servicenow

FedRAMP Accelerator on ServiceNow

Rosalind Morville
ServiceNow

Sarah Lange
Partner – Public Sector

Ahmed Bilal
Developer

Safe Harbor Notice for Forward-Looking Statements

This presentation may contain "forward-looking" statements that are based on our beliefs and assumptions and on information currently available to us only as of the date of this presentation. Forward-looking statements involve known and unknown risks, uncertainties, and other factors that may cause actual results to differ materially from those expected or implied by the forward-looking statements. Further information on these and other factors that could cause or contribute to such differences include, but are not limited to, those discussed in the section titled "Risk Factors," set forth in our most recent Annual Report on Form 10-K and Quarterly Report on Form 10-Q and in our other Securities and Exchange Commission filings. We cannot guarantee that we will achieve the plans, intentions, or expectations disclosed in our forward-looking statements, and you should not place undue reliance on our forward-looking statements. The information on new products, features, or functionality is intended to outline our general product direction and should not be relied upon in making a purchasing decision, is for informational purposes only, and shall not be incorporated into any contract, and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion. We undertake no obligation, and do not intend, to update the forward-looking statements.

Join us at future webinars and meetups

See the schedule

Link will be shared in today's chat

Housekeeping

We saved time at the end for Q&A. Please use the Q&A button at the bottom of your screen along the way.

The presentation will be recorded and shared on the ServiceNow Community.

After the event, you will be prompted to fill out a short survey. Thank you for your feedback!

Agenda

- Introduction
- About Securitybricks, Inc.
- FedRAMP Accelerator
- Demo

Who We Are

Our consultants are all U.S. citizens in 4 time zones on U.S. soil with an average of 15+ years of experience, including DoD experience

Certifications include CISSP, CEH, CRISC, CISM

Focus – Cloud security & Compliance

FedRAMP · CMMC-AB C3PAO · servicenow SPECIALIST Partner Consulting & Implementation · servicenow PLATFORM Partner Build · Microsoft Cloud Solution Provider · StateRAMP · ISO/IEC 17020:2012 · AICPA SOC

DoD SKILLBRIDGE

Transitioning veterans to cybersecurity since 2021

Areas of Focus

FedRAMP

- *Enable Cloud Service Providers to do business with US Federal agencies*

- *Enable DoD subcontractors to comply to DFARS/CMMC requirements*

- *AppStone platform to secure software supply chain*

servicenow

- *Security and compliance automation platform*

Microsoft Federal

- *Implement security controls in Azure Government clouds*

Glossary of Terms

FedRAMP - The Federal Risk and Authorization Management Program provides a standardized approach to security authorizations for Cloud Service Providers (CSPs).

ATO - An Authorization to Operate is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations.

FedRAMP Sponsorship - To participate in the FedRAMP Program, customers must obtain Sponsorship from a Federal Agency or go through the Joint Authorization Board, the primary governing body for FedRAMP which includes the Department Of Defense (DoD), Department Of Homeland Security (DHS), and General Services Administration (GSA).

POA&M - The Plan of Action and Milestones identifies areas of weakness in security controls. This is the process CSPs use to track and mitigate findings.

CIS/CRM Workbooks - The Control Implementation Summary/Customer Responsibility Matrix Workbooks are security artifacts that delineate the security responsibilities of CSPs and customers (Federal Agencies).

What Is The Process to Achieve a FedRAMP Authority to Operate (ATO)?

SELECT AN AUTHORIZATION PATH:
AGENCY OR
JAB PROCESS
READINESS DESIGNATION

PREPARATION
AGENCY - READINESS ASSESSMENT PRE-AUTHORIZATION
JAB - FULL SECURITY ASSESSMENT
READINESS ASSESSMENT WITH 3PAO
LISTED IN MARKETPLACE AS "IN PROCESS"

AUTHORIZATION
AGENCY - FULL SECURITY ASSESSMENT
JAB - AUTHORIZATION PROCESS
READINESS ASSESSMENT REPORT
MOVE FROM "IN PROCESS" TO ATO OR DESIGNATED "READY"

CONTINUOUS MONITORING

FedRAMP Rev. 5 Compliance

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Access Control	Identification and Authentication	Audit and Accountability	Incident Response	Continuous Monitoring
Contingency Planning	Awareness & Training	System and Information Integrity		
Planning	Configuration Management	Security Assessment and Authorization		
PII Processing & Transparency ★	Maintenance			
Program Management ★	Media Protection			
Personnel Security	Physical and Environmental Protection			
Risk Assessment	System and Communications Protections			
System and Services Acquisition				
Supply Chain Risk Management ★				

★ Represents new Control Families under Rev. 5

servicenow

FedRAMP

Low Baseline - caters to federal systems with minimal security needs.

