knowledge17

http://clabs.link/lab132022

WORK at LIGHTSPEED

Proving Compliance of Security Controls

Syra Arif
Security Solutions Architect
ServiceNow

David Perodin
Security Solutions Architect
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Introduction
- Why is Security Compliance Important?
- What You Will Learn
- Lab
- Wrap-up

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Syra Arif

Title: Solutions Architect, Security & Risk Practice

Function: Technical Overlay for Security & Risk Business Unit

Company: ServiceNow

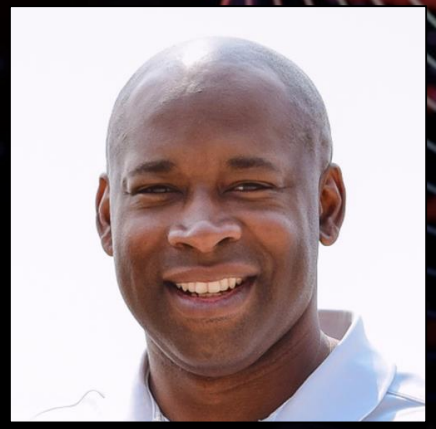
Background: Prior to ServiceNow, Syra was a part of the Archer GRC and IAM Sales Engineering Teams at RSA and worked at Cisco for 4 years supporting the service provider business with a focus on Mobile Internet Technology

Expertise: Governance, Risk & Compliance (GRC), Vulnerability Management, Security Incident Response, Identity & Access Management, 3G/4G Mobile Packet Core

Current Projects: Collaborating with ServiceNow customers on improvements to Vulnerability Response solution

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: David Perodin

Title: Security Solutions Architect

Function: Technical Overlay for Security & Risk Business Unit

Company: ServiceNow

Experience: 16 yrs. in Network Architecture & Cloud, 10 yrs. in Security (Federal and Commercial markets)

Expertise: L3-L7, Unix Administration, Full-Proxy Solutions, Security, Load-balancing, Cross-Domain tools

Achievements: Patent on cross-domain capability for F5 load-balancers

Current Projects: Developing/Managing GRC plugin to spefically handle Certification/Accrediation process within Servicenow. End Goal: Take a 2-month C&A process down to a couple of weeks or sooner.

© 2017 ServiceNow All Rights Reserved

Objectives and What You Will Learn

Objectives

- Proving Compliancy of Security Controls within your organization

What you will learn

- Understanding the need for Organizational Policy
- Become familiar with policy structure
- Policy, Policy Statement, Citations, Controls, & Indicators
- Generate/update compliance reports

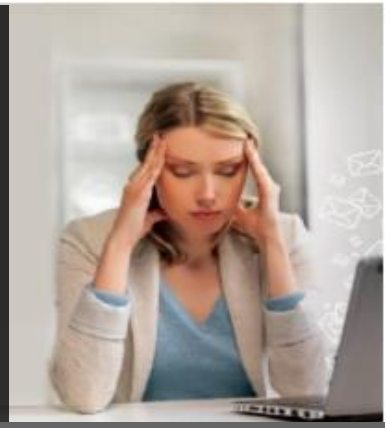
© 2017 ServiceNow All Rights Reserved

Why Are We Here?

© 2017 ServiceNow All Rights Reserved

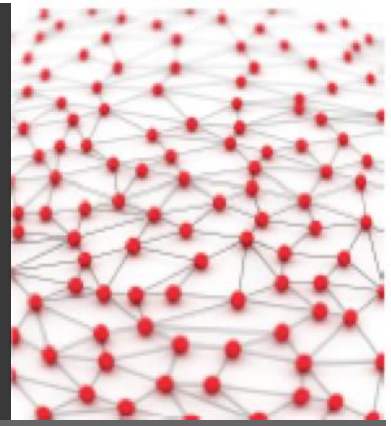
Key Challenges Keeping the CISO Awake at Night

Difficulty Providing Assurance



Evidence of control activities are performed so inconsistently across our organization that it's nearly impossible to make it through an audit without major findings.

Redundant Processes and Systems



Our risk and compliance processes are reactive and inefficient. As a result, we end up assessing the same business areas multiple times, while completely missing other high-risk areas.

Inadequate Security Control



So much of our effort is spent on regulatory risk management that we fail to monitor controls that mitigate other high impact and emerging risks.

© 2017 ServiceNow All Rights Reserved

ServiceNow and Governance, Risk, and Compliance

Why GRC, Why ServiceNow

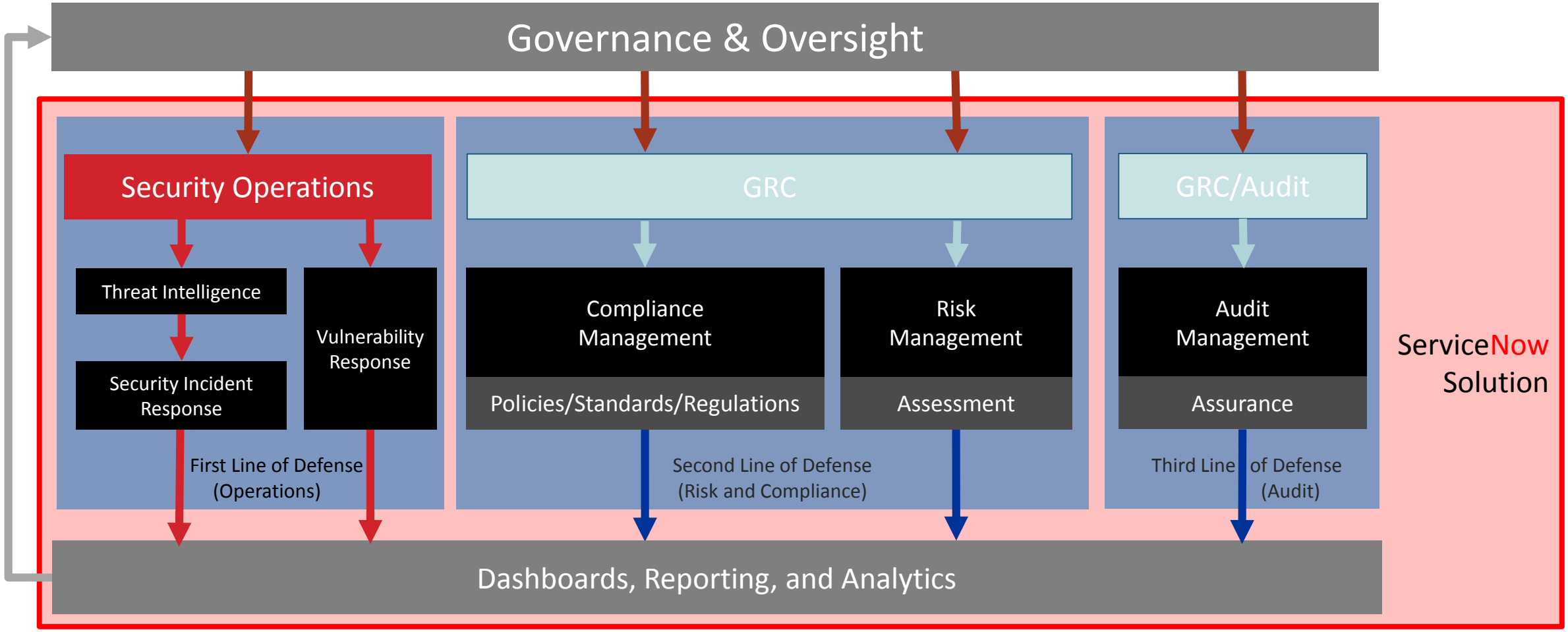
- Governance, Risk and Compliance has become increasingly important as organizations drive to **ensure the compliance** and **mitigate operational risk**.
- The **discipline** has become even **more prevalent** in the last few years due to **increased regulation** across financial, medical, and publicly traded organizations.
- Organizations are held **accountable for accuracy and integrity** in their business operations and they must have effective and reliable governance and compliance procedures in place
- Organizations **manage compliance** using expensive tools, or more commonly, as a **manual process** with documents, spreadsheets, and email.
- With ServiceNow's GRC application, organizations can **proactively manage** by **aligning those controls** with departmental and corporate policies.
- By **automating the collection of testing evidence** and reporting, GRC strengthens an organization's position during external audits, reducing compliance reporting costs and improving the ability to manage risks.

