servicenow | MeriTalk

Jump-start your RMF process with ServiceNow and Okta

Agenda

The Risk Management Framework

Jump-start RMF with ServiceNow

Okta automates RMF authorization

ServiceNow and Okta in action

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

…An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks…

OMB Memorandum M-17-25
Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [OMB M-17-25]

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

The RMF process

Source: BAP

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Respond faster to security incidents, vulnerabilities, and enterprise risk

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

NIST RMF Use Case Accelerator on ServiceNow GRC

Homepages, Reports

Metrics, Reports, and Dashboards

Audit

Audit Engagement: *Scoping (Controls/Risks), Execution (Test Plans, Control Tests, Indicator Results)* — 3 Implement

Data Sets

Controls
- 2 Select
- 3 Implement
- Assessment, Indicators, Test plans
- Assess 4
- Monitor 6

Profiles (RMF Target)

Risks
- 4 Assess
- Attestation, Indicators
- Assess 4
- Monitor 6

Policy Statement

Profile Class, Types, Relationships

Risk Statement

1 Categorize

5 Authorize

Use Case Accelerators

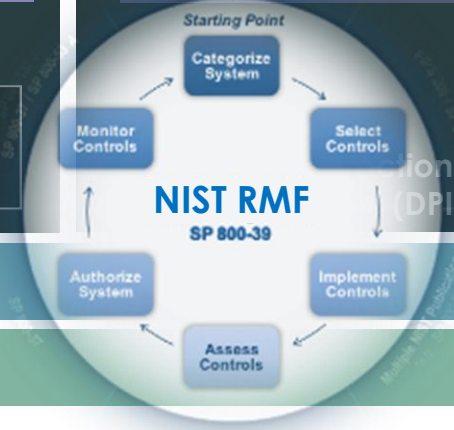
NIST Risk Management Framework (RMF)

NIST Cybersecurity Framework (NIST CSF)

Risk Assessment

Profiles

Profile Class, Types, Relationships



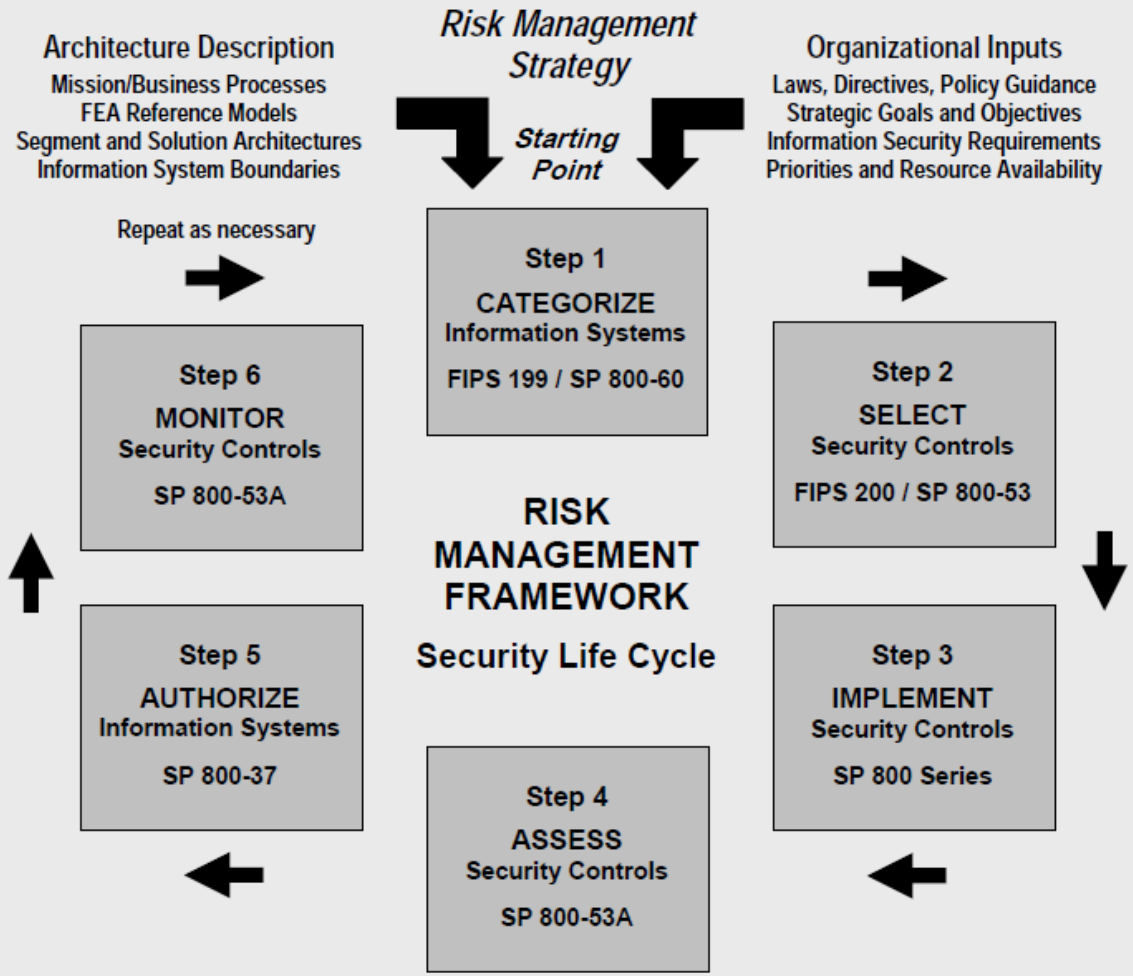
ion Impact (DPIA)

