

NIST Cyber Risk Scoring (CRS)

Program Overview

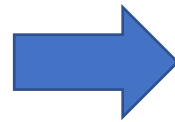
February 2021

- CRS Project Background
- Risk Profiling and Risk Scoring
- Information Security Continuous Monitoring (ISCM) & Ongoing Authorization (OA)
- Privacy Capabilities
- Management Dashboards
- Questions?

Assessing, Understanding, and Managing Security and Privacy Risks

NIST's Cyber Risk Scoring (CRS) Solution enhances NIST's security & privacy Assessment & Authorization (A&A) processes by presenting real-time, contextualized risk data to improve situational awareness and prioritize required actions.

Previous Process



CRS Solution



- Integrated view of NIST risk posture across the enterprise with quantitative metrics across systems and components
- More frequent, meaningful and actionable risk information to System Owners & Authorizing Officials
- Improved efficiency through automating assessments of certain controls and auto-generation of ATO documentation
- A data-driven basis for ongoing authorization decisions
- Present the organization's overall security posture from different perspectives, e.g., the Risk Management Framework (RMF) and Cyber Security Framework (CSF)

The CRS toolset provides end users the following capabilities:

Archer:

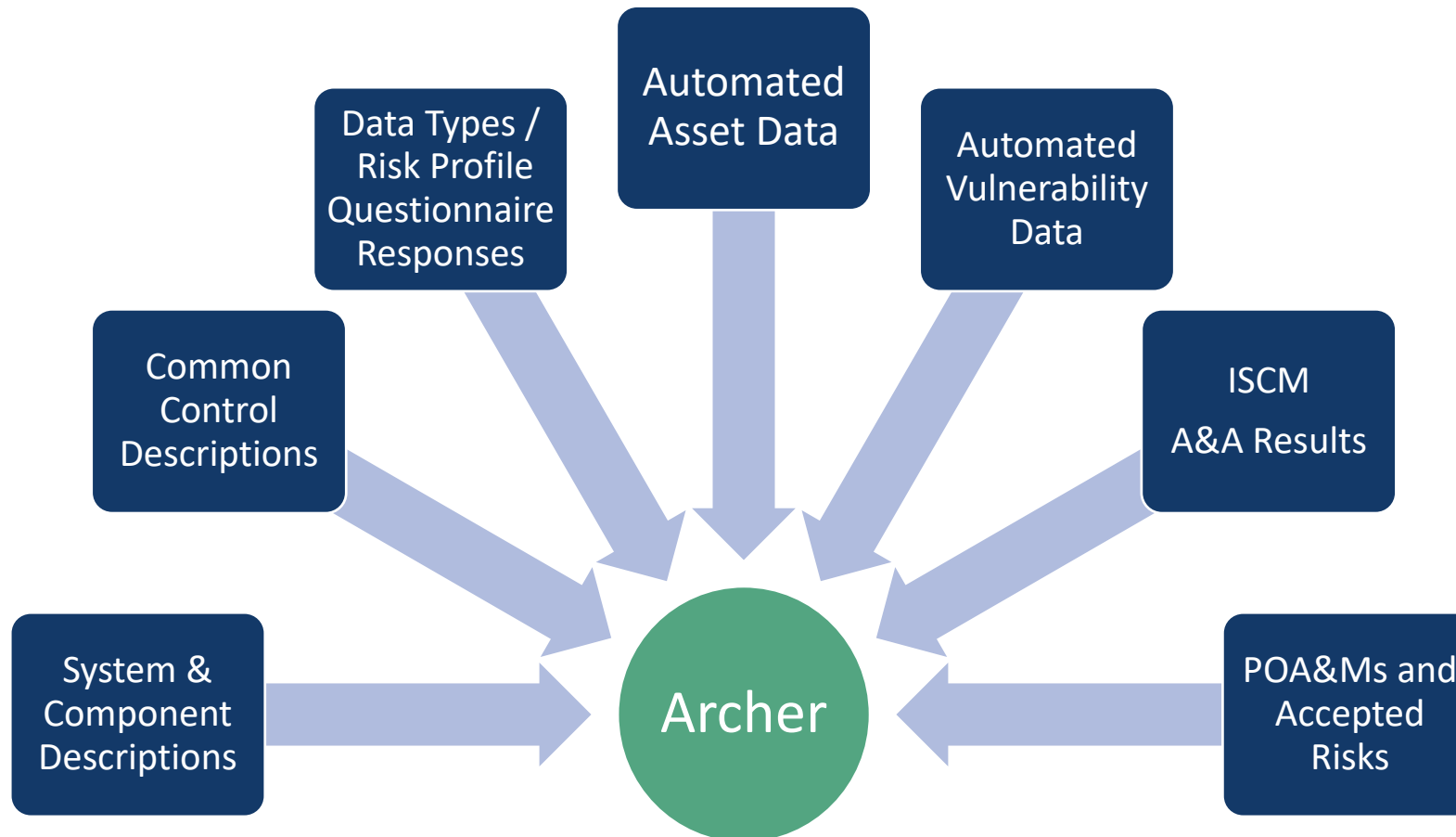
- Prioritize security & privacy control assessments
- Manage A&A and significant change schedules
- Track Accepted Risks and POA&M milestones
- Generate security and privacy documentation
- Provide compliance and vulnerabilities scan results in near-real time

Tableau:

- View risk at multiple organizational levels
- Integrate vulnerability data into risk scoring
- Drill-down into specific assets and their current vulnerability exposures
- Respond to data calls quickly with details (e.g. CVEs and affected assets)
- Analyze risks against the CSF

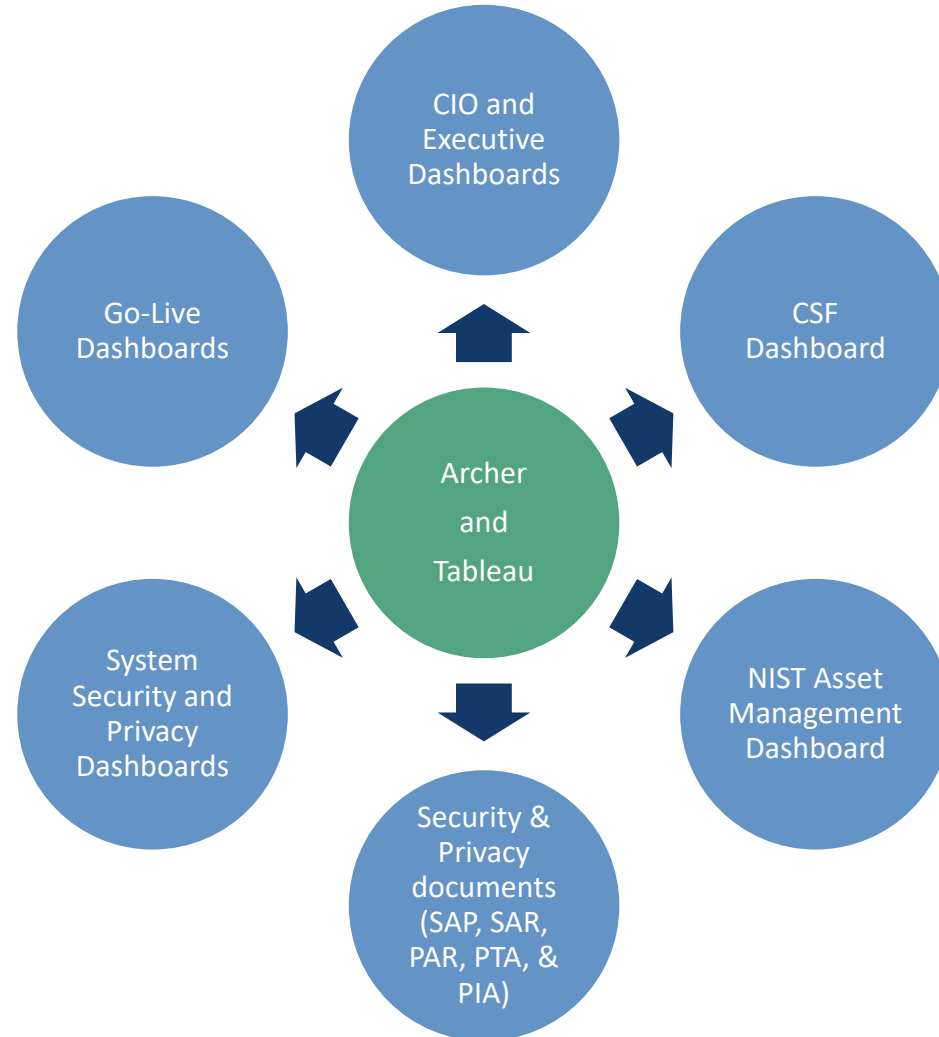
CRS Inputs

These data are ingested into Archer and analyzed for presentation in Tableau.