© 2017 ServiceNow All Rights Reserved

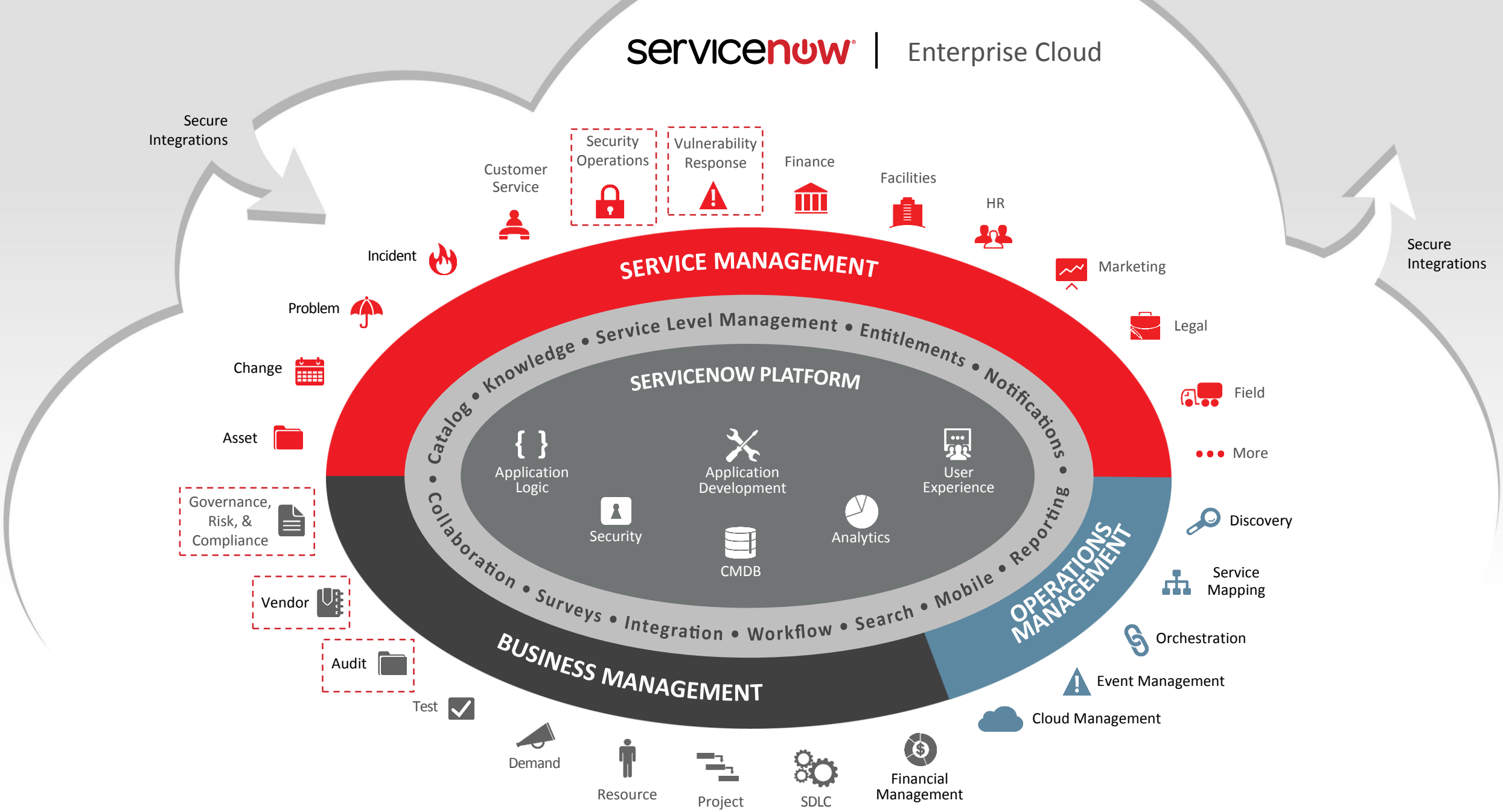
ServiceNow GRC + SecOps, Better Together

© 2017 ServiceNow All Rights Reserved

GRC, Security Incident, Vulnerability: The ServiceNow Solution



© 2017 ServiceNow All Rights Reserved


servicenow | Enterprise Cloud
Secure Integrations
Secure Integrations
Customer Service
Security Operations
Vulnerability Response
Finance
Facilities
HR
Incident
Problem
Change
Asset
Governance, Risk, & Compliance
Vendor
Audit
Test
Marketing
Legal
Field
More
Discovery
Service Mapping
Orchestration
Event Management
Cloud Management
SERVICE MANAGEMENT
Catalog • Knowledge • Service Level Management • Entitlements • Notifications •
SERVICENOW PLATFORM
Application Logic
Application Development
User Experience
Security
CMDB
Analytics
• Collaboration • Surveys • Integration • Workflow • Search • Mobile • Reporting
BUSINESS MANAGEMENT
OPERATIONS MANAGEMENT
Demand
Resource
Project
SDLC
Financial Management
- - - - Risk Management Applications