Governance, Risk, & Compliance

ServiceNow Platform

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

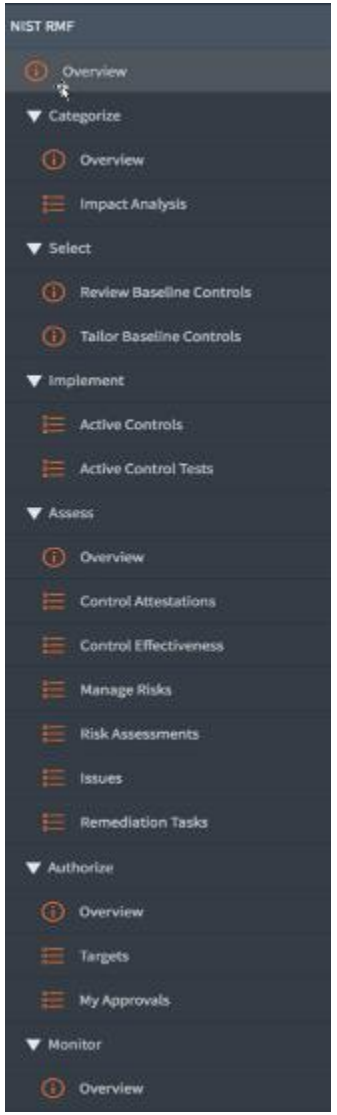
NIST Risk Management Framework



© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

RMF Use Case Accelerator

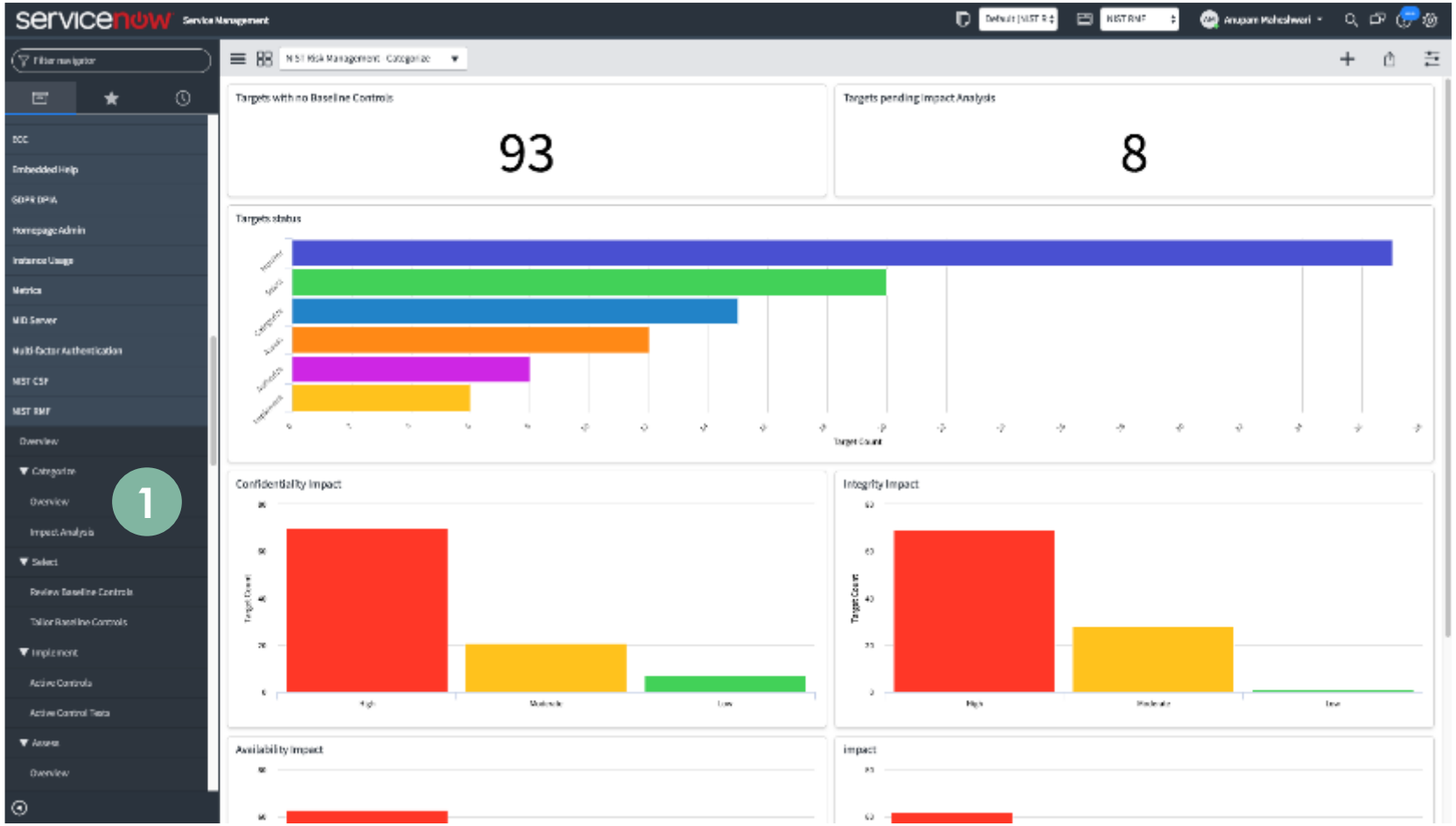
- Policies
- Controls
- Assessments/Attestations
- Risks
- Issues
- Remediation tasks
- Test plans
- Dashboard



© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

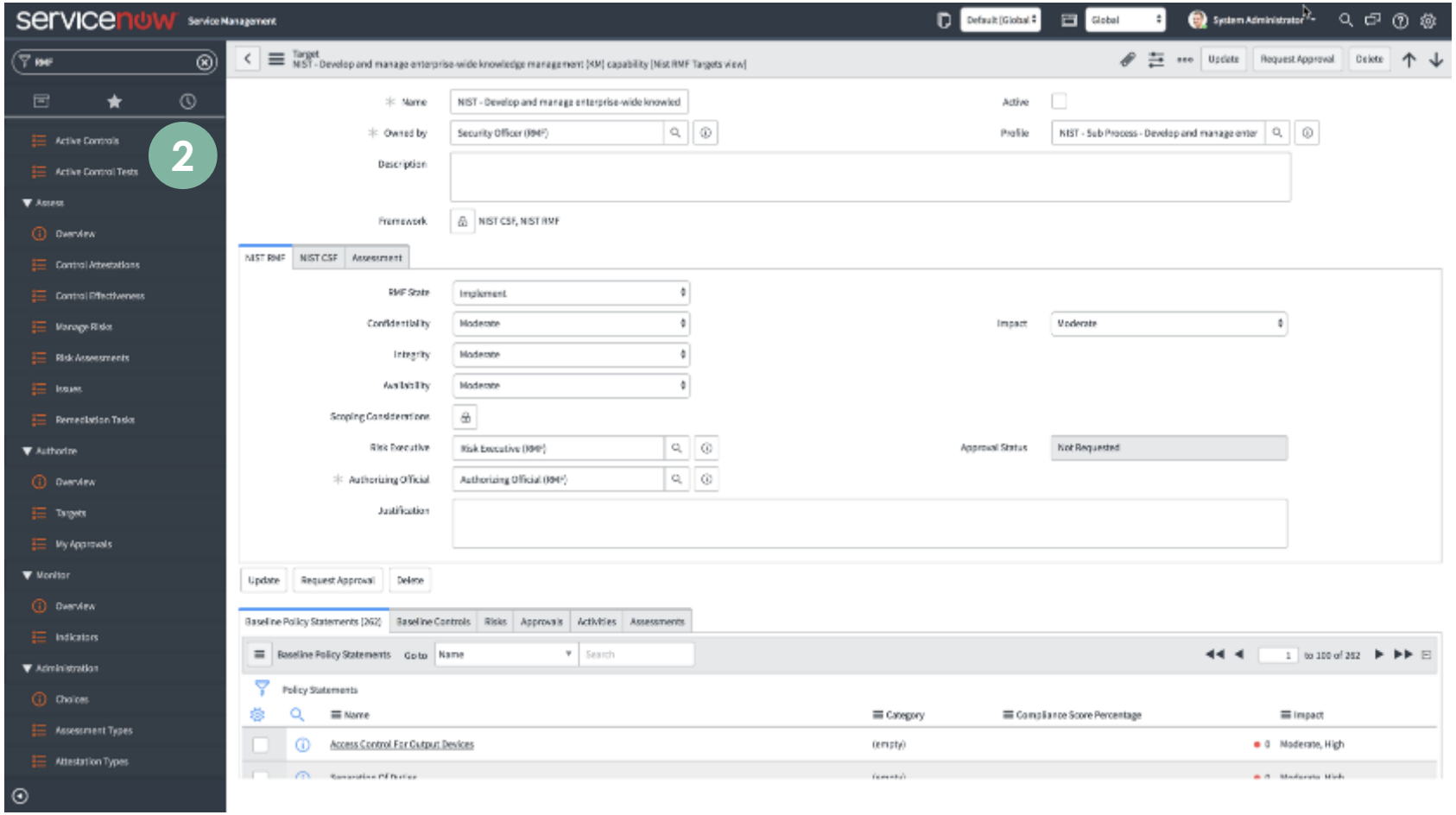
Step 1: Categorize Information Systems



- For the information systems, assess the criticality of the assets and potential adverse impact to business from any state changes
- Use Confidentiality, Integrity and Availability factors in the assessment.
- Based on this criticality identify the assets that are most critical and represents the high risk.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

