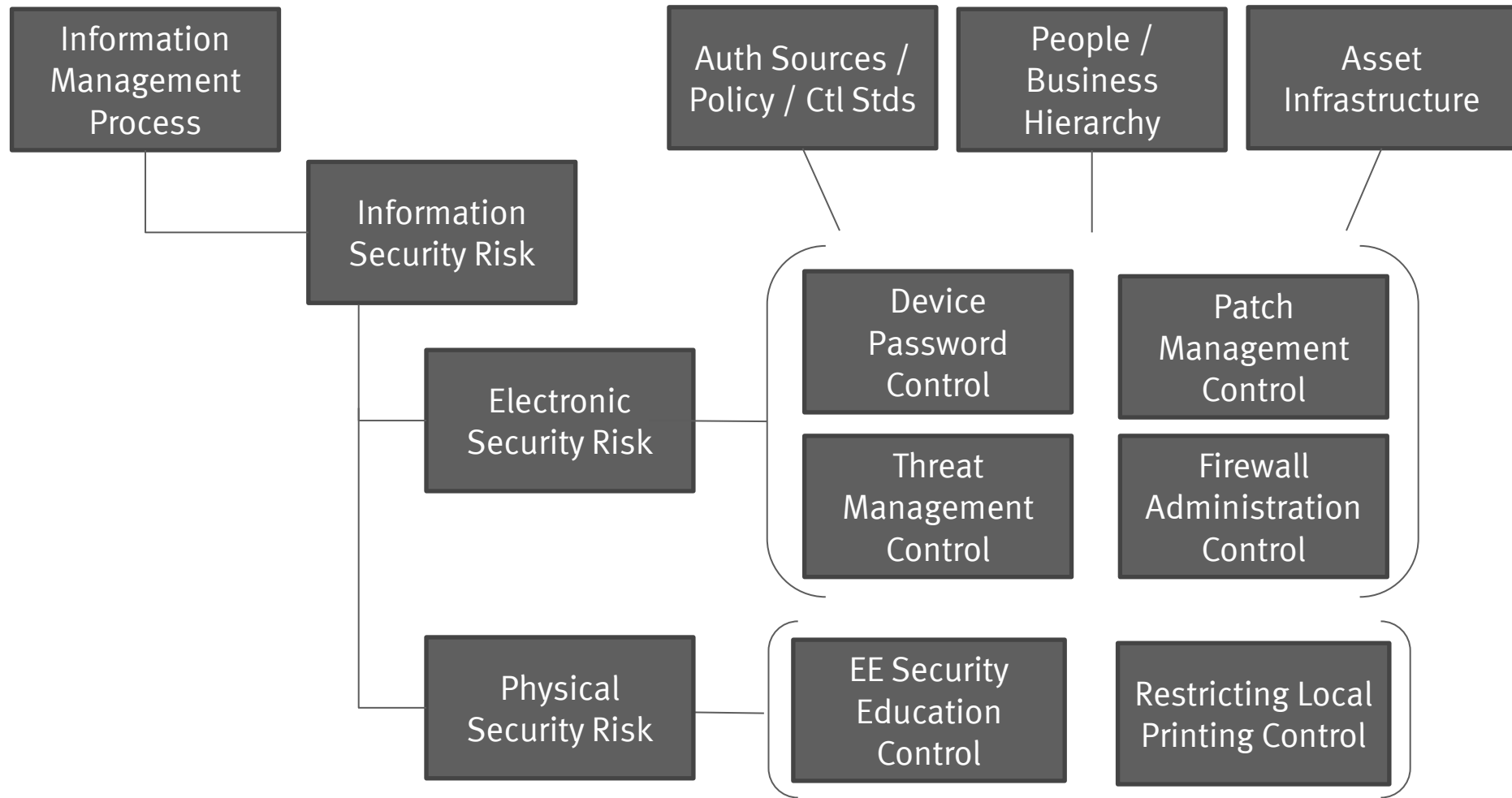
Compliance Challenges

- Knowing where all the controls are & should be
- Failure to focus on controls commensurate with their risk
- Significant cost to demonstrate compliance
 - Redundant focus on controls that mitigate multiple regulations/risks
 - Manual testing is laborious, expensive, and incomplete
 - Connecting the dots is time consuming and expensive
- Managing compliance with multiple regulations
- Coordination with other assurance functions
- Resource limitations
- Testing processes are inconsistent
- Exception reporting, remediation, and tracking
- Satisfying high profile stakeholders