Creating Policies & Associating Policy Statements

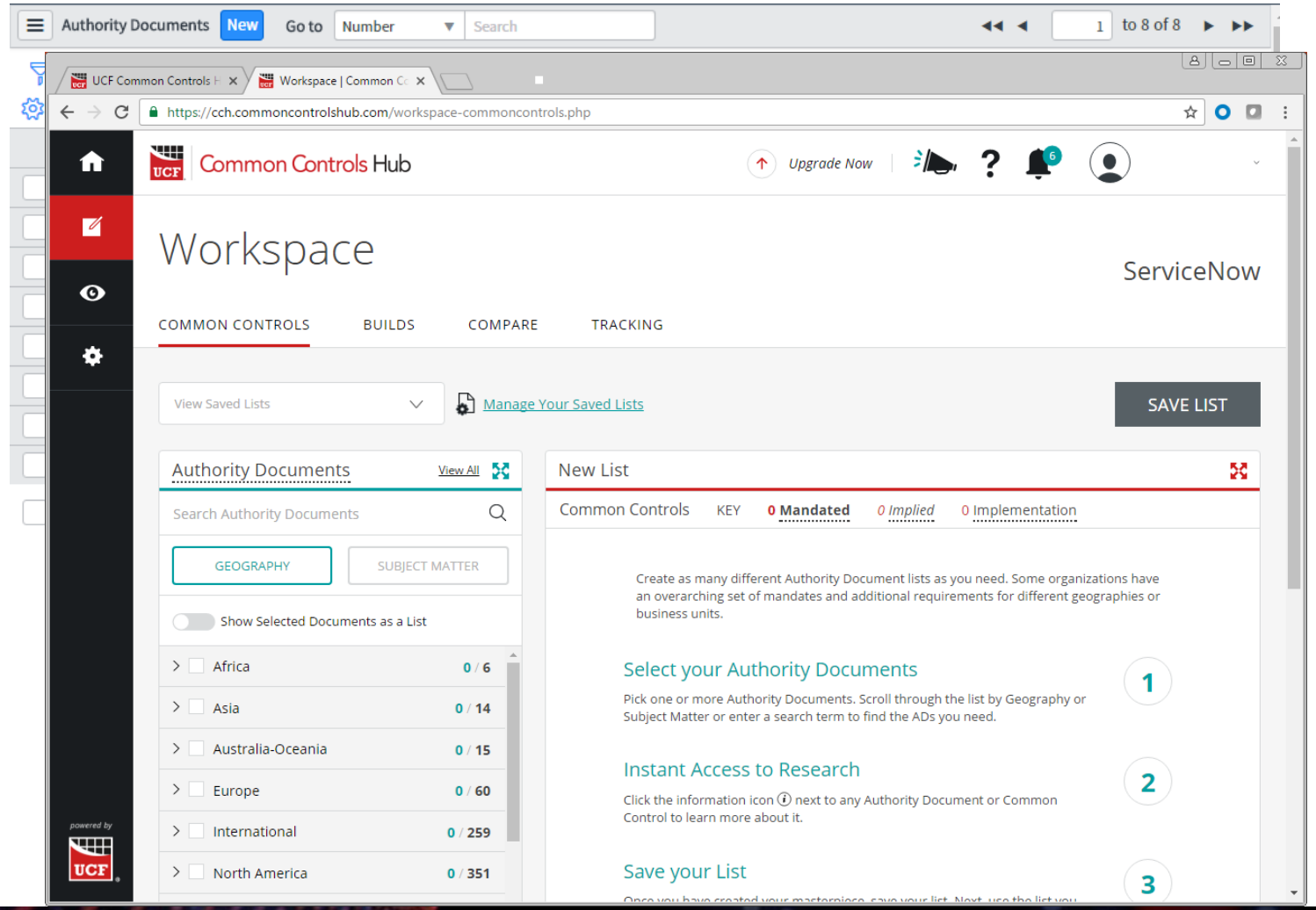
Task 1

© 2017 ServiceNow All Rights Reserved

GRC – Policy and Compliance Management

Authoritative Document Management

- Keep Regulations, Standards, and Frameworks in one place
- Cross-Reference and Rationalize your controls framework
- Enable a “test once, comply with many” control test approach
- Map citations from various documents to Policy Statements
- *Functional Change in Istanbul*
- Documents may be imported for the *Unified Compliance Framework* through the *Common Control Hub (CCH).*
  - *A client subscription to the UCF content is required.*
  - *UCF Interface is where the UCF content is managed.*
  - *Link to CCH: https://commoncontrolshub.com/*

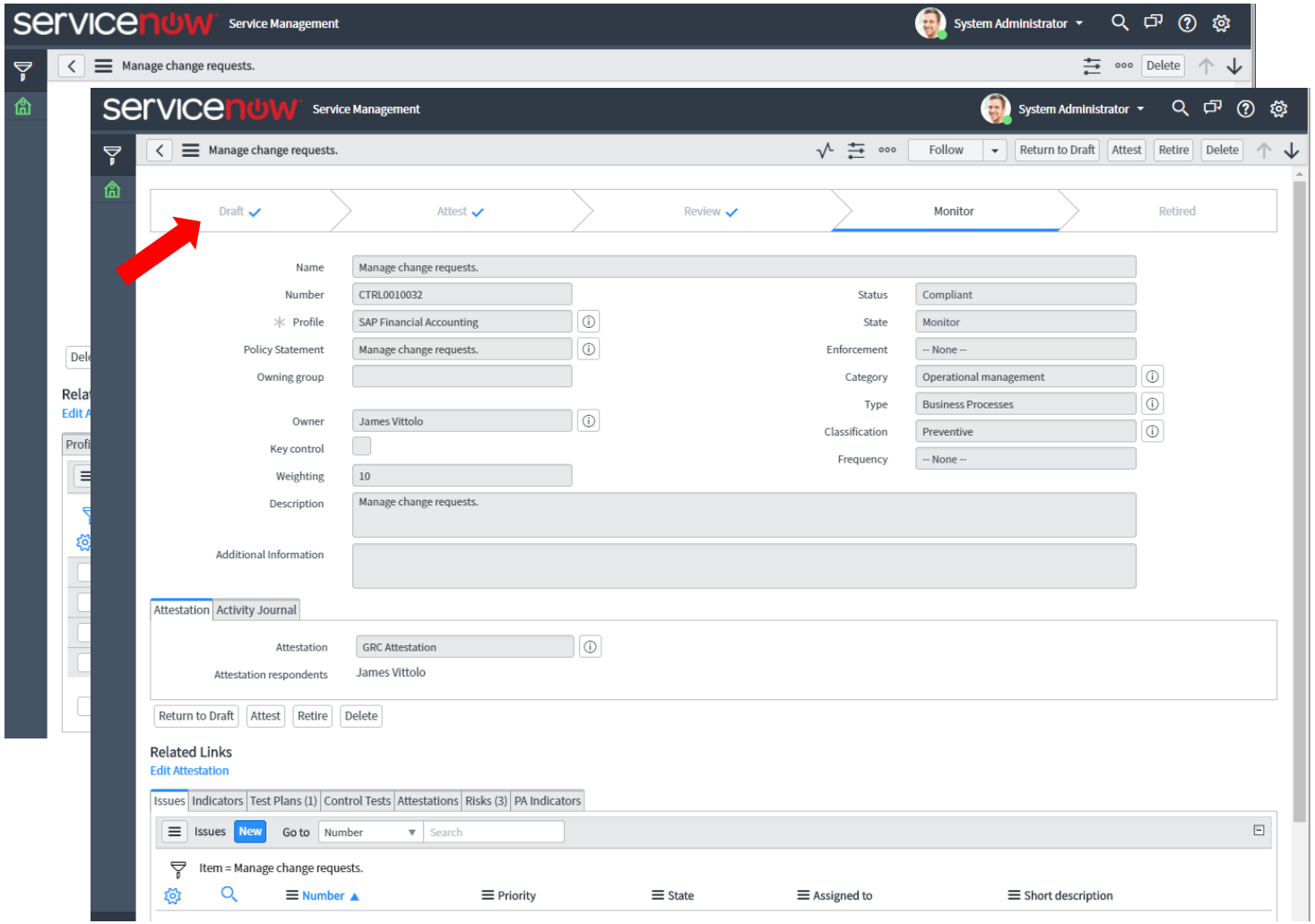


© 2017 ServiceNow All Rights Reserved

GRC – Policy and Compliance Management

Policy Statements & Controls

- A Policy Statement is the control to be measured and assigned.
- Authoritative Citations are mapped to the Policy Statements
- Attestations can be assigned at the Policy Statement level.
- Indicators are a form of self testing.
  - Indicator Templates are defined in the Policy Statement
- A Control is created when a Policy Statement is mapped to a Profile.
- Controls have a process flow that can be linked to defined workflow.
- Indicators can be assigned for individual controls