CRS Outputs

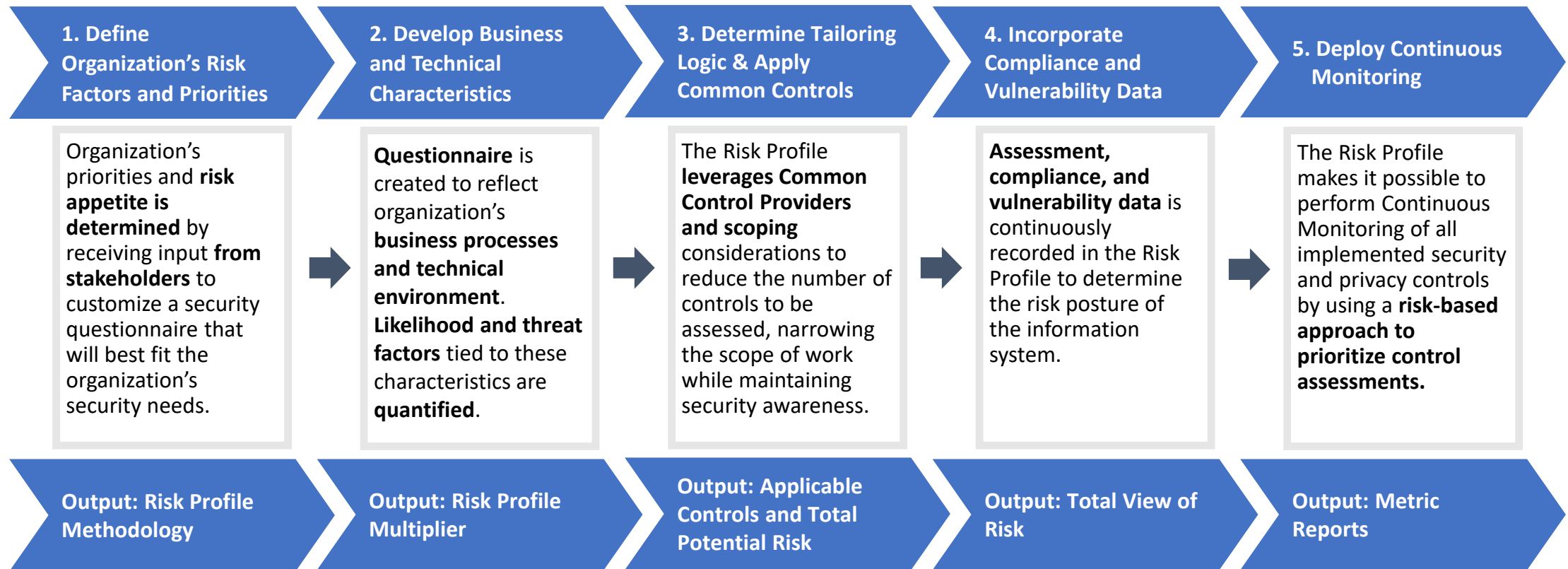
After analysis users can generate ATO documentation on-demand & view metric-based risk management dashboards.



Risk Profiling and Scoring

Risk Profiling Overview

- **Risk Profiling** is a process that allows NIST to determine the **importance of a system** to the **organization's mission**.
- By first understanding the **business and technical characteristics** that impact system risk, an agency can **identify and align controls to a component** based on the likelihood that a weakness will be exploited and the **potential impact to the organization**.



Risk Scoring Variables

Risk Scoring provides a foundation for **quantitative risk-based analysis**, assessment, and reporting of organizational IT assets. By applying ratings to controls and generating scores for components, stakeholders have a **relative understanding of risk** from one system compared to another.

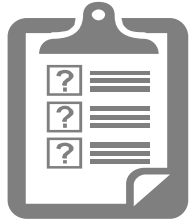
The variables that can affect a control's potential risk score is outlined below.

Variable	Description	Considerations
Control Baseline Risk Score	Every control is assigned an initial weighting (1-10) based on an analysis of its importance to the security and privacy posture.	<ul style="list-style-type: none">• What is the potential security impact of this control to NIST?
Data Type Questionnaire Responses	Initial CIA ratings (1-10) are assigned to controls, based on criticality of the information type(s), upon completion of the Data Type Questionnaire.	<ul style="list-style-type: none">• What is the impact of Confidentiality (C), Integrity (I), and Availability (A) to the types of information that are used within this component?
Risk Profile Questionnaire Responses	Additional adjustments are applied as indicated by responses to the Risk Profile Questionnaire, including business risks.	<ul style="list-style-type: none">• What assets or applications are part of the component?• What is potential security impact of this component to the enterprise?

Risk Calculation Overview

The following steps are completed in Archer for each system component to calculate potential risk.

Complete Questionnaires



Generate Risk Profile



Calculate Risk Score



- **Data Type Questionnaire:** Determines an overall system security category for the component, assigns the security control “baseline” (Low/Moderate/High), and calculates initial risk score modifier.
- **Risk Profile Questionnaire:** Performs additional control scoping and calculates final risk score modifiers for the resulting set of applicable controls.

- The Risk Profile outlines the **controls** that should be implemented.
- Security controls are assigned **ratings** for Confidentiality, Integrity, and Availability to quantify risks.
- Components are **assessed** based on their implementation of these controls.

- The **sum** of all Component potential risk equals the **System potential risk**
- Final scores include a **multitude of security inputs** (e.g., manual inputs, vulnerabilities, compliance scans).
- Risk scores create the ability to make **“apples-to-apples” comparisons** across the enterprise.

Information Security Continuous Monitoring and Ongoing Authorization Approach

ISCM promotes more frequent and targeted monitoring of system security and privacy posture to enable risk-based Ongoing Authorization (OA) decisions.

Through CRS, NIST implements ISCM and OA by:

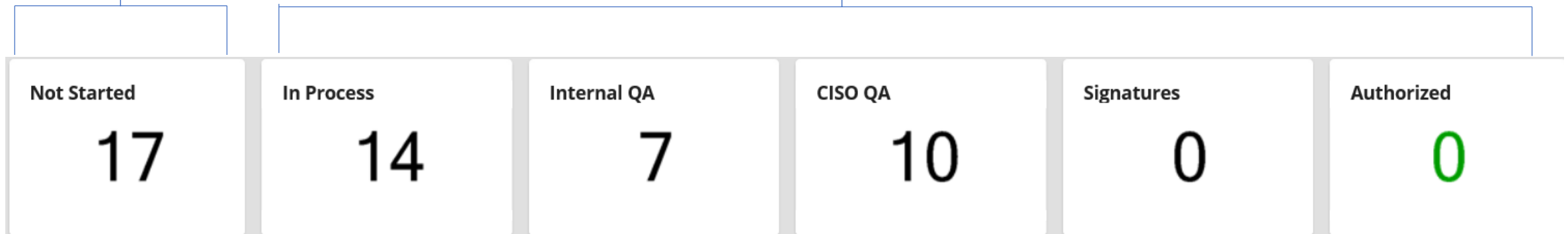
- Prioritizing the set of controls to be evaluated for each assessment
- Providing on-demand reporting of security and privacy metrics (SARs, SAPs, PAPs, and PARs) and management dashboard summaries

NIST System ATO Schedule

- NIST has 46 operational systems + Common Controls
- NIST System ATOs are on a semi-annual ATO Cycle
- ATO status is managed in Cyber Risk Scoring solution (Archer)

ATOs Expirations ~9/30

ATOs Expirations ~4/1



ISCM Schedule for Security Controls





Security control assessments are prioritized based on importance to the organization (DoC Volatile Controls and Common Controls) and number of potential risk points.