RSA Archer Approach to Compliance Management

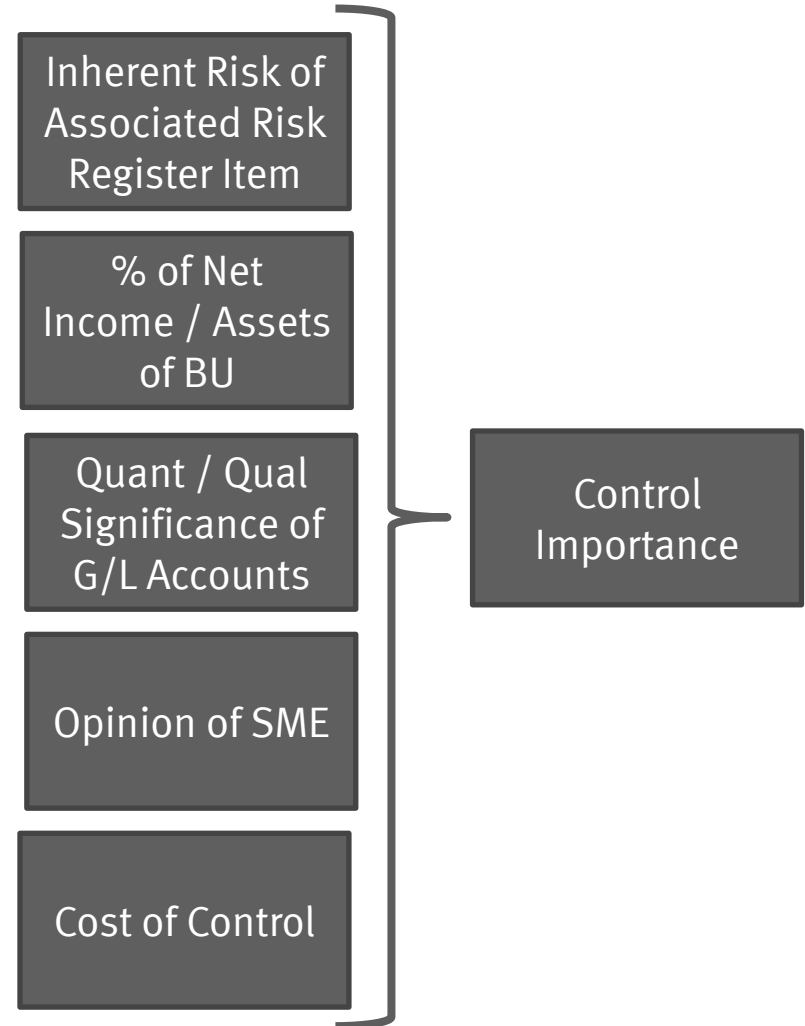


Document Controls & Associate them with GRC/ERM Framework



Assess Importance & Cost of the Control

- Risk-based Scoping of Controls is established in context of
 - Inherent Amount of Risk being Mitigated
 - Financial Significance of the Business Unit, Process
 - Quantitative & Qualitative Significance of associated G/L Accounts
 - Subjective opinion of assessor
- Estimate the cost of control(s) to compare with inherent risk
- Cull out controls that are not significant or cost more than the inherent risk they mitigate
- Scope tests based on significance