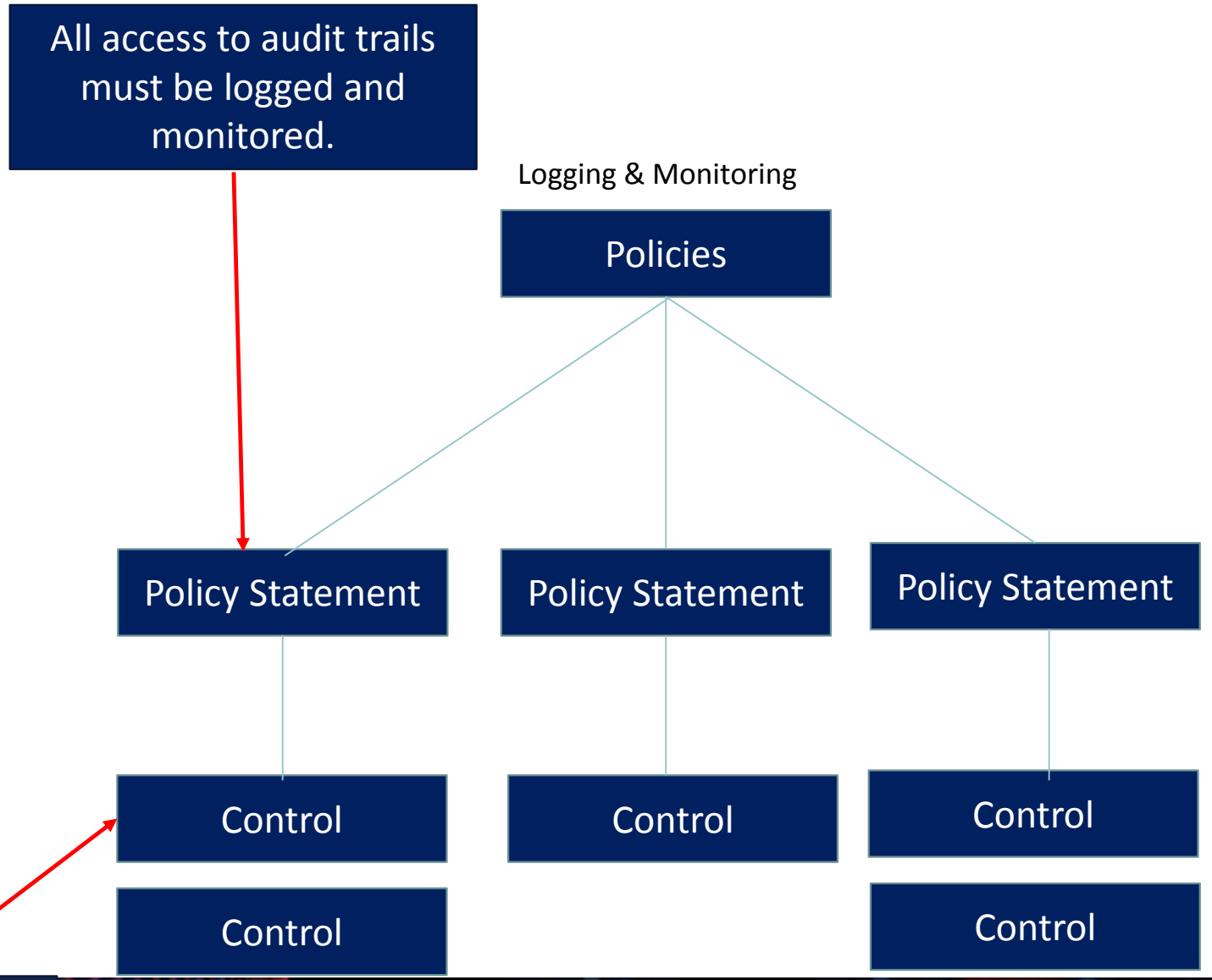


© 2017 ServiceNow All Rights Reserved

ServiceNow GRC

Policy & Compliance Management

- Policies are managed through the full lifecycle
- Policy statements can be thought of as control templates
- When a policy statement is applied to a profile, controls are generated and can be assessed and continuously monitored for compliance

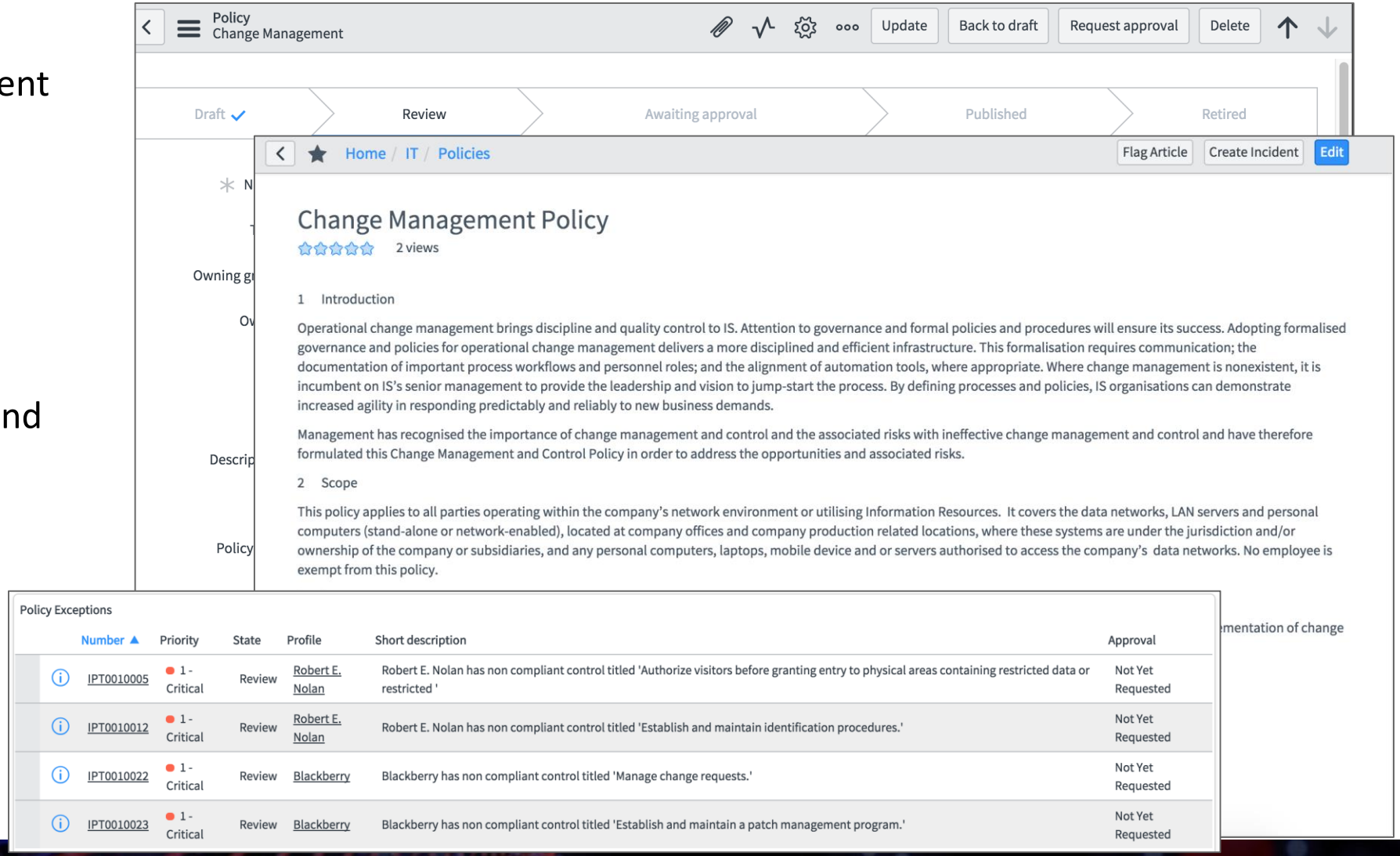


© 2017 ServiceNow All Rights Reserved

Task 1: Establish

Policy Lifecycle Management

- Integrated Policy Management Workflow
- Automated Review and Approval Process
- Publish Policies to the Knowledge Base
- Automated Policy Scoping and Control Creation
- Policy Exception Handling