Sample Assessment Schedule

Automated Assessments

Assessment Type	Scan Frequency
Vulnerabilities	Weekly
Compliance Scans	Monthly
Web Applications	Annually and as needed

Manual Assessments*

-  Full control set assessed annually
-  Half of the control set is assessed each year
-  One third of the control set is assessed each year
-  One sixth of the control set is assessed each year

Controls	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
DoC Volatile Controls						
Common Controls						
High Risk Controls*						
Moderate Risk Controls*						
Low Risk Controls*						

*Risk score ranges were determined by calculating baseline risk score multipliers

Assessment Process

System Level Data

Archer captures system information that supports ongoing assessment and authorization efforts.

General ST&E Activities High Level Findings POA&Ms Accepted Risks System Artifacts PTA/PIA SAP PAP ISCM FY2021 ISCM FY2020

GENERAL INFORMATION

* System ID: Updated by on 11/16/2015 10:41:53 AM

* System Name: Updated by Enloe, Christian on 3/26/2020 12:54:06 PM

Division:

Compliant:

System Operational Status (CSAM):

* CSAM ID: Updated by Kiran, Santi on 7/27/2016 12:49:30 PM

Last Authorization Date:

ATO Expiration Date: 10/30/2021

PIA SAOP Authorized Date:

WebInspect VSA Start Date:

System Description: The NIST Director's Office (DO) System supports the day-to-day functions of the NIST DO suite, NIST Office of General Counsel, Executive Officer for Administration and all related divisions/offices, Chief of Staff and all related divisions/offices, and the three Associate Director's (AD) top level offices.

The Divisions covered within the scope of this system are as follows:

Division Number	Staff Office Name
100	Director's Office; Office of the Chief Counsel; Executive Officer for Administration; Office of the Chief of Staff; Onboarding Office
101	Management and Organization Office

System Migrated To Archer?: Yes

Overall System Security Category: Moderate

Overall Confidentiality: Moderate

Overall Integrity: Moderate

Overall Availability: Low

Contains PII?: No

Contains BII?: No

Tailored Control Set

Upon completion of the questionnaires, each component is provided with a tailored set of controls.

Component :

[EDIT](#)
[VIEW](#)
[SAVE](#)
[SAVE AND CLOSE](#)

First Published: 6/1/2017 3:49 PM Last Updated: 9/24/2020 11:04 AM

Control Family	Control Number	Control Name	Baseline	Control Applicability	Assessment Date	Control Status
Access Control	AC-1	Access Control Policy and Procedures	Low Moderate High	Hybrid	7/26/2019	
Access Control	AC-2	Account Management	Low Moderate High	Applicable	7/19/2019	Satisfied
Access Control	AC-2(1)	Automated System Account Management	Moderate High	Applicable	7/19/2019	Satisfied
Access Control	AC-2(2)	Removal of Temporary/Emergency Accounts	Moderate High	Applicable	7/26/2019	Satisfied
Access Control	AC-2(3)	Disable Inactive Accounts	Moderate High	Applicable	7/19/2019	Satisfied
Access Control	AC-2(4)	Automated Audit Actions	Moderate High	Applicable	7/19/2019	Satisfied

Tailored Controls : AC-2

[EDIT](#)
[VIEW](#)
[SAVE](#)
[SAVE AND CLOSE](#)

First Published: 6/2/2017 10:19 PM Last Updated: 8/20/2019 9:43 AM

General	Risk Scores	CCP Implementation Statement										
<p>▼ RISK SCORES</p> <table border="0"> <tr> <td>Potential Risk - (SOR): 284</td> <td>Potential Risk: 284</td> </tr> <tr> <td>Mitigated Risk - (SOR): 284</td> <td>Mitigated Risk: 284</td> </tr> <tr> <td>Residual Risk - (SOR): 0</td> <td>Residual Risk: 0</td> </tr> <tr> <td>Residual Risk - Accept Risk (SOR): 0</td> <td>Risk - Accept Risk: 0</td> </tr> <tr> <td>Residual Risk - POA&M (SOR): 0</td> <td>Residual Risk - POA&M: 0</td> </tr> </table>			Potential Risk - (SOR): 284	Potential Risk: 284	Mitigated Risk - (SOR): 284	Mitigated Risk: 284	Residual Risk - (SOR): 0	Residual Risk: 0	Residual Risk - Accept Risk (SOR): 0	Risk - Accept Risk: 0	Residual Risk - POA&M (SOR): 0	Residual Risk - POA&M: 0
Potential Risk - (SOR): 284	Potential Risk: 284											
Mitigated Risk - (SOR): 284	Mitigated Risk: 284											
Residual Risk - (SOR): 0	Residual Risk: 0											
Residual Risk - Accept Risk (SOR): 0	Risk - Accept Risk: 0											
Residual Risk - POA&M (SOR): 0	Residual Risk - POA&M: 0											

Control Assessment Input

Assessors can document assessment results and supporting details in this interactive form.

MANUAL AND AUTOMATED ASSESSMENT INPUT FORM | Cancel | Options

Component Name 2	Overall Component Security Category	Associated System 1	Assessment Scope
---------------------	-------------------------------------	------------------------	------------------

Associated System:

Low	ISCM
-----	------

Control Number	Baseline	Assessment Date	Control Assessment Type	Control Criticality	ISCM FY	Control Name	Control Applicability	Control Applicability Override	Reason for Override	Control Inherited from CCP	Control Status	New Assessment Result	Assessment Method	Assessment Details
AC-2	Low Moderate High	10/14/2020	Security	Volatile	2021	Account Management	Applicable				Satisfied	Satisfied	Examine	

1 2 ▶

Go to Page

SAP/SAR Generation

The images below show the Security Assessment Plan (SAP) and Security Assessment Report (SAR) Assessors complete in Archer. Upon completion of assessments, the documentation is generated directly from Archer.

Security Assessment Plan

Index	Component	Control Number	Control Name	Assessment Date	ISCM FY	Control Applicability	Control Applicability Override	Reason for Override	Control Inherited from	Control Status	New Assessment Result	Assessment Method
1		AC-1	Access Control Policy and Procedures	7/26/2019	2024	Hybrid	Hybrid		CCP Div 181 (OSM IT Sec: ury Policies)			Examine
1		AC-1	Access Control Policy and Procedures	8/13/2019	2024	Hybrid	Hybrid		CCP Div 181 (OSM IT Sec: ury Policies)	Satisfied	Satisfied	Examine

Security Assessment Report

System ID: [REDACTED]
System Name: [REDACTED]
Division: [REDACTED]
Compliant:

System Operational Status (CSAM): Operational

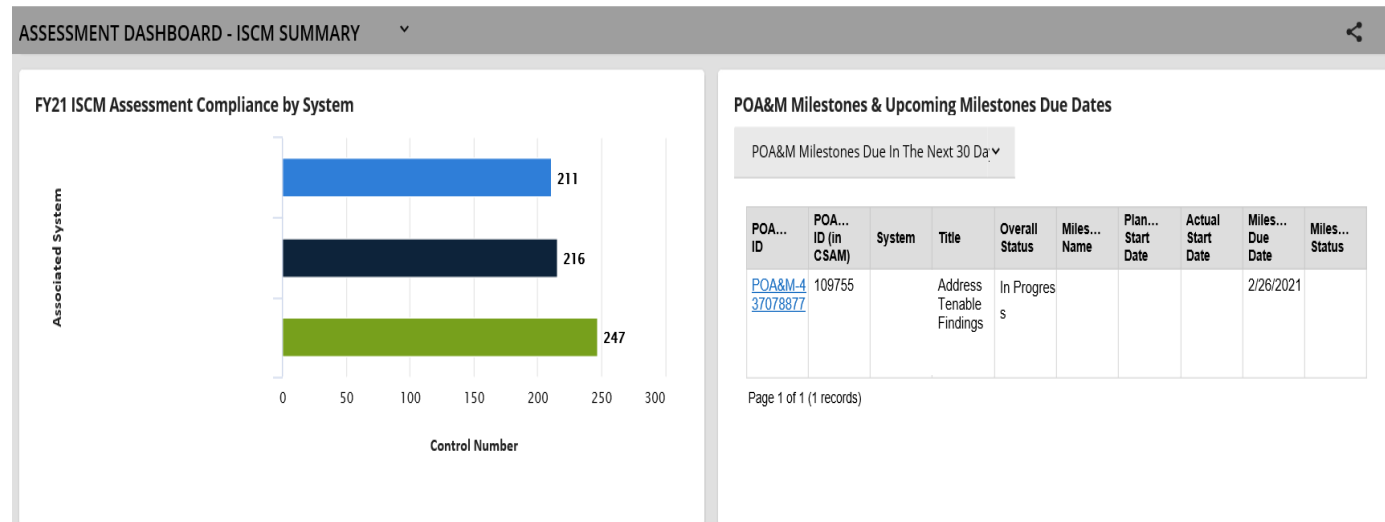
System Description: General Description/Purpose of System:
The system contains the hardware and software required by the developing and maintaining, supporting the implementation of, diverse environment and complying with applicable laws and regulations. Add
The hardware of the 150-01 system consists of the following comp