Establish Key Control Indicators

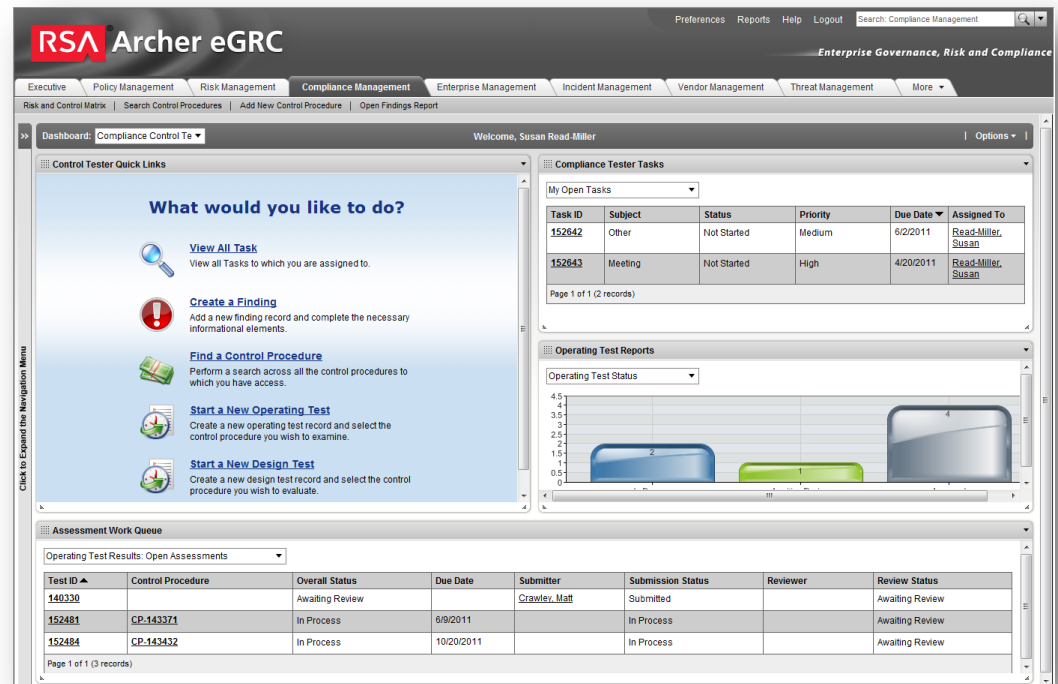
- Metrics documented in the Risk Management Solution can target control procedures
- Continuous control monitoring
- Automated feeds around IT technical assets

Conduct Assessments / Assertions

- Control Self-Assessments
- Financial Close Checklist - Assess the activities performed in the financial close process to ensure all required steps have been completed
- Quarterly Certifications
- Technical Control Manual Assessments
- Integration with scanning tools such as Qualys, McAfee, iSIGHT, etc.
- 36 Questionnaires; > 15,000 Questions