© 2017 ServiceNow All Rights Reserved

Managing Profile Types & Profiles

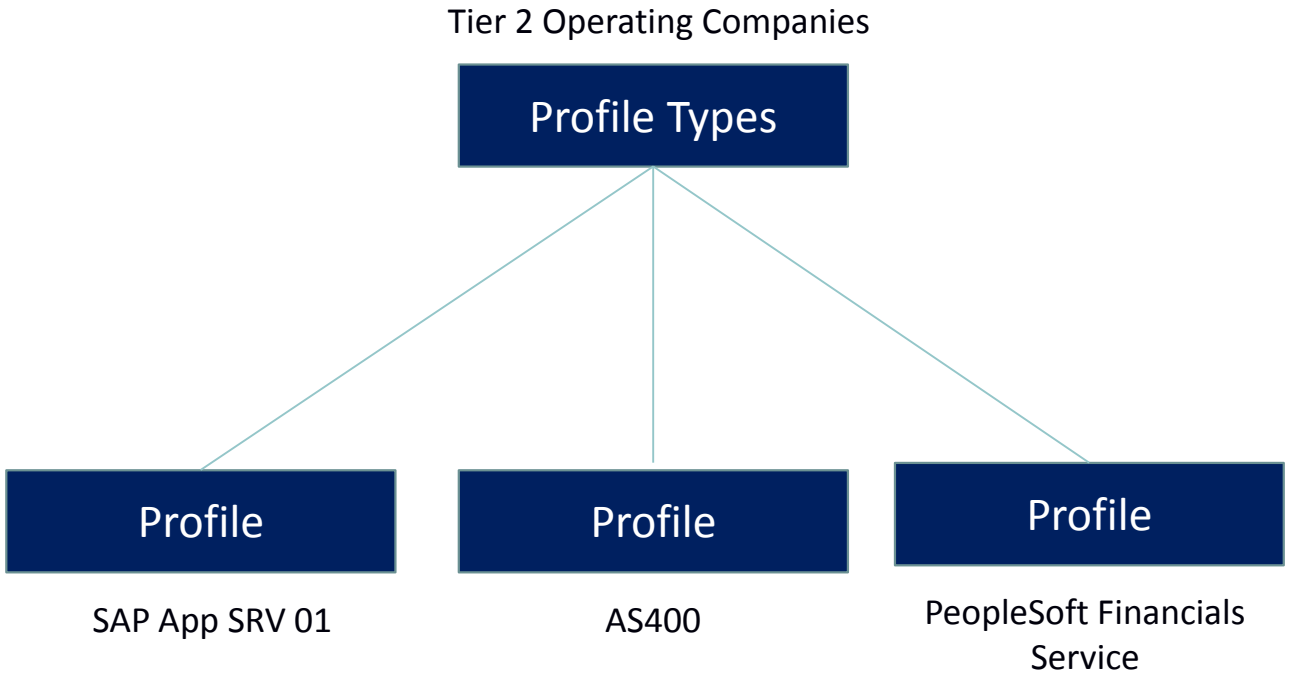
Task 2

© 2017 ServiceNow All Rights Reserved

ServiceNow GRC

Profiles & Profile Types

- Profiles are used for scoping which entities a risk, control, policy applies to
- Profile Types are used to bucket multiple profiles, making it easier to apply GRC elements and manage conveniently
- Profiles can be users, assets, locations, business services, or any other criteria defined in a ServiceNow table

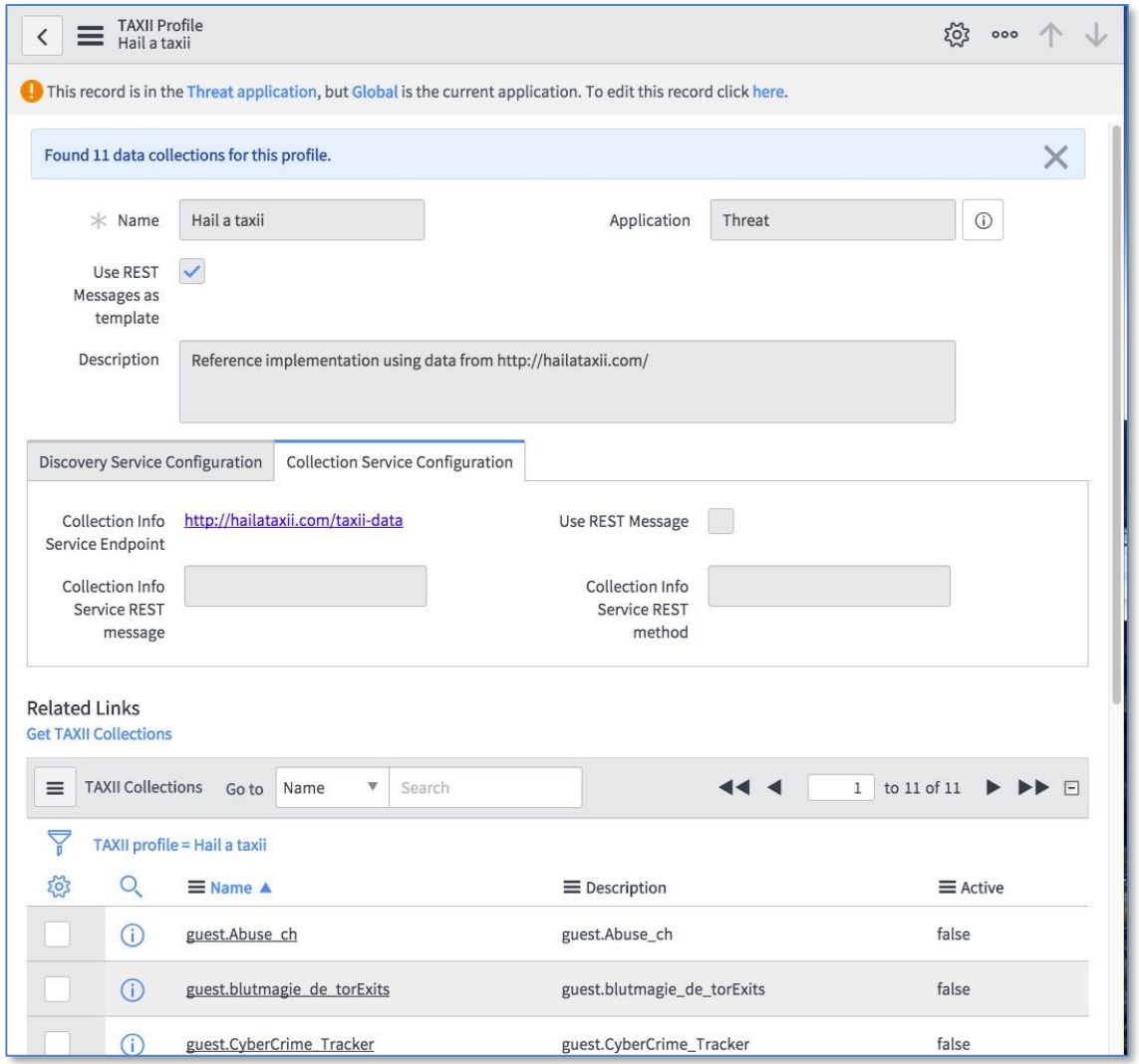


© 2017 ServiceNow All Rights Reserved

Task 2: Prevent & Detect

Threat Portal

- Support for multiple threat intelligence feeds accelerates threat identification
- Includes comprehensive catalog of Indicators of Compromise (IoC) for threat identification
- Embeds IoCs with linked incidents and systems to enabling accelerated threat detection and historical information
- Supports multiple threat feeds to automate lookups against intel databases and enrich incident context