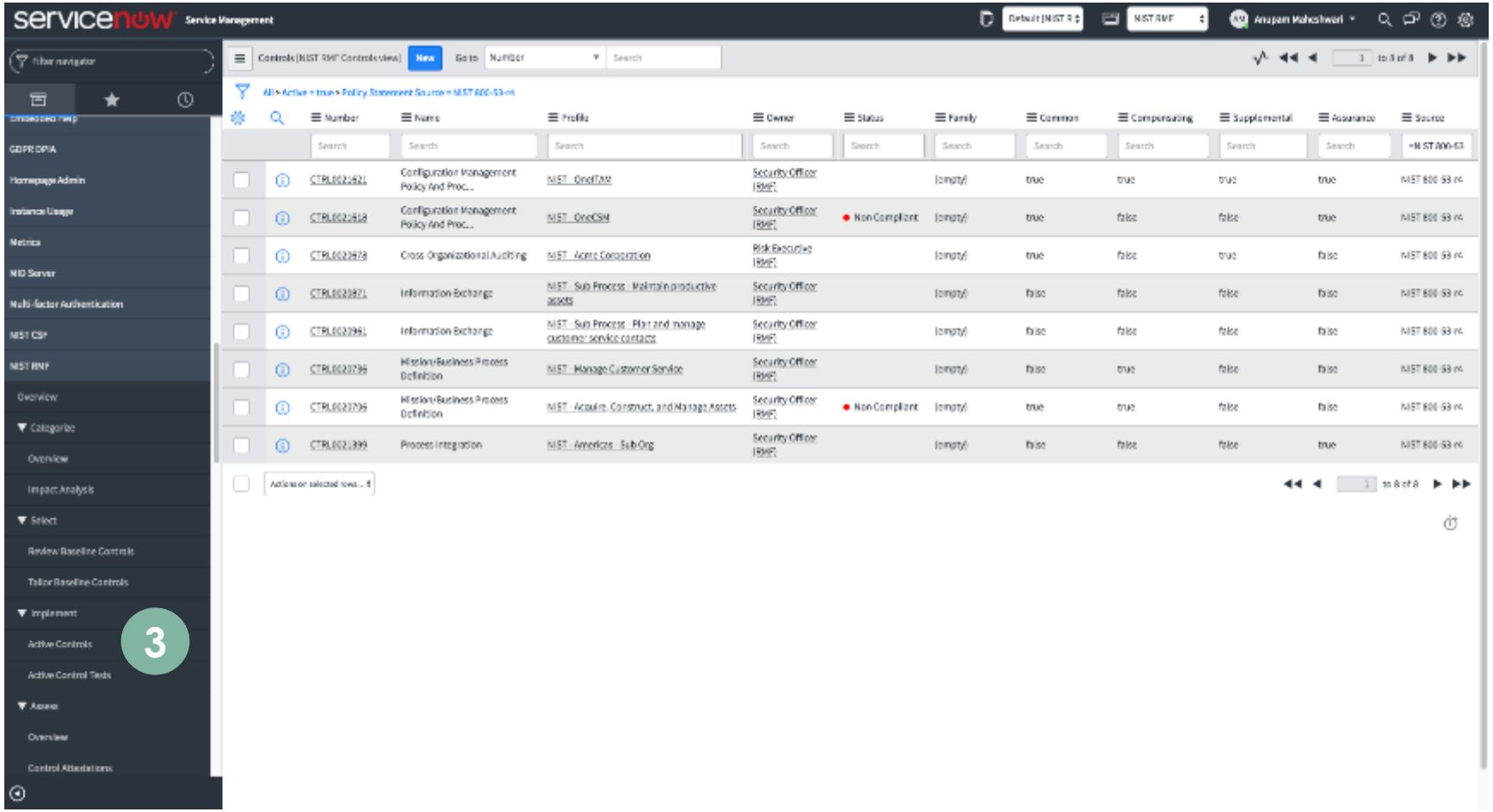
Step 2: Select baseline controls



- Select the baseline security controls based on the criticality of the assets, apply tailoring guidance based on the context and identify supplemental controls if required.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

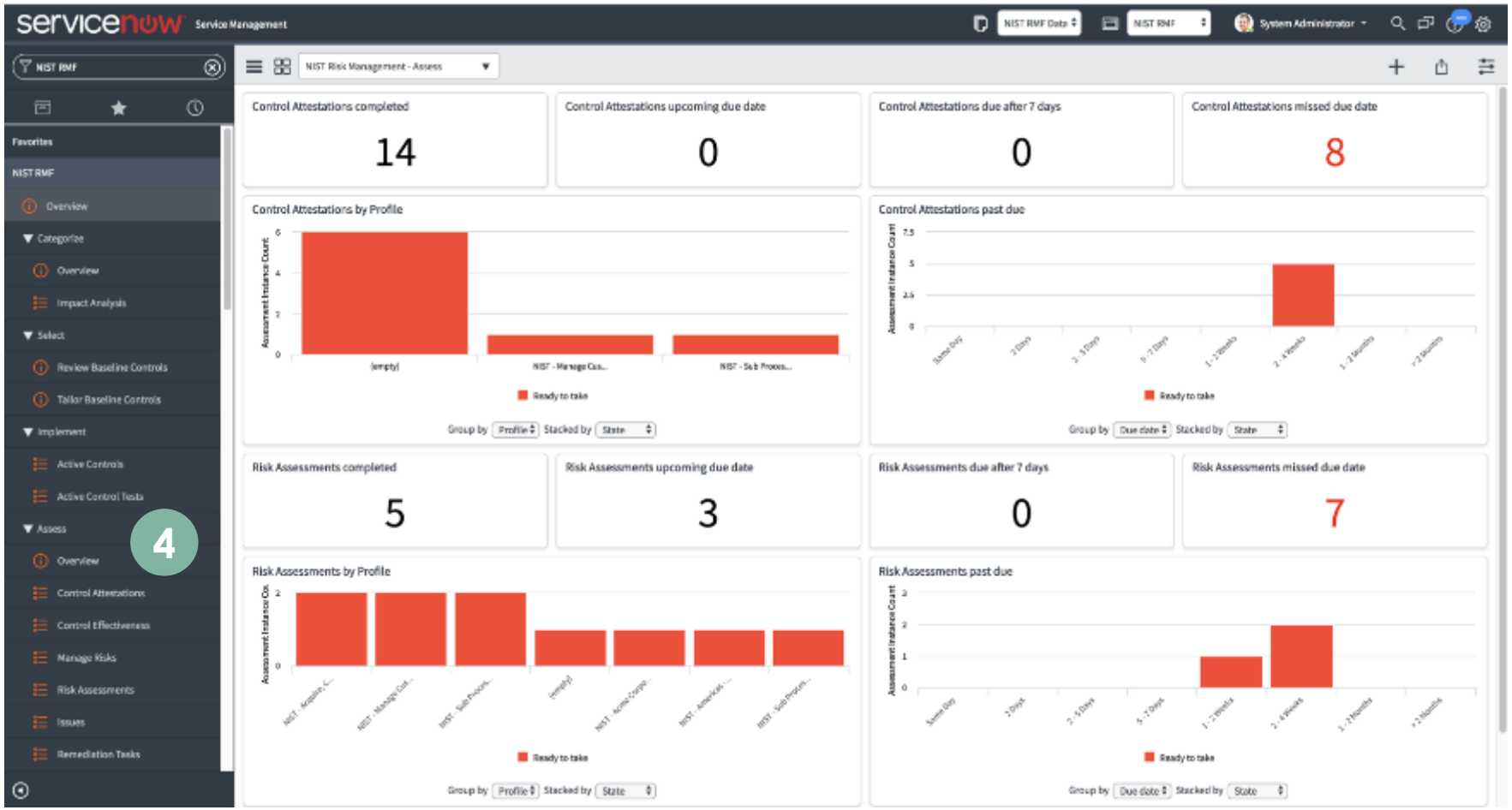
Step 3: Implement controls



- Implement the controls for the identified assets within the enterprise architecture; use management discretion to apply security configurations settings on controls.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