CSAM ID: 2325
Last Authorization Date: 4/1/2020
ATO Expiration Date: 4/1/2021
PIA SAOP Authorized Date: 9/30/2019
Webinspect VSA Start Date: [REDACTED]

Sample Assessor & Management Dashboards

In Archer, role-based dashboards display task prioritization and management of A&A activities.

Assessor Dashboard



Management Dashboard

A&A SYSTEM METRICS DASHBOARD

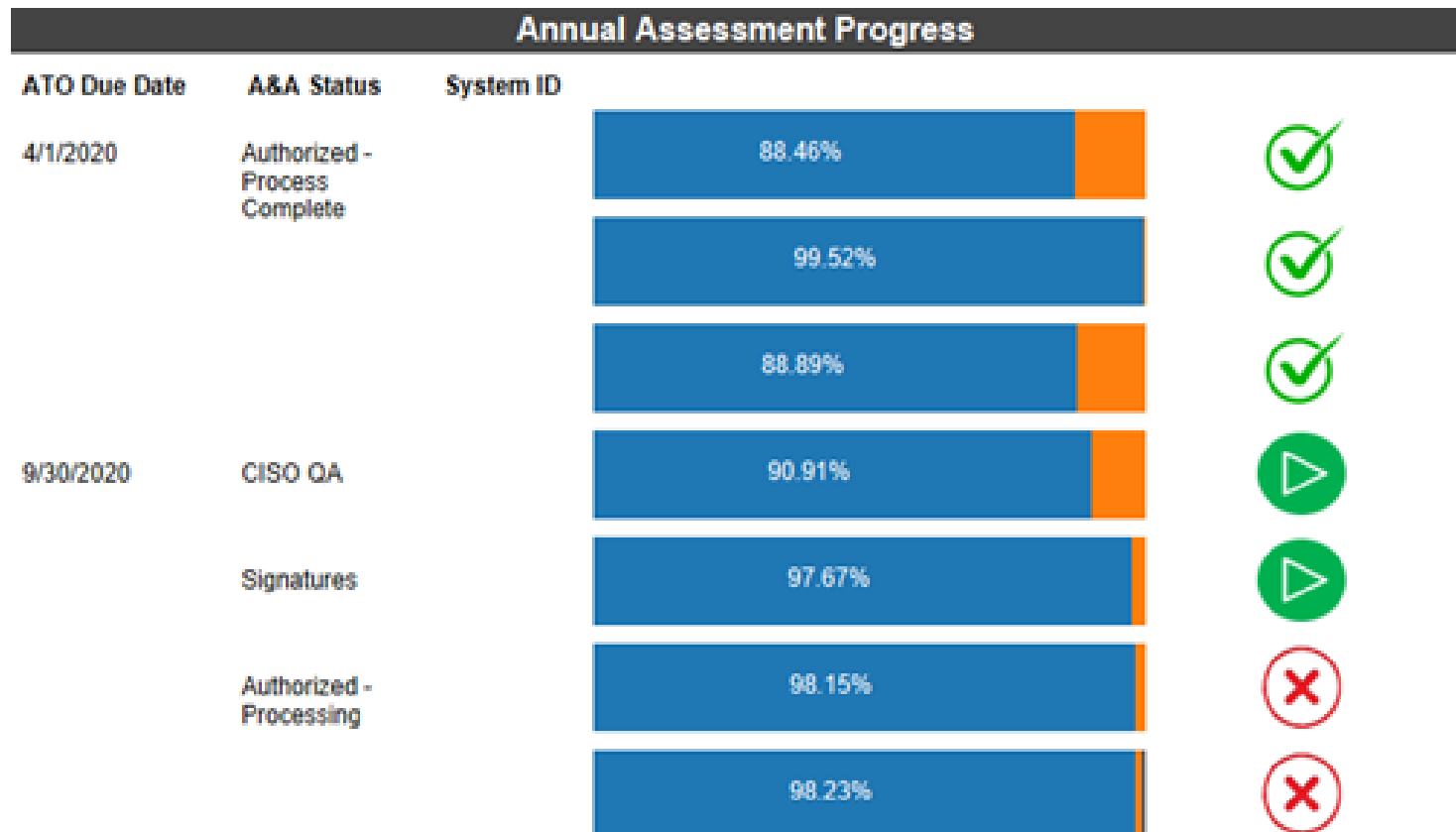
System A&A Summary Reports

A&A Status - OISM Management - FY2020

Schedule	System	A&A Schedule Comment	A&A Status	Current Responsible	ATO Due Date	Personally Identifiable Information (PII)?	PIA Due to DOC	NIST: Primary Security Assessor (A&A)
Annual Assessment - Annual Assessment - FY2020			Authorized - Process Complete	A&A Coordinator	4/1/2020	Yes		Moore, Maureen
Annual Assessment - Annual Assessment - FY2020		Files need to be uploaded to CSAM.	Authorized - Process Complete	A&A Coordinator	4/1/2020	Yes		Vijayaverl, Rathini
Annual Assessment - Annual Assessment - FY2020		Files need to be uploaded to CSAM.	Authorized - Process Complete	A&A Coordinator	4/1/2020	Yes		Repaci, Jonathan

ISCM Status Tracker

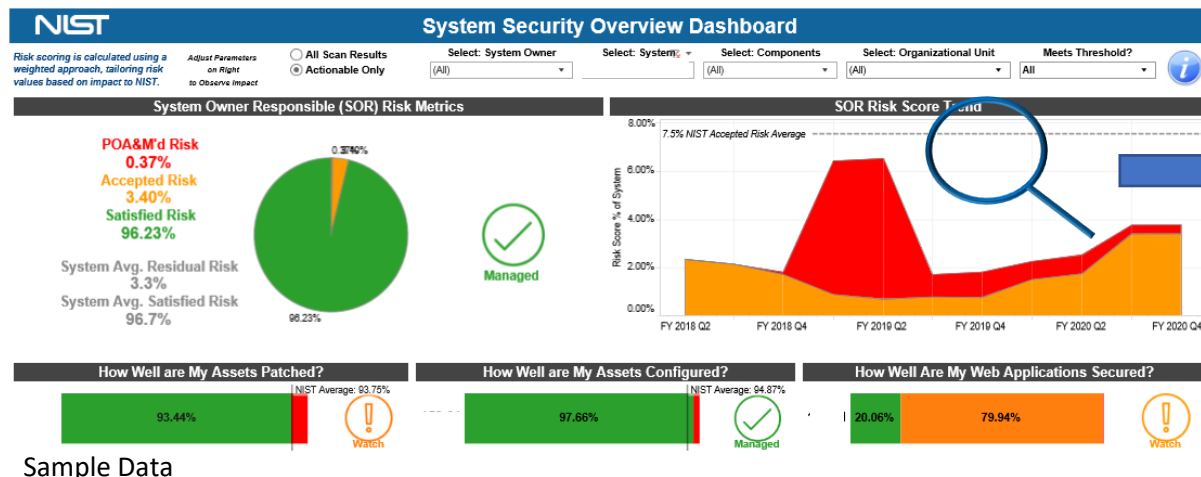
In Tableau, the Annual Assessment Progress report displays status of ISCM assessments by system.