© 2017 ServiceNow All Rights Reserved

Using Indicator Templates to Deploy Indicators for Continuous Monitoring

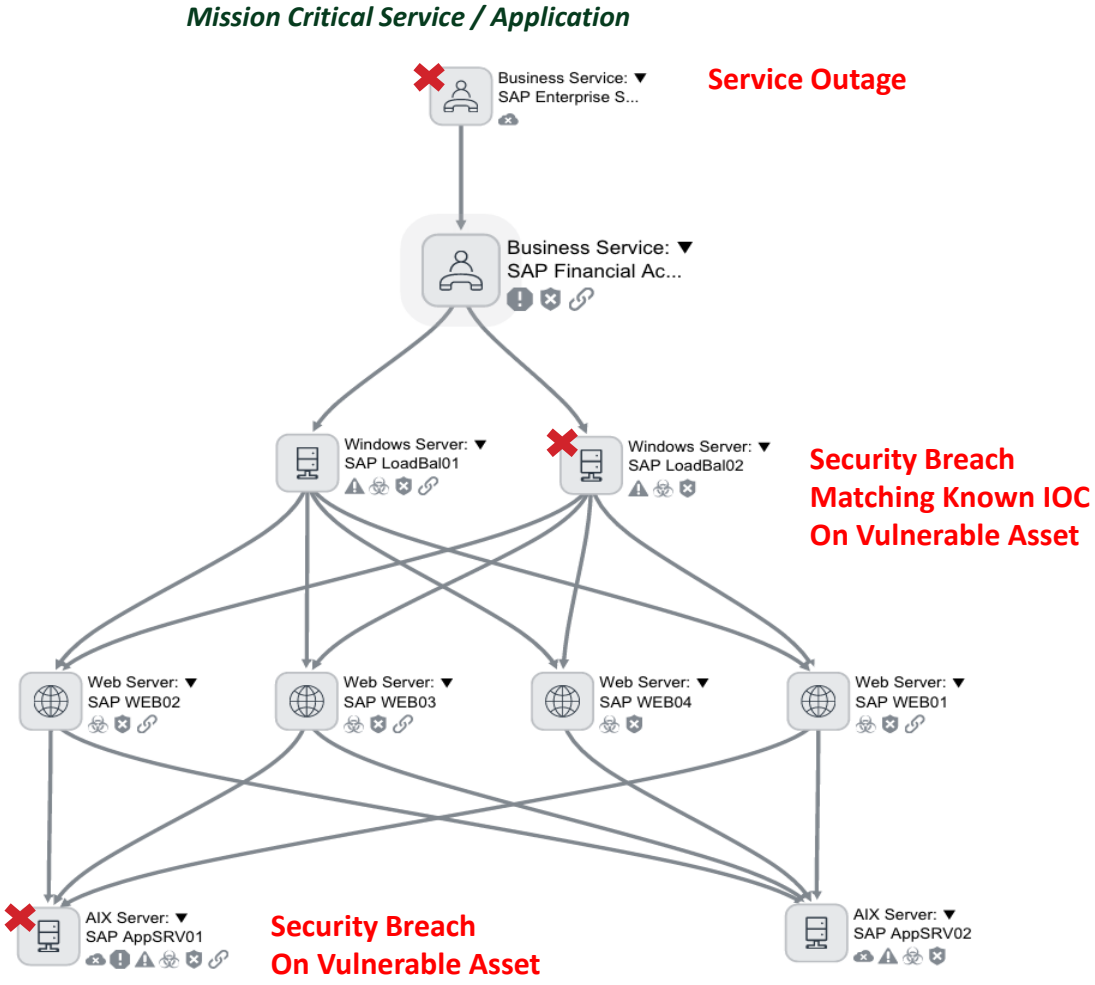
Task 3

© 2017 ServiceNow All Rights Reserved

Task 3: Respond

Security Incident Response: Understanding the Business Impact

- Provide Situational Awareness:
  - Have we seen this before?
  - What do these assets mean to the business?
  - What business risks are tied to these assets?
  - How vulnerable are these assets?
  - Is anything else is going on with these assets?
  - What are our plans?
- Open Up Communication:
  - Security Catalog
  - Virtual War Room through Connect



© 2017 ServiceNow All Rights Reserved

Executing Indicators to View Indicator Results

Task 4

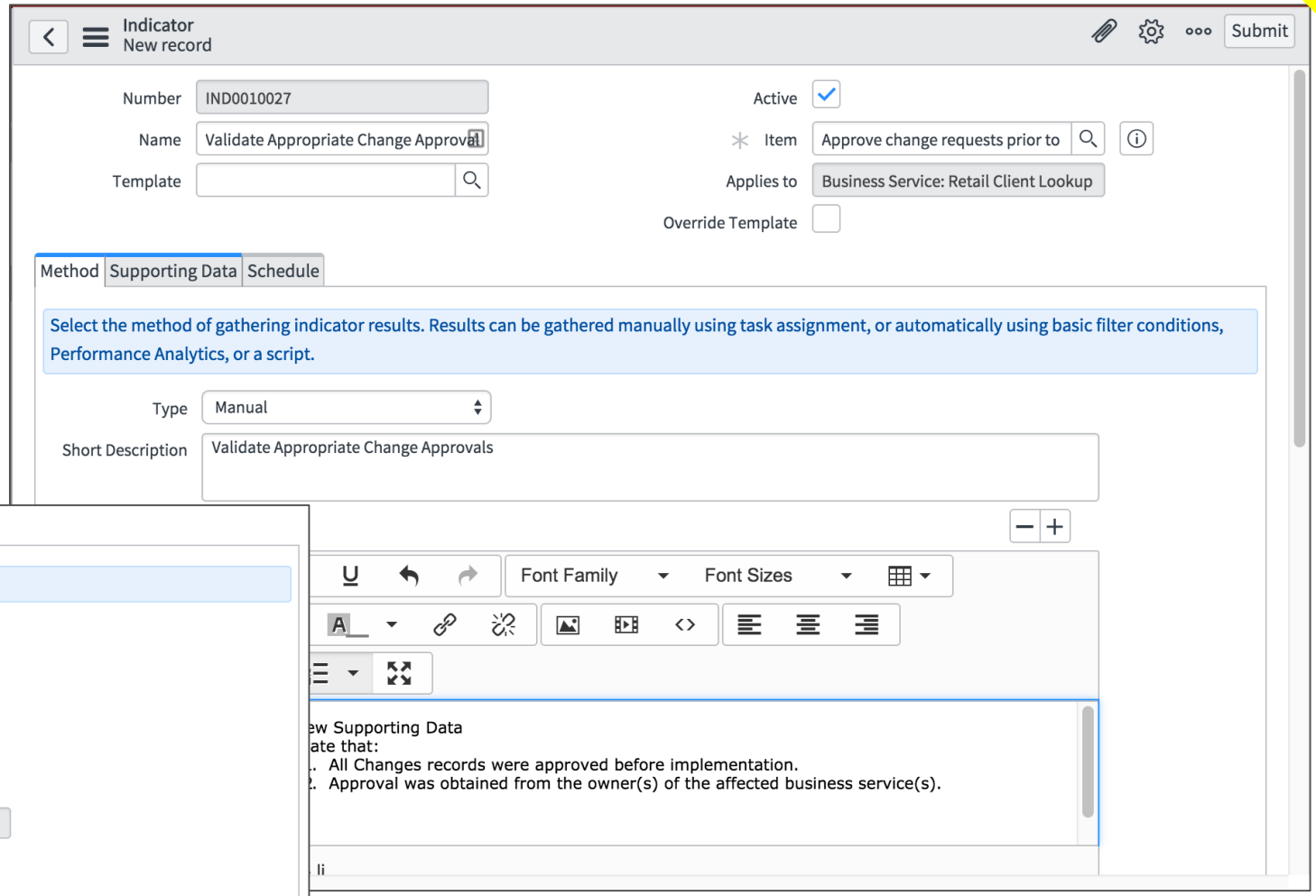
© 2017 ServiceNow All Rights Reserved

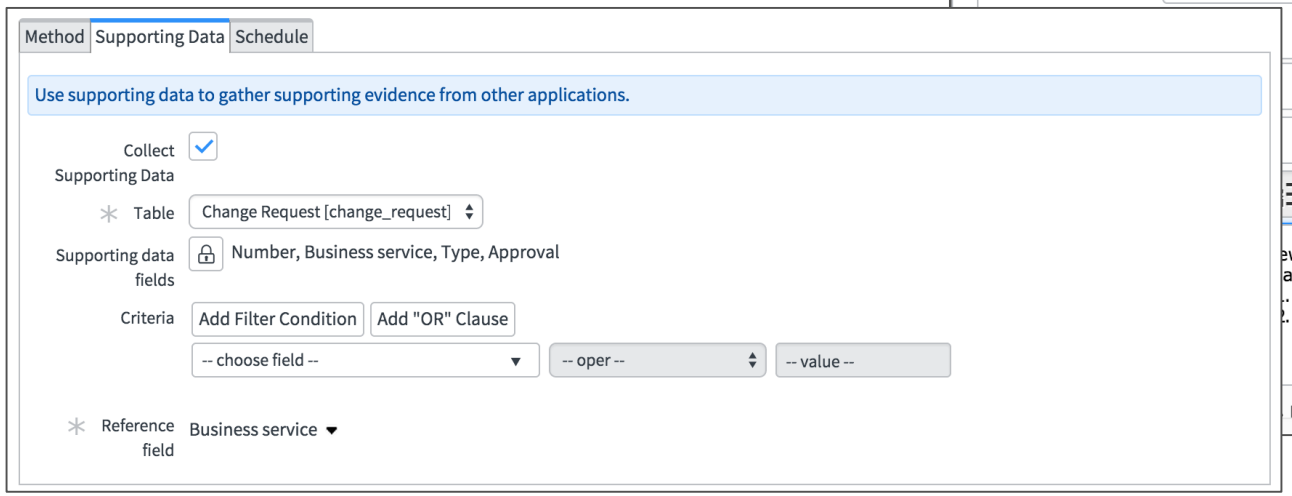
Task 4: Monitor (Better Together)

DEMO

Continuous Monitoring

- Indicators
  - Define Scheduled Control Tasks for Control Owners to Complete
  - Identify Compliance and Non-compliance automatically through exception reporting
  - Leverage Performance Analytics Indicator thresholds to identify non-compliance.