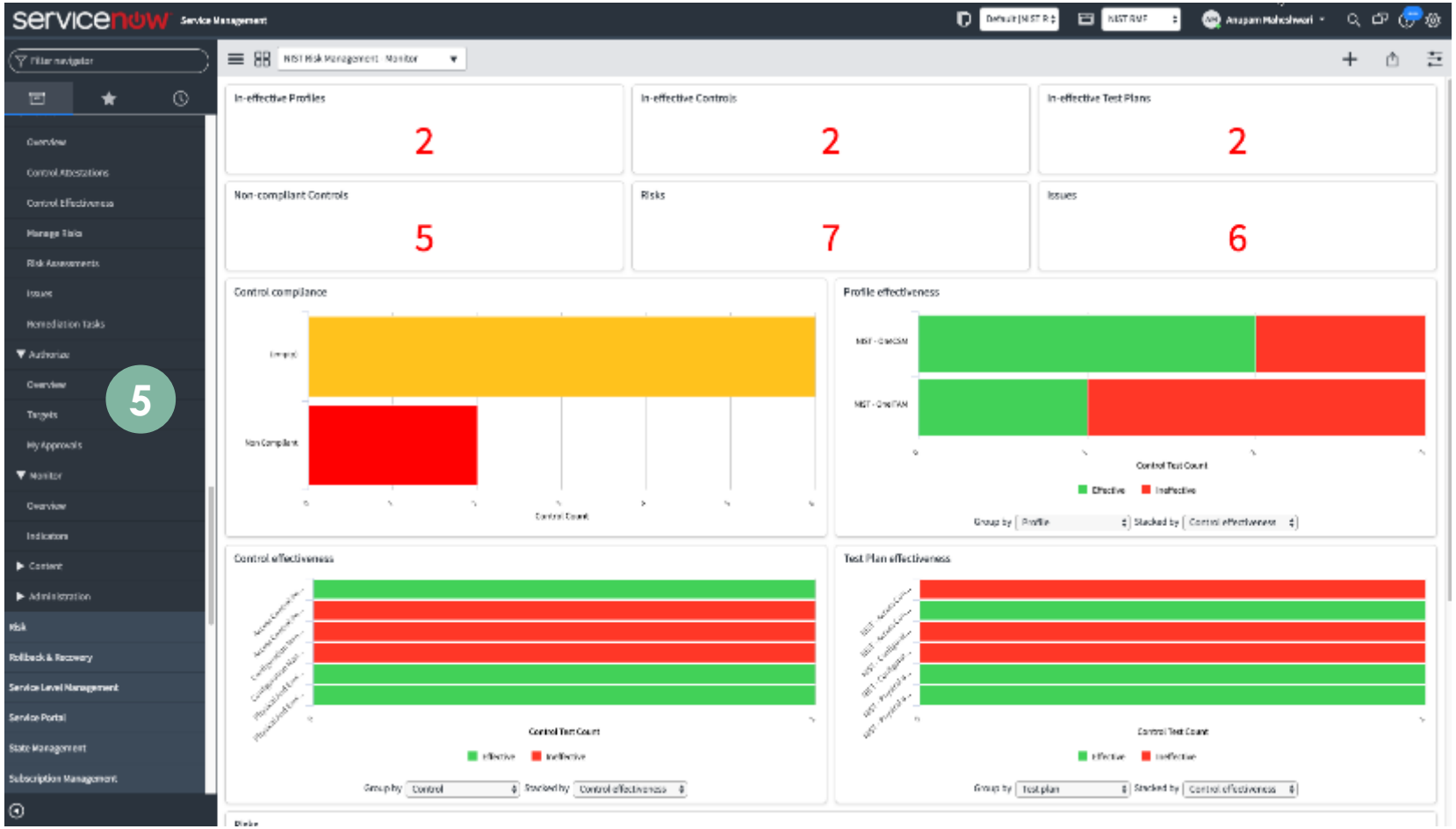
Step 4(a): Controls owners perform attestation of controls



- Trigger attestation to control owners to ensure controls are implemente for the respective information assets and ask for evidence.
- In case of non-compliance, trigger an issue to ensure remediation is done and controls are implemented on priority.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