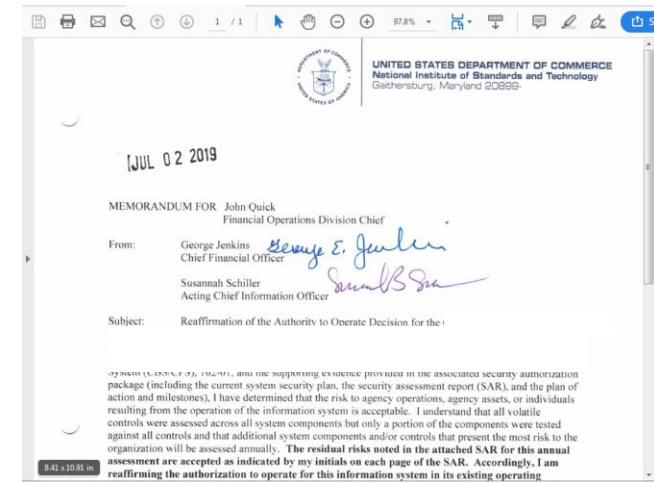
Ongoing Authorization

Historical data was evaluated to create initial risk thresholds in support of Ongoing Authorization decisions.

- Current threshold: **NIST-wide Accepted Risk Average (all time)**
- SOs and AOs can review a system's current security posture and risk trend:
 - Risk scores **at or below** the NIST average threshold could result in automatic reauthorization
 - Risk scores that **exceed** the threshold may require further review and discussion



Sample Data



Privacy

Aligning Privacy with CRS

Privacy capabilities have been integrated into the CRS Solution to standardize security and privacy processes across NIST.

End users can complete the following privacy activities in CRS:

- Automate control assignments (NIST SP 800-53 Rev. 4, Appendix J.) for systems that contain PII
- Complete and generate on-demand DOC-required forms such as Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and Annual Recertification
- Perform privacy control assessments and generate required documentation on-demand (Privacy Assessment Report and Privacy Assessment Plan)
- Quantify privacy risk based on CRS's scoring methodology

Privacy objectives (Predictability, Manageability, and Disassociability) scores are added together to calculate the Total Potential Risk for a single privacy control.

Integrating CRS with Privacy

The following steps are completed in Archer for each system component to maintain privacy documentation and allocate applicable controls.

Complete PTA



- A **PTA** is **required** for every system
- The **PTA** determines if a **PIA** is **required**
- CRS incorporates the **current DOC PTA template**



Complete PIA



- The **PIA** collects information about the types of **privacy data** which is **stored and processed, why** it is collected, and **how** it is handled
- **Privacy controls** are **allocated as determined by the PIA**



Generate Annual PIA Recertification Form



- The **PIA recertification form** is generated annually for ongoing authorization
- It also ensures that any **changes** to the **Systems, Components**, or privacy risks are identified and mitigated

PTA/PIA Generation

The images below show the PTA and PIA Questionnaires ISSOs complete in Archer. Upon completion of the questionnaires, the PIA, PTA, and PIA Recertification forms are generated from Archer.

PTA and PIA Questionnaires

The screenshot shows the Archer interface for completing PTA and PIA questionnaires. It features a sidebar with navigation options like 'PTA GENERAL QUESTIONS', 'INFORMATION IN THE SYSTEM', and 'PERSONALLY IDENTIFIABLE INFORMATION (PII)'. The main content area displays several questions with radio button options. For example, PIA-1 asks 'What is the status of this information system?' with options for 'new information system', 'existing system with changes', or 'existing system with no changes'. PTA-1 asks 'What is the status of this information system?' with more detailed options. PTA-2 asks 'Is the IT system or its information used to support any activity which may raise privacy concerns?' with 'Yes' or 'No' options. PTA-3 asks 'Does the IT system collect, maintain, or disseminate business identifiable information (BII)?' with 'Yes' or 'No' options. PTA-4 asks 'Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?' with 'Yes' or 'No' options. At the bottom, there is a table for 'PTA SUPPORTING ARTIFACTS' with columns for Name, Size, Type, Upload Date, Downloads, and History.

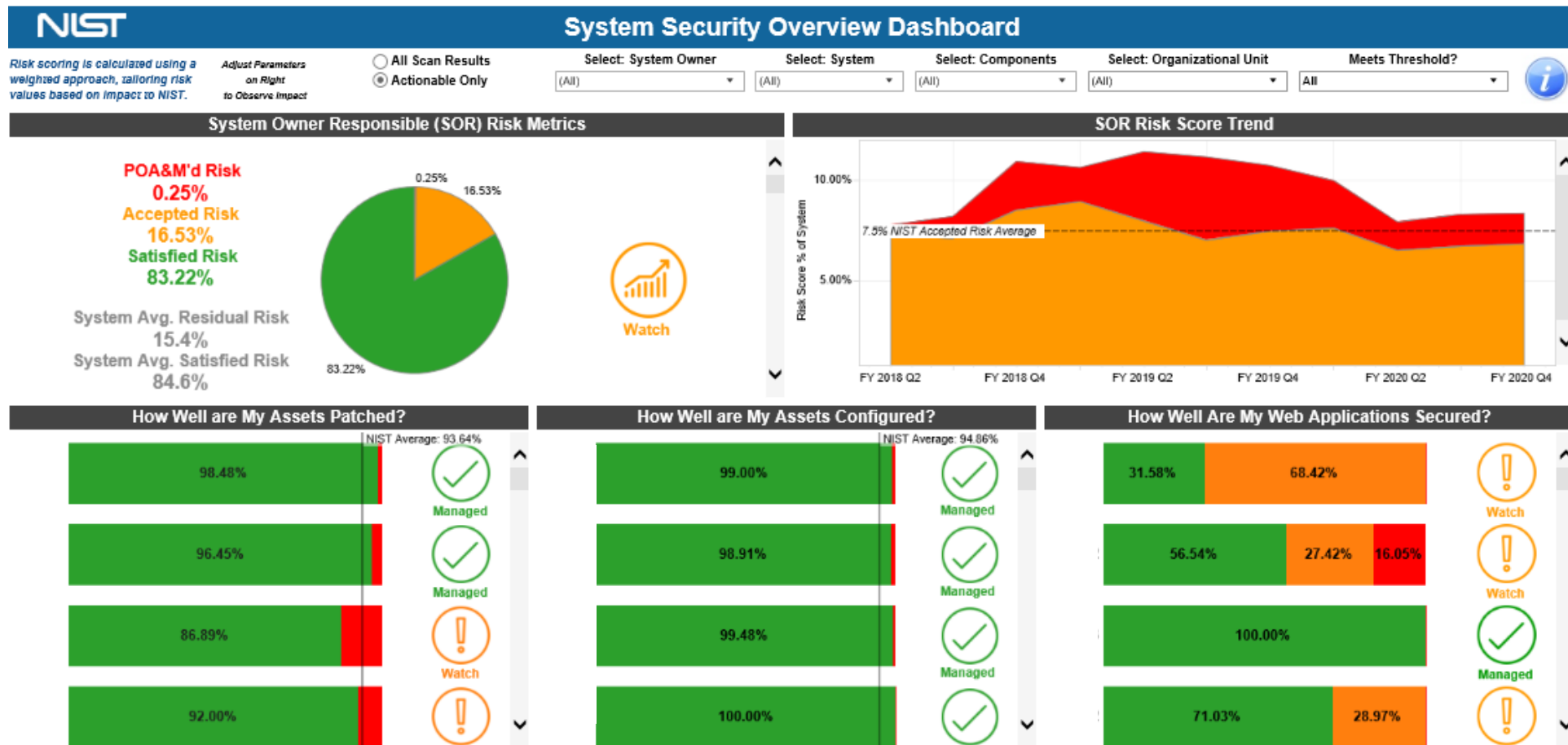
PIA, PTA, and PIA Recertification forms

The image displays three generated forms from Archer. The top form is the 'U.S. Department of Commerce Privacy Threshold Analysis' (PTA) form, version 01-2019, from NIST. It includes a 'Unique Project Identifier' section and an 'Introduction' section. The middle form is the 'U.S. Department of Commerce Privacy Impact Assessment' (PIA) form, version 01-2019, from NIST. It includes an 'Introduction' section and a 'Description of the Information' section. The bottom form is the 'U.S. Department of Commerce Privacy Impact Assessment' (PIA) 'ANNUAL REVIEW CERTIFICATION FORM', version 01-2019, from NIST. It includes a 'Date of PIA Review' field (09/28/2019), a 'Name of System Owner' field (Couch, Charles), a 'Signature of System Owner' field, a 'Date of Privacy Act (PA) Review' field, a 'Name of Reviewer' field (Fletcher, Catherine S., Privacy Act Officer), a 'Signature of Privacy Act (PA) Reviewer' field, a 'Date of BCPO Review' field, a 'Name of the Reviewing Bureau Chief Privacy Officer (BCPO)' field (Schiller, Susannah), a 'Signature of the Bureau Chief Privacy Officer' field, and a date field (January 2018).