Moderate Baseline - serves those with more substantial risk factors (most commonly used baseline).

High Baseline - provides the most comprehensive level of protection.

Cloud Service Providers must complete the initial Federal Information Processing Standard **(FIPS)-199 task to develop standards for categorizing their information and systems.

Common Problem Statements for a FedRAMP Assessment

Authorization Boundary Diagram

- Dynamic in nature and includes all systems, apps, 3rd party vendors, processes that touch the FedRAMP system.
- Based on computing environment (data center/cloud providers like Microsoft GCC or MSSP), diagrams may be complicated to design.

SSP (System Security Plan)

- System Security plan is the single artifact that will demonstrate FedRAMP readiness.
- A 500–600-page document that includes information related to all the 20 NIST controls, as well as, data flow, interfaces, cloud solution description, policies, procedures, and a Continuous Monitoring Strategy.
- A 3PAO uses the SSP as the guidance document for the entire assessment.

POA&M

- Many assessments will have gaps that need to be addressed at a later stage.
- A Plan of Action & Milestones (POA&M) document will help provide guidance on when the risks/issues will be remediated.
- All critical and high vulnerabilities need to be resolved within 30 days, medium 90 days, and low vulnerabilities within 180 days.

Inherited/Shared Responsibility Controls

- Many customers have concerns over whether a particular control should be Fully or Partially Inherited or Shared between the Cloud Provider or the Customer.
- The CIS & CRM Workbooks will need to be populated and reviewed with all parties before the FedRAMP package is submitted to make sure every control has been categorized properly.

Continuous Monitoring

- The Continuous Monitoring is a huge effort. Someone will be identified to keep track of all the Daily, Weekly, Bi-Weekly, Monthly, and Yearly requirements that need to be kept in good standing.
- Companies are willing to pay a 3rd-Party to manage this initiative so they can be prepared for their next assessment.

What the Securitybricks FedRAMP Accelerator Solution offers

- Securitybricks FedRAMP Accelerator is built to integrate with the existing reporting capabilities of the GRC Module to provide real-time visibility into the status and progress of FedRAMP C&A (Certification & Accreditation) activities.
- Enable collaboration and communication between stakeholders involved in the FedRAMP C&A process.
- Developed to provide a centralized repository that automates the collection for storing and managing all FedRAMP C&A (Certification & Accreditation)-related artifacts, and evidence from within ServiceNow modules and extending to your cloud environment.
- Streamlines the entire ATO lifecycle by automating assessments and evidence gathering

FedRAMP Accelerator Features

Assessment/Readiness

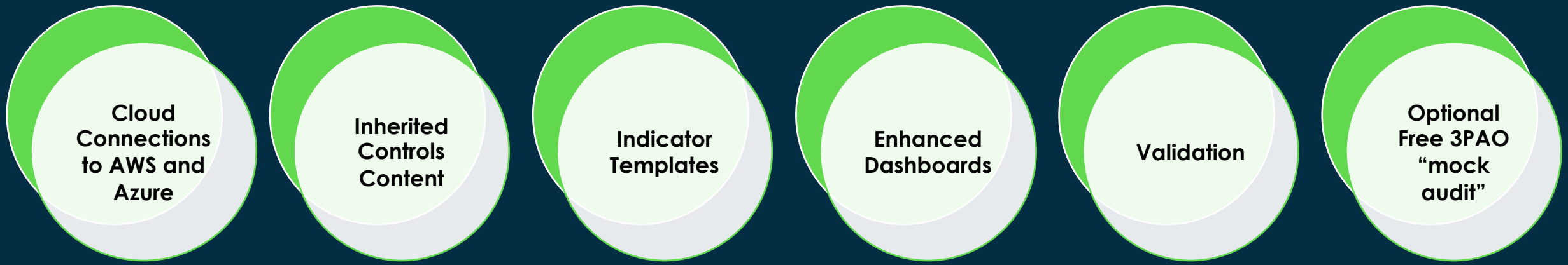
- Built on ServiceNow in the IRM module.
- Provide evidence for 44 inherited & 114 shared FedRAMP controls from Azure & AWS.
- Automate 65% evidence collection of 323 controls via ITSM, ITAM, SecOps, etc.
- Comprehensive questionnaires with guidance & evidence criteria.
- FedRAMP templates ready to submit to their 3PAO such as the system security plan(SSP) and Plan of Action and Milestones(POA&M).
- Provide evidence for each FedRAMP control.

Continuous Monitoring/Reporting

- Features connectors for AWS Security Hub & Azure Security, allowing easy import of security configurations to ServiceNow, integrating cloud security into compliance management.
- Generate NOW dashboards and several built-in reports.
- Automation of Monthly FedRAMP reporting such as POA&M and deviation request forms.

Product Demo

Extending the Accelerator – Our Solution



Questions?

servicenow

Thank you