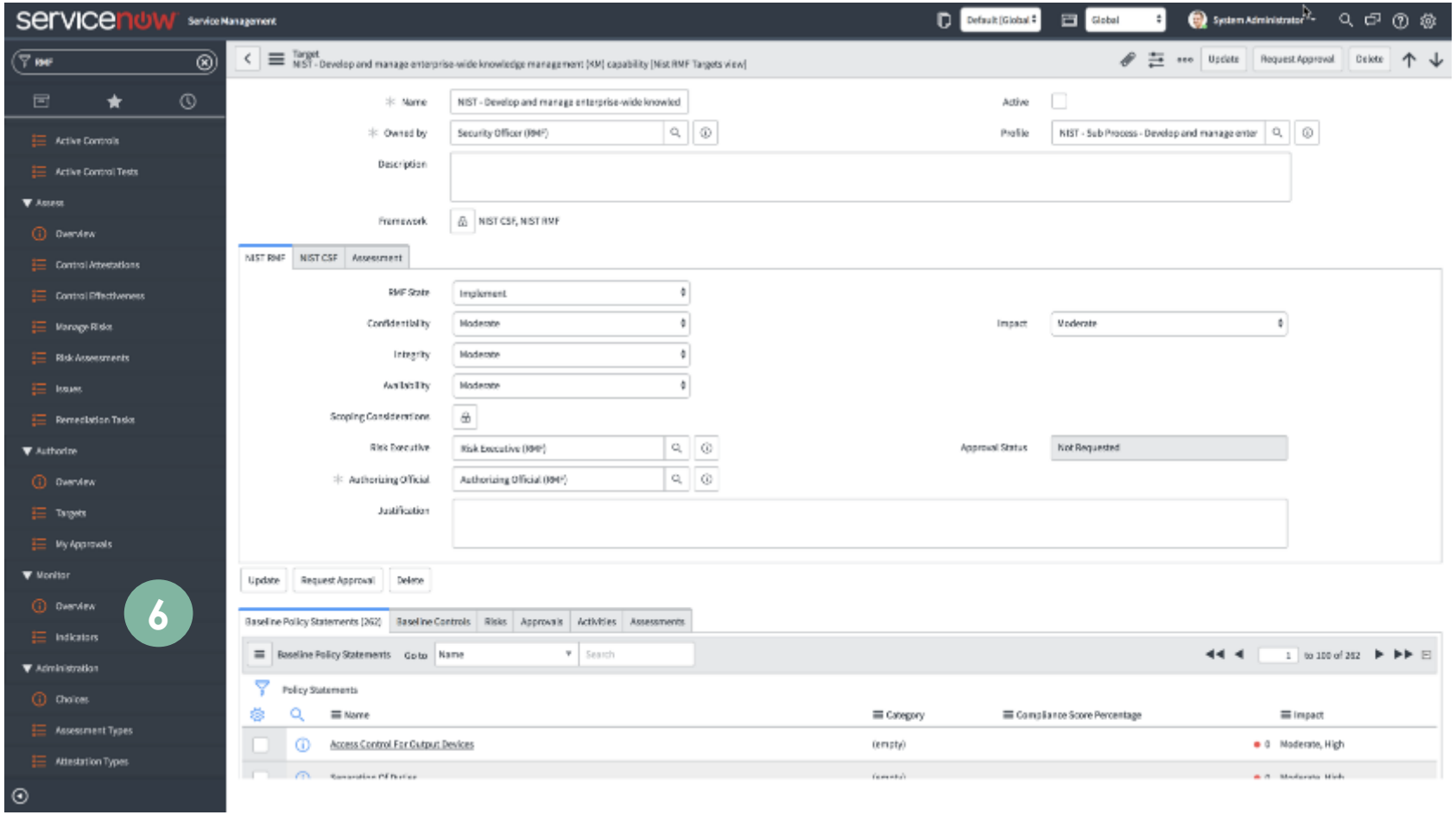
Step 5: Authorize



- Ensure all activities such as risk assessment, control testing and issues are reviewed by management.
- If acceptable, authorize operations.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Step 6: Monitor



- Setup indicators for continuous monitoring of the risks and controls.
- Monitor the overall risk profile for the information assets through reports on dashboard.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Here's the problem…

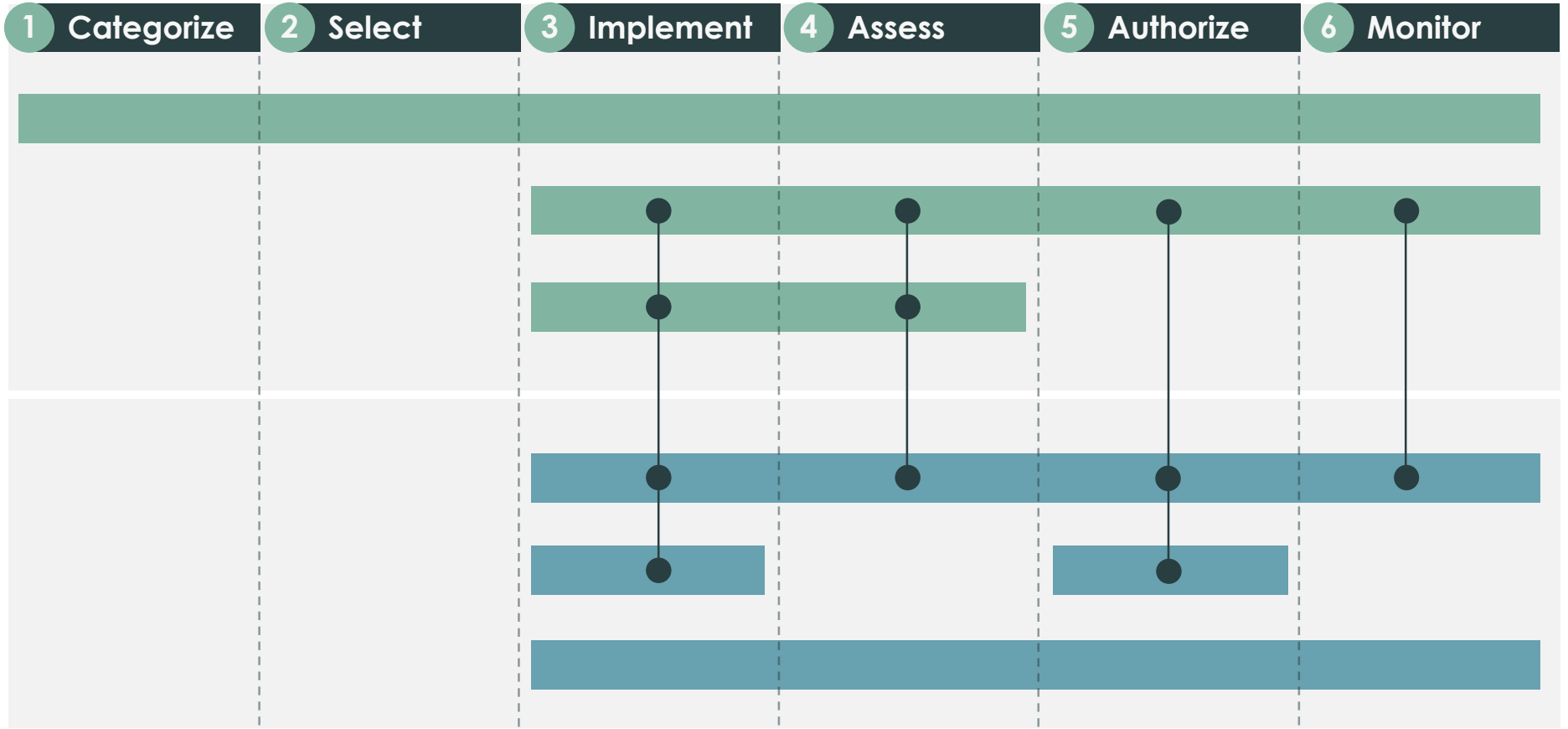
Managing user onboarding and off boarding, and application permissions is a time consuming activity that if not automated and orchestrated delays RMF authorization, thus delaying value activation by agency enterprise.