Enterprise Management Dashboards

Enterprise System Security Dashboard

The Tableau dashboards supports NIST in maintaining ongoing awareness of information security and privacy to support organizational risk management decisions.

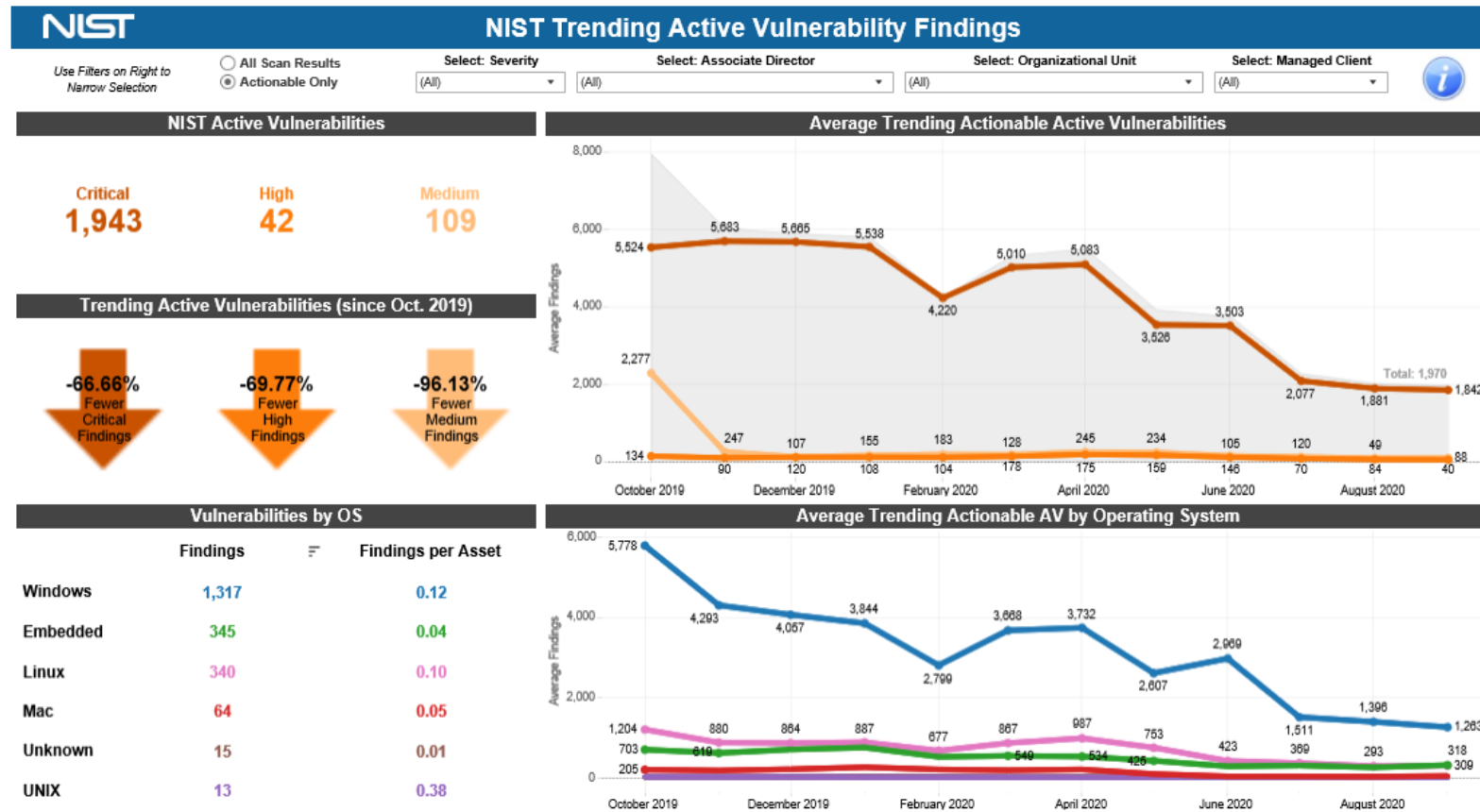


Data last refreshed from CRS on: 9/4/2020 6:51:16 AM

Enterprise Vulnerability Trending Dashboard

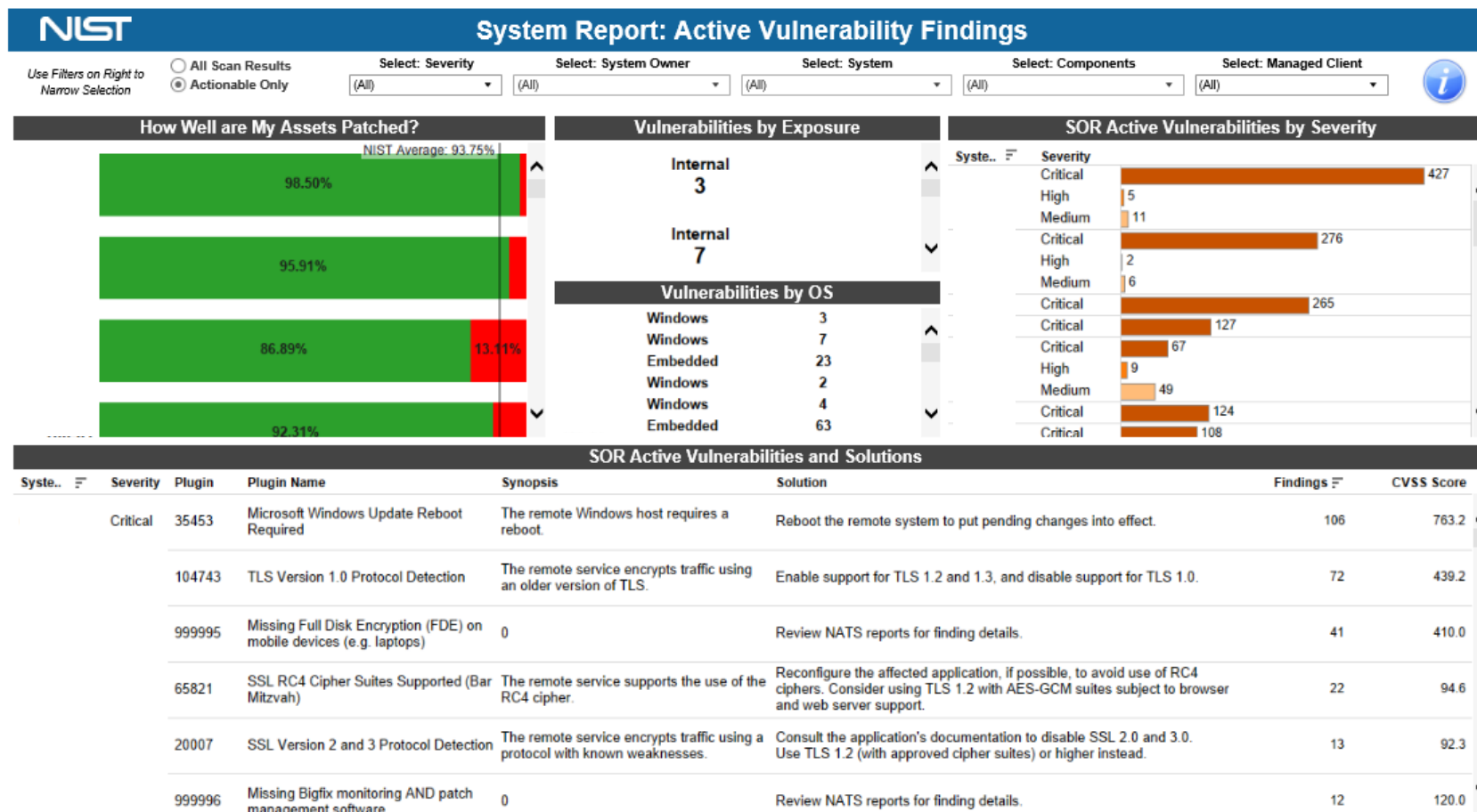


The dashboard below summarizes the organization's active vulnerability trends over the past year.