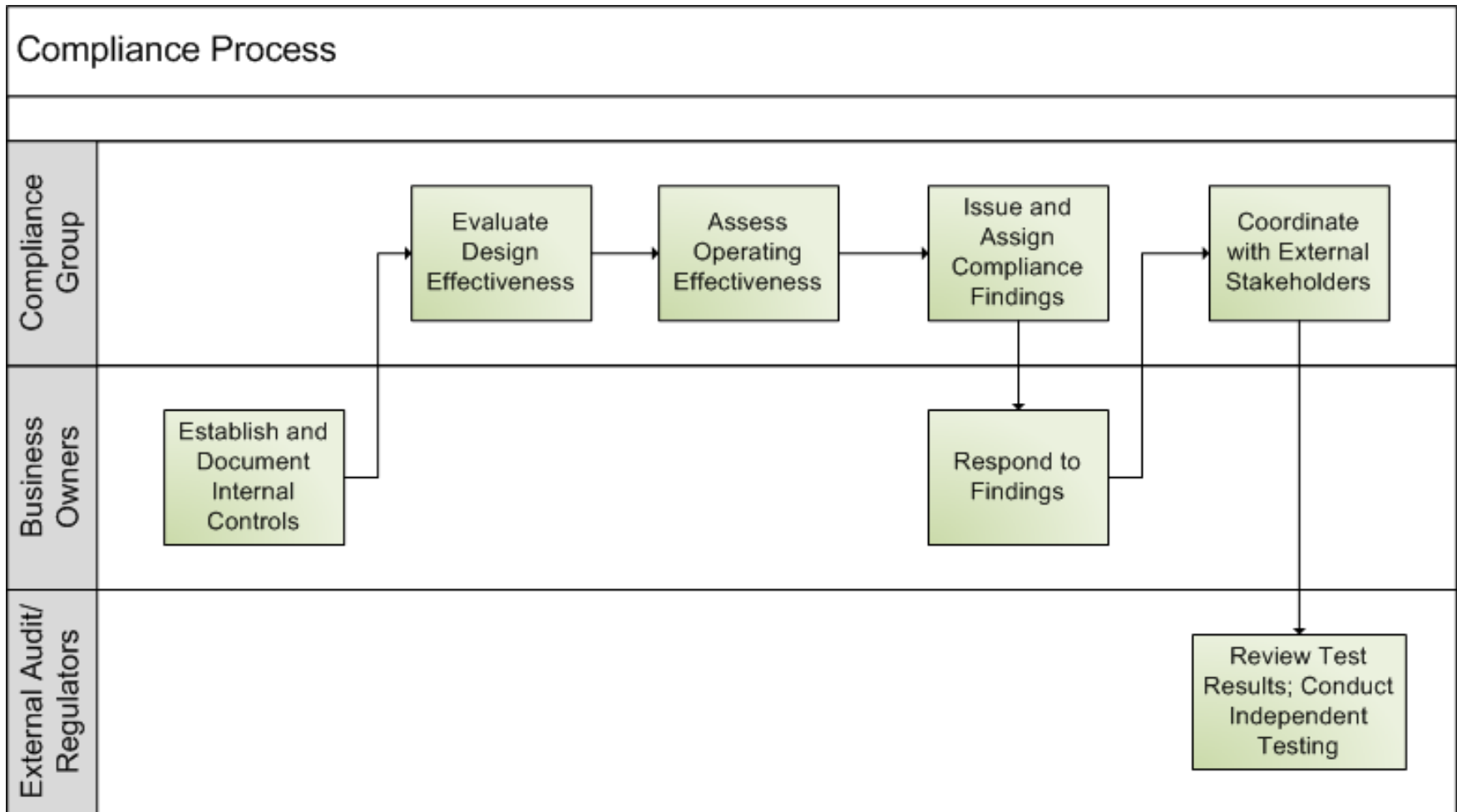
Execute Design and Operating Tests

- Assess whether design tests will mitigate the risk as intended
- Inform testers of their work queues via rules-driven workflow and “My Tasks” lists
- Execute operating tests to identify if the control is working as designed