We have the answer…

© Okta and/or its affiliates. All rights reserved. Okta Confidential

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

RMF and speed of value delivery



© Okta and/or its affiliates. All rights reserved. Okta Confidential

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

NIST 800-53v4 RMF Control sample use cases

IA-2(1) and IA-2(12)—Admin login using PIV

Okta Single Sign On

ServiceNow GRC

- Okta Single Sign-on Provides PIV Enforcement
- ServiceNow GRC and SecOps provides configuration validation and response

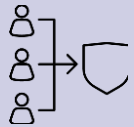
AU-12—Audit Policy Control with Time Correlation

Okta Activity Log

ServiceNow Collection and Correlation to Policy

- Okta Identity Cloud provides Audit and Access Logs of all applications and configurations
- ServiceNow GRC and SecOps provides consolidation and time correlation

SI-7(7)—Integration of Detection and Response



Okta Identity Data Feed

User Security Controls

- Okta Identity Cloud Provides Identify Feed Including High Risk Actions
- User controls embedded into ServiceNow Security Incident Response

© Okta and/or its affiliates. All rights reserved. Okta Confidential

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Okta + ServiceNow Integration Portfolio

Okta Identity Cloud for Enterprise/Express

Single Sign-On

Provisioning

- Embedded Okta
- Identity for ServiceNow

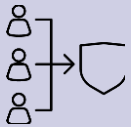
Okta Orchestration Activity Pack

Custom Activities

Integrate to Workflow

- Automation and Self-Service
- Onboarding / Offboarding

Okta Identity Cloud for Security Operations