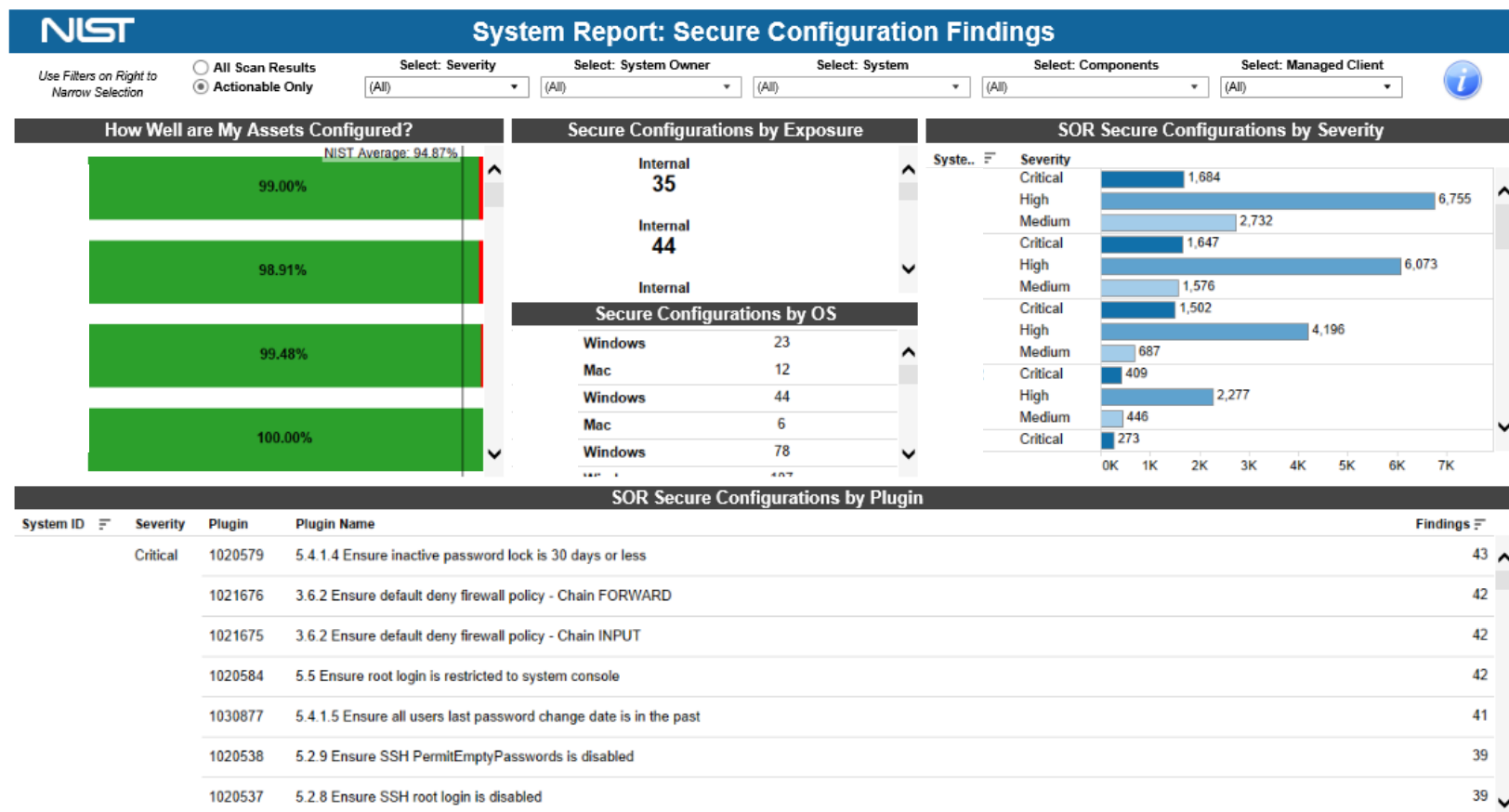
Enterprise Vulnerabilities Dashboard

The dashboard below summarizes vulnerability scan results by system and categorizes vulnerabilities by severity exposure.



Enterprise Secure Configuration Dashboard

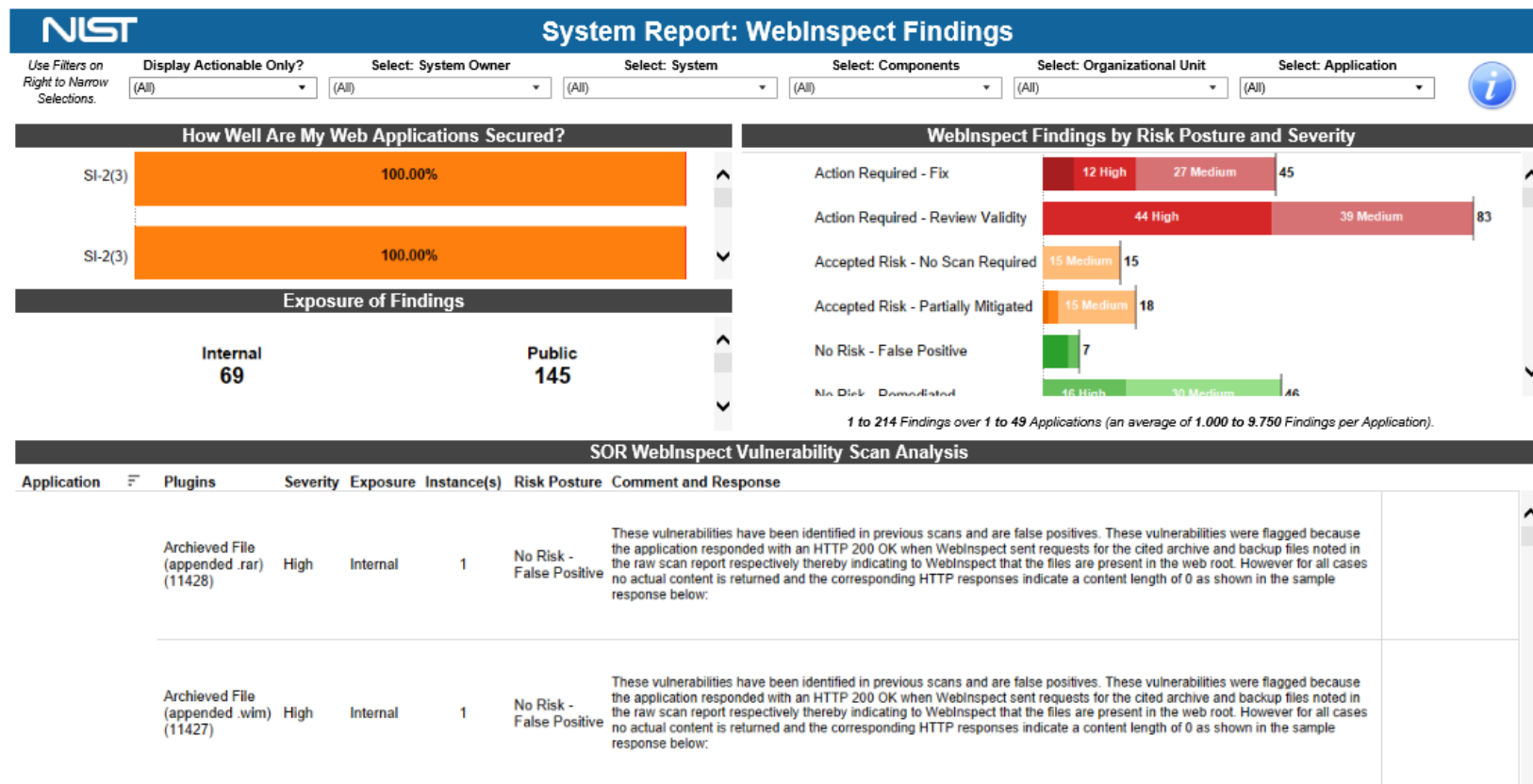
The dashboard below summarizes secure configuration scan results by system and categorizes findings by severity and exposure.