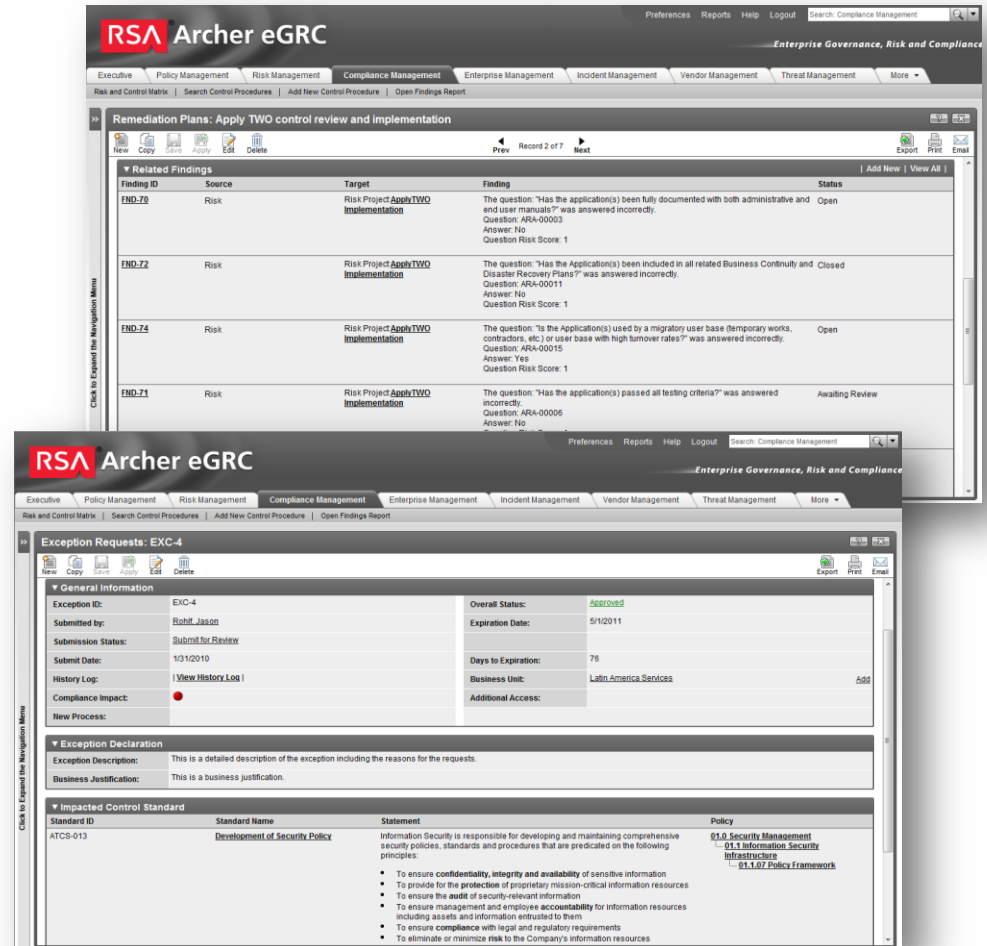
RSA Archer Compliance Control Tester Dashboard