© 2017 ServiceNow All Rights Reserved

Viewing Compliant and Non-Compliant Controls, Managing Issues

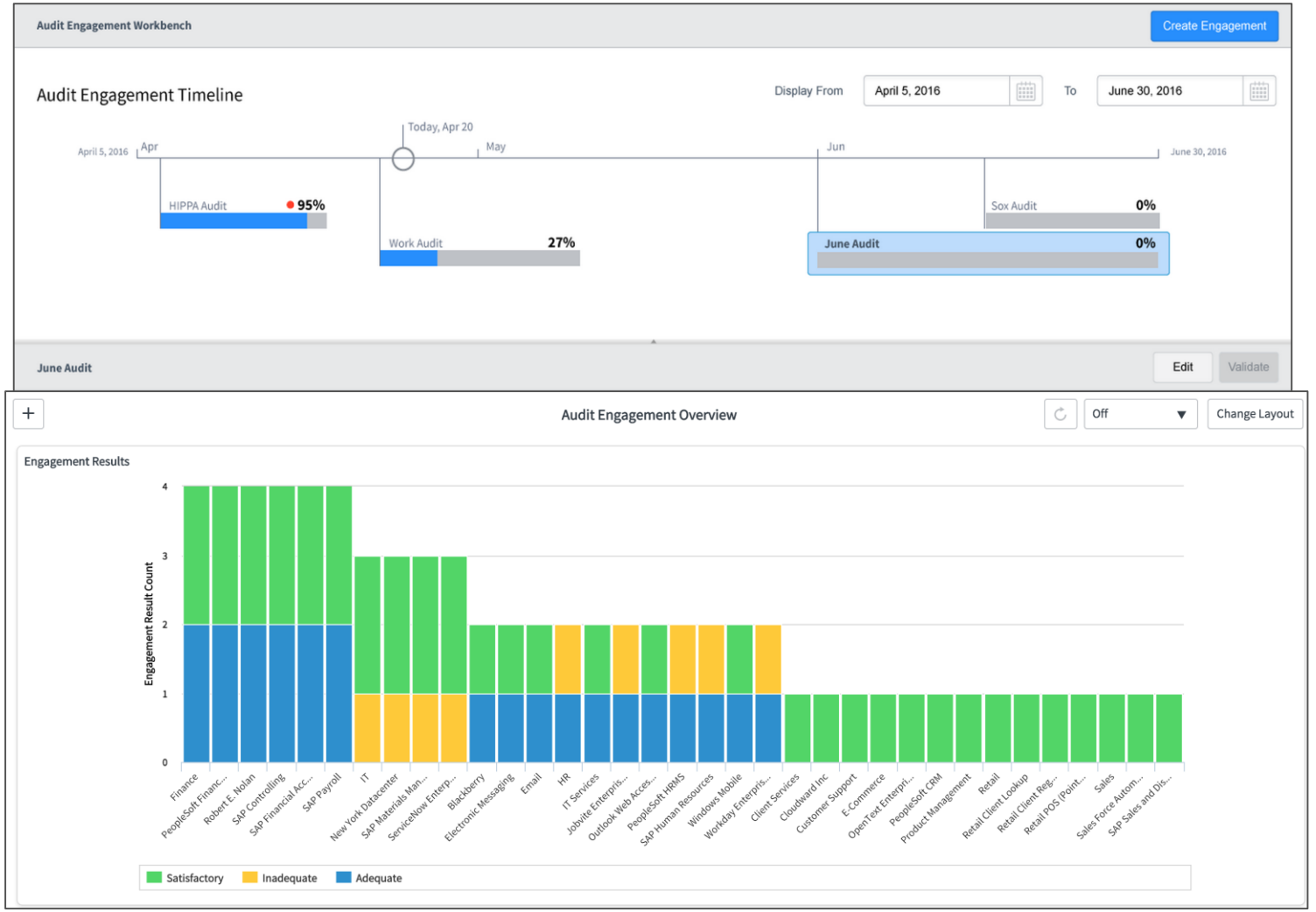
Task 5

© 2017 ServiceNow All Rights Reserved

Task 5: Monitor

Engagement Management

- Internal Audit
  - Project driven audits allow internal auditors to quickly plan, scope, and execute audit activities.
  - Leverage Risk Assessment data to develop a risk-based audit plan.
  - Schedule Interviews, Walkthroughs, and Control Test Activities in advance and assign resources.
  - Perform independent testing of control design and operational effectiveness.
  - Leverages continuous monitoring data for automatic control evidence collection.