Identity Data Feed

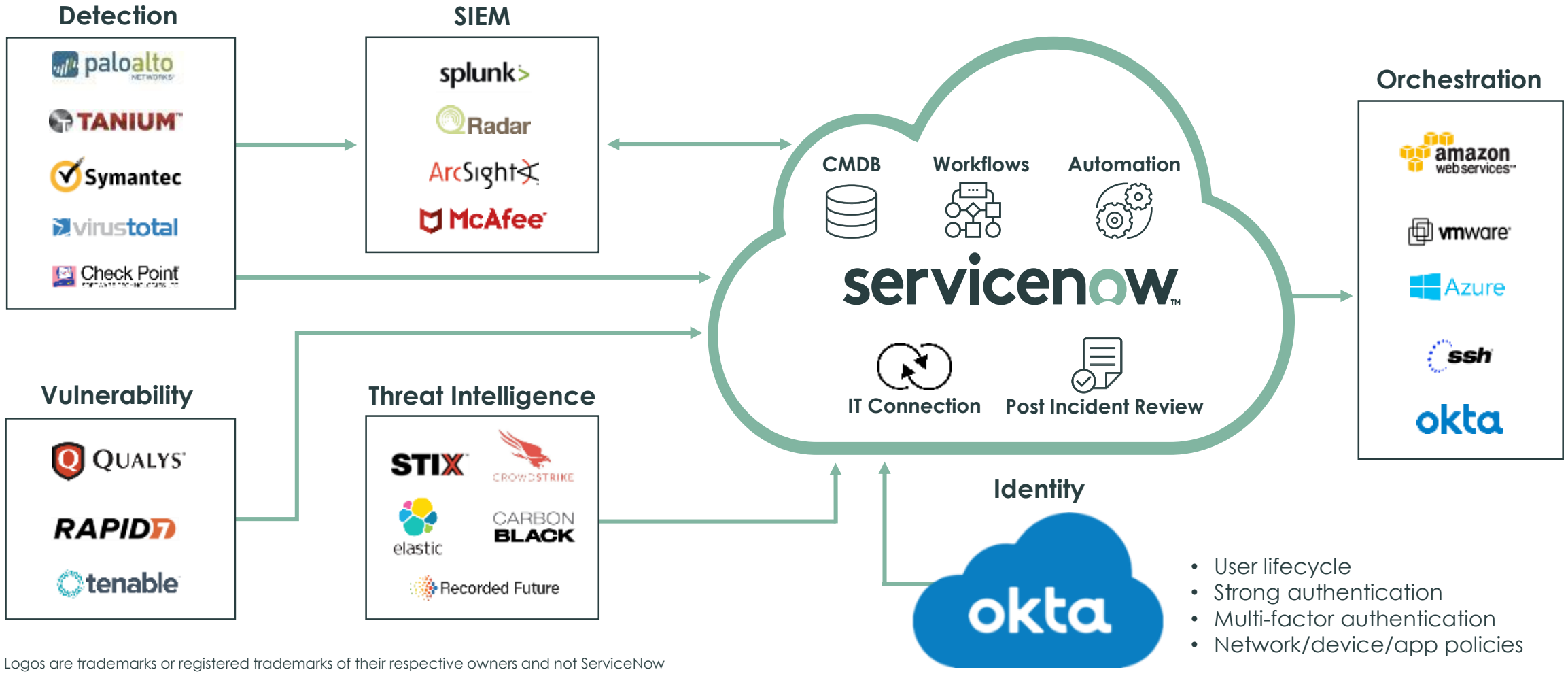
ServiceNow User Security Controls

- User controls embedded into ServiceNow Security Incident Response

© Okta and/or its affiliates. All rights reserved. Okta Confidential

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Security ecosystem



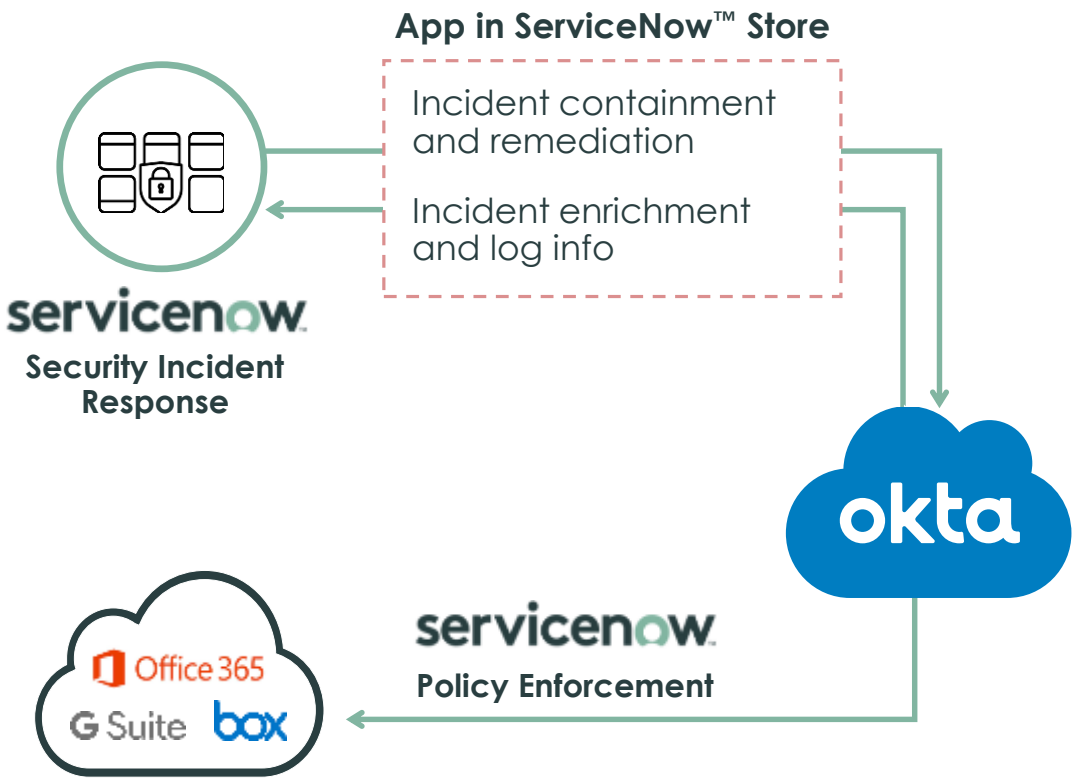
- User lifecycle
- Strong authentication
- Multi-factor authentication
- Network/device/app policies

Logos are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Okta Identity Cloud for Security Operations

Automatic User enrichment and Identity controls for **Security Incident Response**



Improve risk scoring; Reduce incident triage time

Add user context to active incidents

- Applications Provisioned
- Group Memberships
- Recent user activity (logins, etc)

Accelerate incident containment

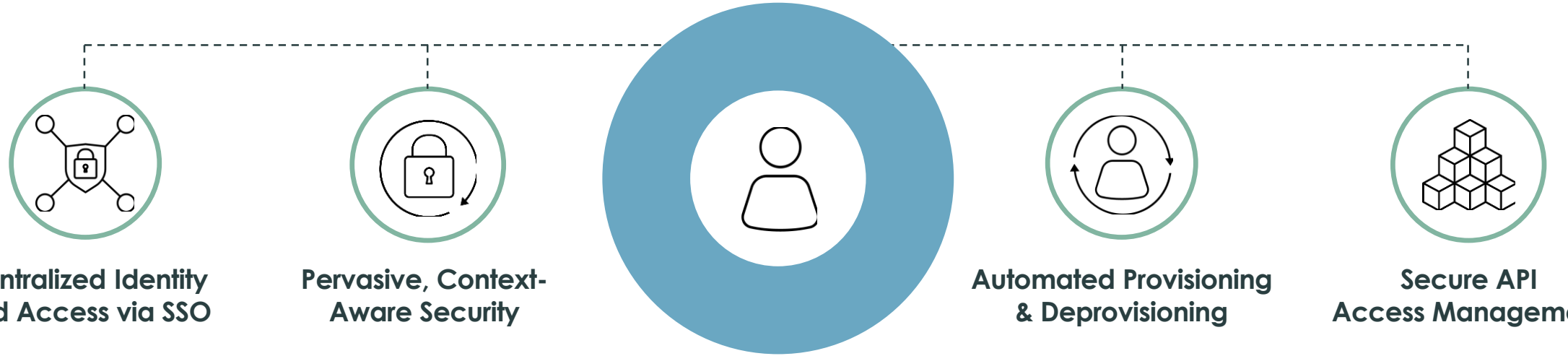
Provide contextual user controls directly within incidents in ServiceNow

- Clear active sessions
- Suspend / Unsuspend user
- Change / Add / Remove application access
- Change / Add / Remove group membership
- Force expire password, MFA token

© Okta and/or its affiliates. All rights reserved. Okta Confidential

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Okta is the foundation for Zero Trust security



© Okta and/or its affiliates. All rights reserved. Okta Confidential

© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Demo

Identifying the business risk of unauthorized access with ServiceNow and Okta

servicenow | MeriTalk

servicenow | MeriTalk

Thank you

Contact info?