Test Design & Operating Effectiveness

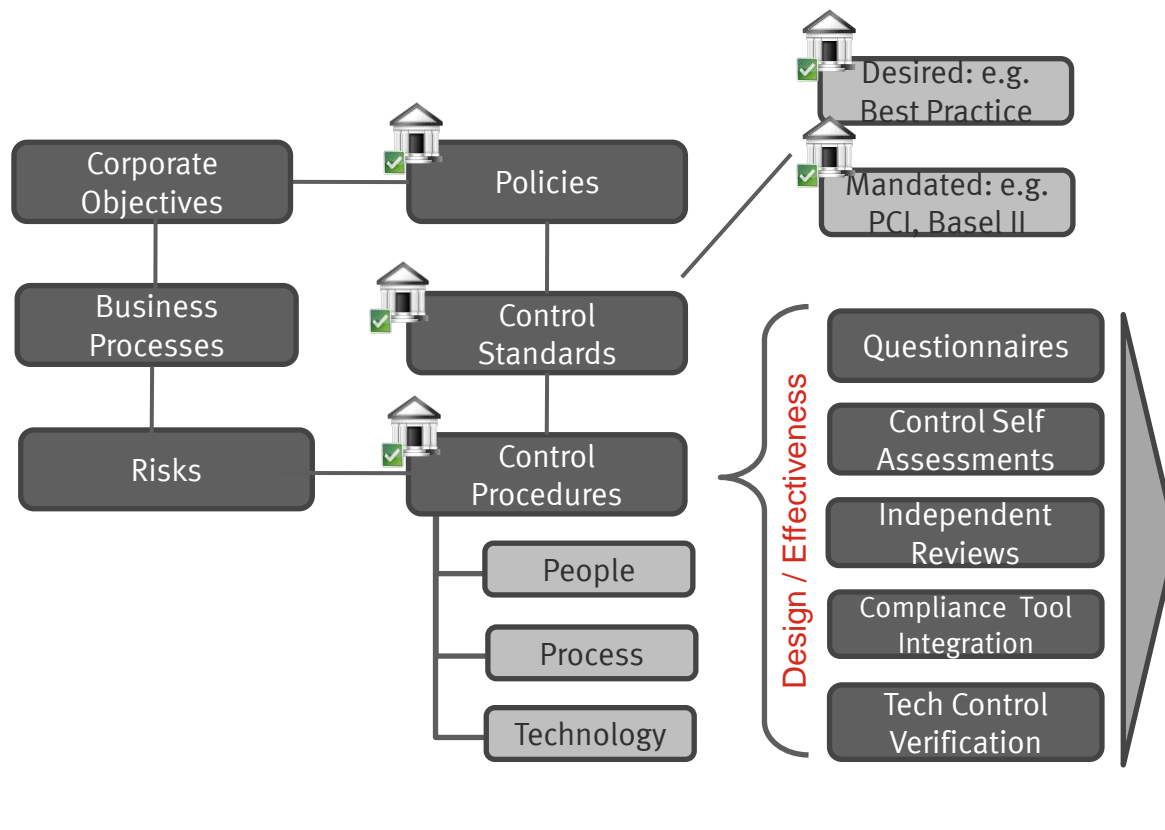


Maintain Continuous Controls Monitoring

- Auto-generate deficiencies based on failures noted within questionnaires and test results
- Understand how findings relate to controls, operating entities, policies, regulations and risk
- Relate multiple findings in a context of a remediation plan to identify larger issues and support informed decision making



Compliance Management Reporting



Answers

- Risks w/o Controls
- Regulations w/o controls
- Standards w/o controls
- Most important controls
- Controls not well designed or operating
- Who is responsible
- When problems are going to be resolved

Respond to Deficiencies

The screenshot displays the RSA Archer eGRC interface, specifically the 'Findings: FND-1' and 'Exception Requests' sections.

Findings: FND-1

General Information	
Finding ID:	FND-1
Status:	Closed
Category:	General
Criticality:	Low
Year:	2011
Date Closed:	2/10/2011
Target:	Applications Customer Service Center
Questionnaire:	
Authoritative Source References:	
Control Standards:	Access Control Features
Source:	Compliance
Source Override:	Compliance

Workflow and Description

Workflow	
Assigned to:	Kamer, Mason
Reviewer:	Lemon, David
Submission Status:	Submitted
Review Status:	Approved