© 2017 ServiceNow All Rights Reserved

Using Policy Dashboards

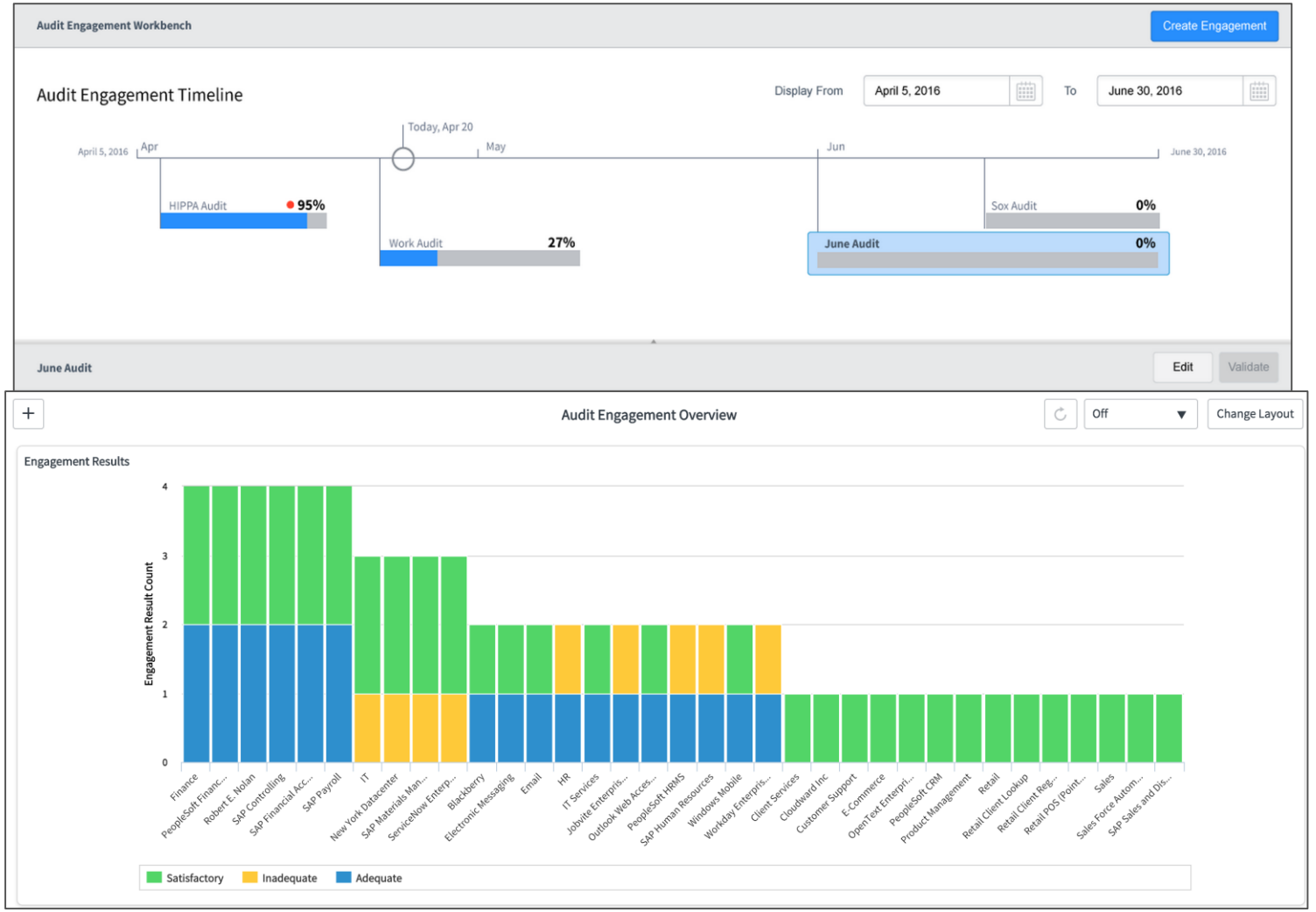
Task 6

© 2017 ServiceNow All Rights Reserved

Task 6: Monitor

Engagement Management

- Internal Audit
  - Project driven audits allow internal auditors to quickly plan, scope, and execute audit activities.
  - Leverage Risk Assessment data to develop a risk-based audit plan.
  - Schedule Interviews, Walkthroughs, and Control Test Activities in advance and assign resources.
  - Perform independent testing of control design and operational effectiveness.
  - Leverages continuous monitoring data for automatic control evidence collection.

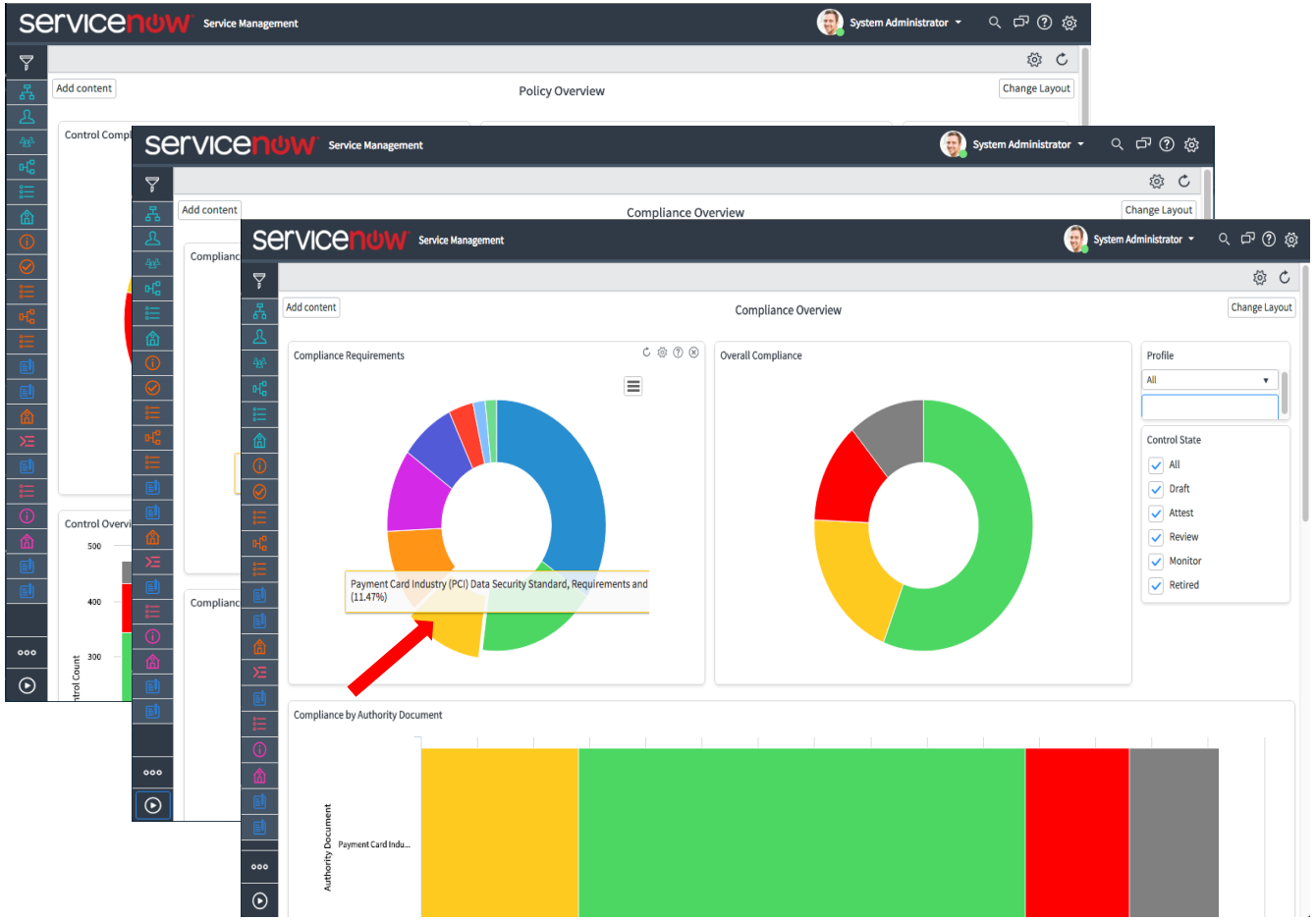


© 2017 ServiceNow All Rights Reserved

GRC – Policy and Compliance Management

Reporting

- Policy Overview
  - Compliant, Non-Compliant, and other measures
  - Dive into the detailed items with one click
- Compliance Overview
  - Review by Overall Compliance
  - Compliant, Non-Compliant, and other measures
  - Review by Compliance Requirement
  - Dive into the detailed items with one click
- Why is this important?
  - Illustrates whether or not the company is compliant and the level of compliance to it own policies as well as other external requirements
  - Defines the number of controls in the environment and the ability to refine the reporting to individual areas (i.e., Department or Requirement)



© 2017 ServiceNow All Rights Reserved

Key Takeaways

© 2017 ServiceNow All Rights Reserved

Challenges and Goals

Challenges

- Existing systems were expensive and laborious to modify
- Disparate processes and controls across CareWorks' six companies resulted in data silos
- Labor intensive process to produce required audit data on time

Results

- Centralized repository of information increases efficiency
- Single system of record across six businesses improves consistency
- Automated audit controls and reports
- Security Control compliance

© 2017 ServiceNow All Rights Reserved

Top Three LightSpeed Takeaways

1 Understanding **risk** and defining the **proper response** should **enable confidence** in the **mitigating controls** and the overall security of the organization

2 Leveraging a **common integrated platform** to manage the risk lifecycle, from preventative measures to detection and incident response, ensures efficiency and **consistent outcomes**

3 Let the CISO sleep! …by answering these three questions: Are we secure? Are things getting better? Do we have effective controls?

© 2017 ServiceNow All Rights Reserved

Thank You

Lab Sponsored by Microsoft Azure



Syra Arif
Security Solutions Architect
ServiceNow

David Perodin
Security Solutions Architect
ServiceNow

#Know17 | http://clabs.link/lab132022

© 2017 ServiceNow All Rights Reserved

Q & A

Syra Arif
Security Solutions Architect
ServiceNow

David Perodin
Security Solutions Architect
ServiceNow

© 2017 ServiceNow All Rights Reserved