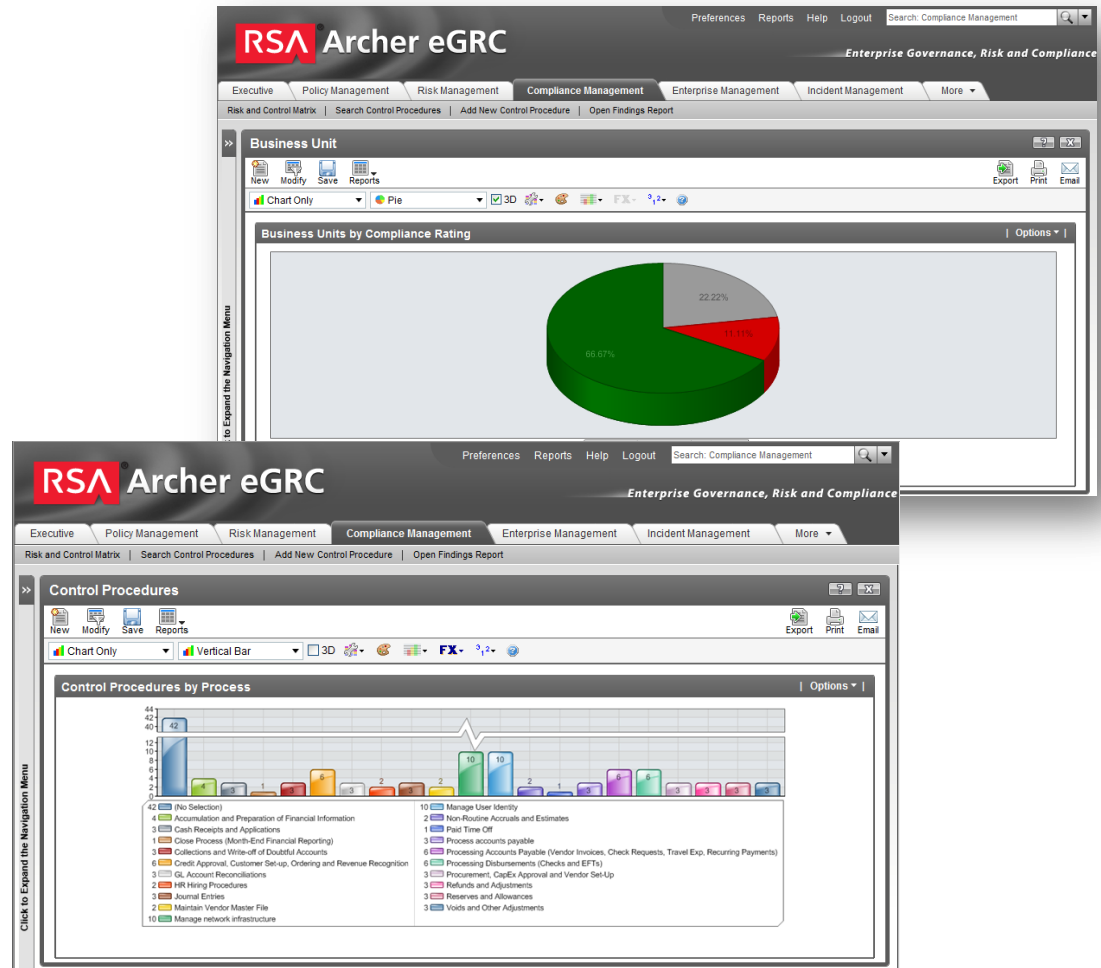
Exception Requests

Exception ID	Overall Status	Exception Description	Impacted Control Standard	Submit Date
EXC-1	Expired	Mainframe system does not have a login mechanism for reporting of failed login attempts. Cannot comply with this standard.	Access Control Features	2/8/2011
EXC-2	Approved	I have vendors that need access computing facility.	Challenging Individuals Not Displaying Access Badges	1/19/2011
EXC-3	Approved	Department has not received information regarding the Acceptable Use Policy. Request waiver until this information has been received.	Acceptance of Technology	1/21/2010
EXC-4	Approved	This is a detailed description of the exception including the reasons for the requests.	Development of Security Policy	1/31/2010
EXC-5	In Review	Password length for application ABCXYZ does not support an 8 character length due to vendor restrictions.	Password Strength Requirements	2/10/2010
EXC-6	In Review	Command line access is required for administration tasks.	Command line access	2/20/2010
EXC-7	In Management Review	Mainframe system does not have a login mechanism for reporting of failed login attempts. Cannot comply with this standard.	Failed Login Attempts	3/2/2010
EXC-8	Approved	Mainframe system does not have a login mechanism for reporting of failed login attempts. Cannot comply with this standard.	Access Control Features	3/12/2010
EXC-9	Approved	I have vendors that need access computing facility.	Challenging Individuals Not Displaying Access Badges	3/22/2010
EXC-10	Approved	Department has not received information regarding the Acceptable Use Policy. Request	Acceptance of Technology	4/1/2010

- Employ automated workflow and task management capabilities to resolve compliance deficiencies
- Route findings and tasks to appropriate personnel
- Complete remediation tasks or log exception requests that identify effective compensating controls
- Review and approve the resolution of deficiencies using the pre-built, fully configurable workflow processes

Report on Overall Compliance

- Use real-time reporting capabilities and dashboards to form a consolidated picture of compliance efforts and remediation
- Ad hoc reporting allows you to deliver status and alert-type reports to users through dashboards, email or exports in a number of different formats



Positive Outcomes of RSA Archer Compliance Management

- After Scenarios
 - Multiple risks & regulations are satisfied while eliminating redundant controls
 - Ability to easily incorporate new or updated regulations within existing compliance processes
 - Consistent management and approach for control testing
 - Continuous monitoring of open compliance findings and remediation plans
 - Ability to report compliance posture against key regulations across the entire organization
- Positive Business Outcomes
 - Fewer redundant and unimportant controls = less control assessments and testing activities (fewer resource hours)
 - Transparency, accountability, and improved control culture
 - Institutionalized knowledge of business operations
 - Easier ability to satisfy multiple stakeholder interests

Compliance Management Demonstration



Q & A



The Security Division of EMC

Thank you!