Enterprise Web Vulnerability Dashboard



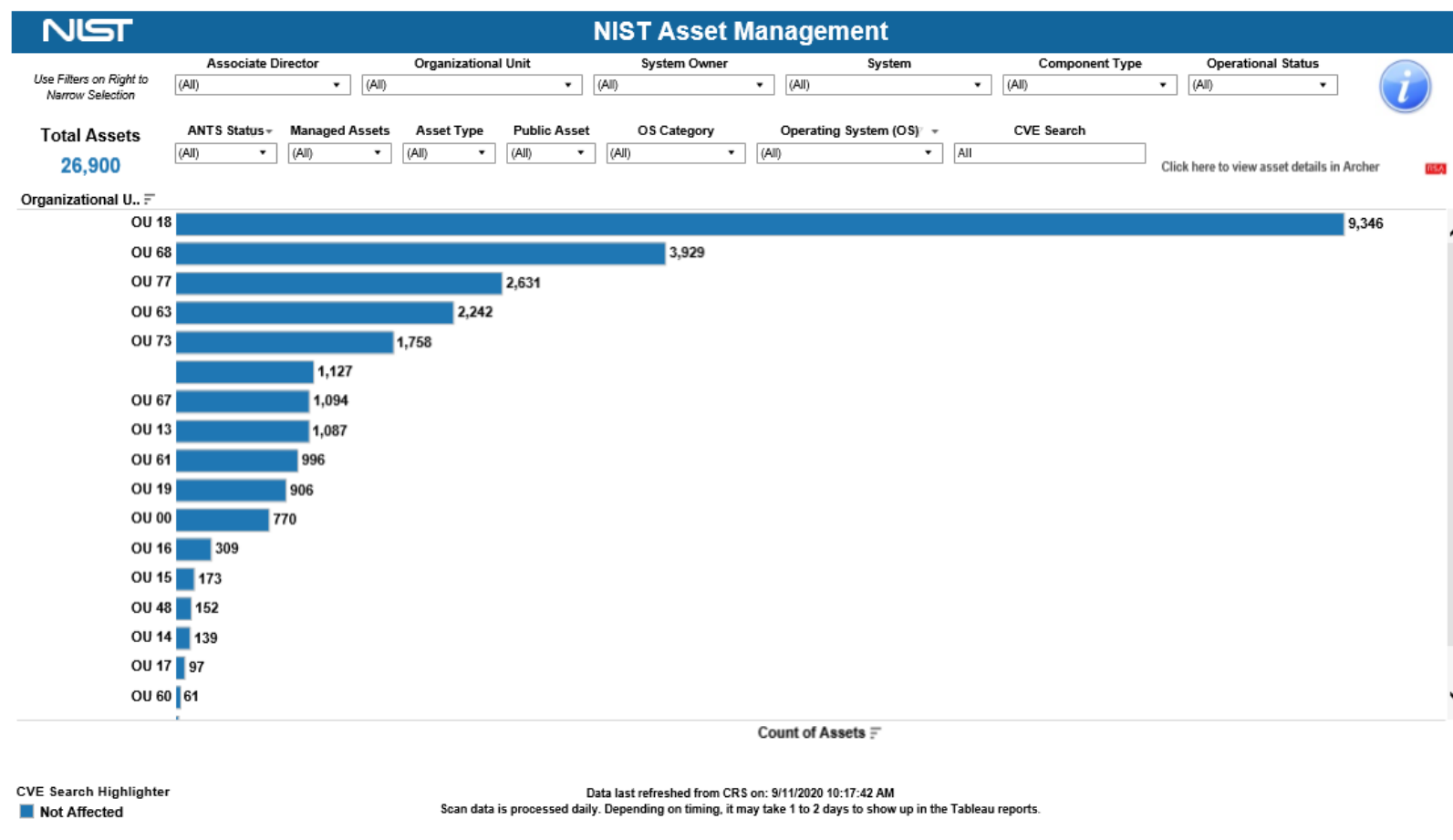
The dashboard below summarizes WebInspect scan results by system and indicates web application vulnerabilities by risk posture and severity.



Enterprise Asset Management Dashboard

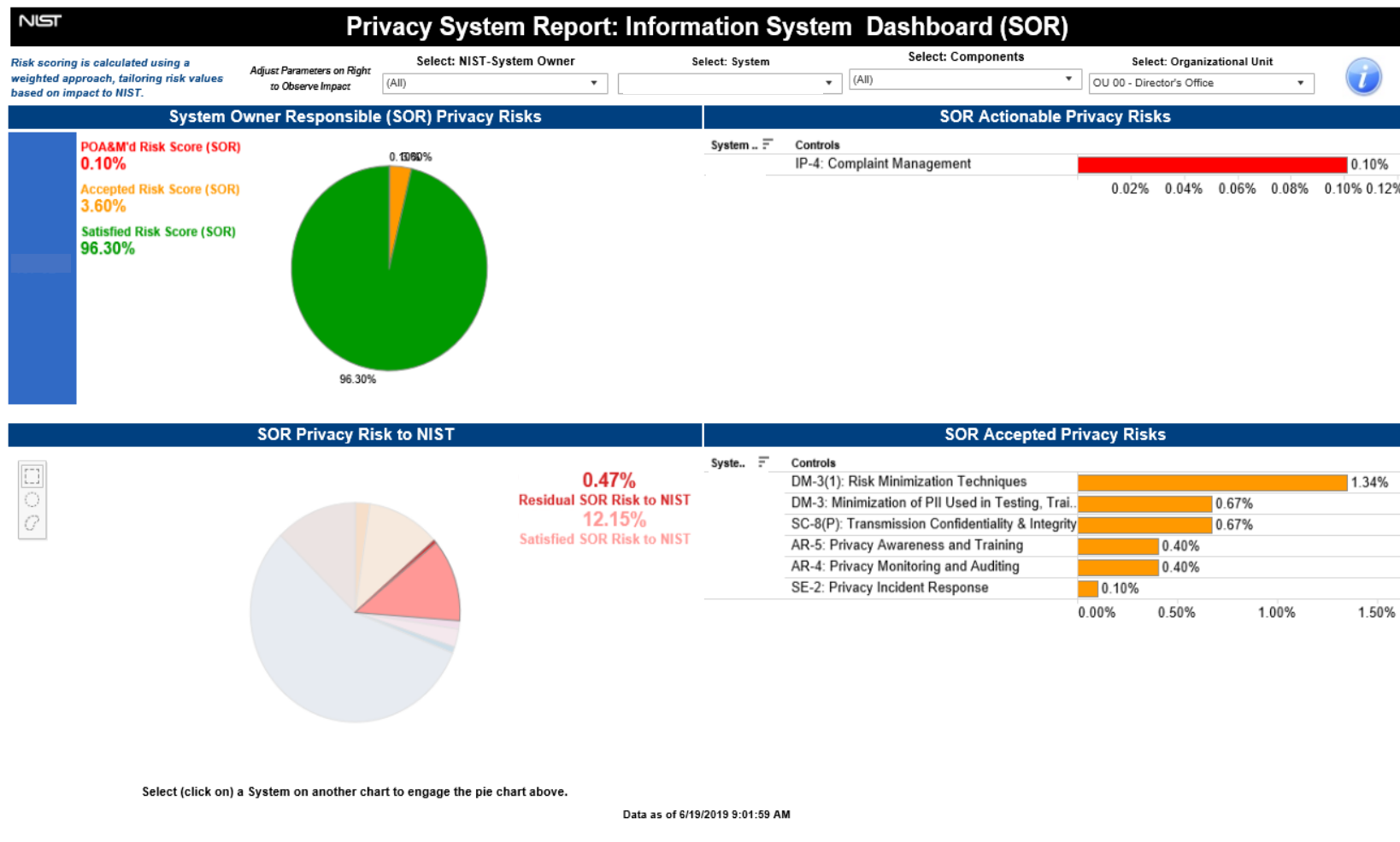


The dashboard below displays the total number of assets within the organization and allows end users to search by CVE number to identify assets impacted by specific vulnerabilities.



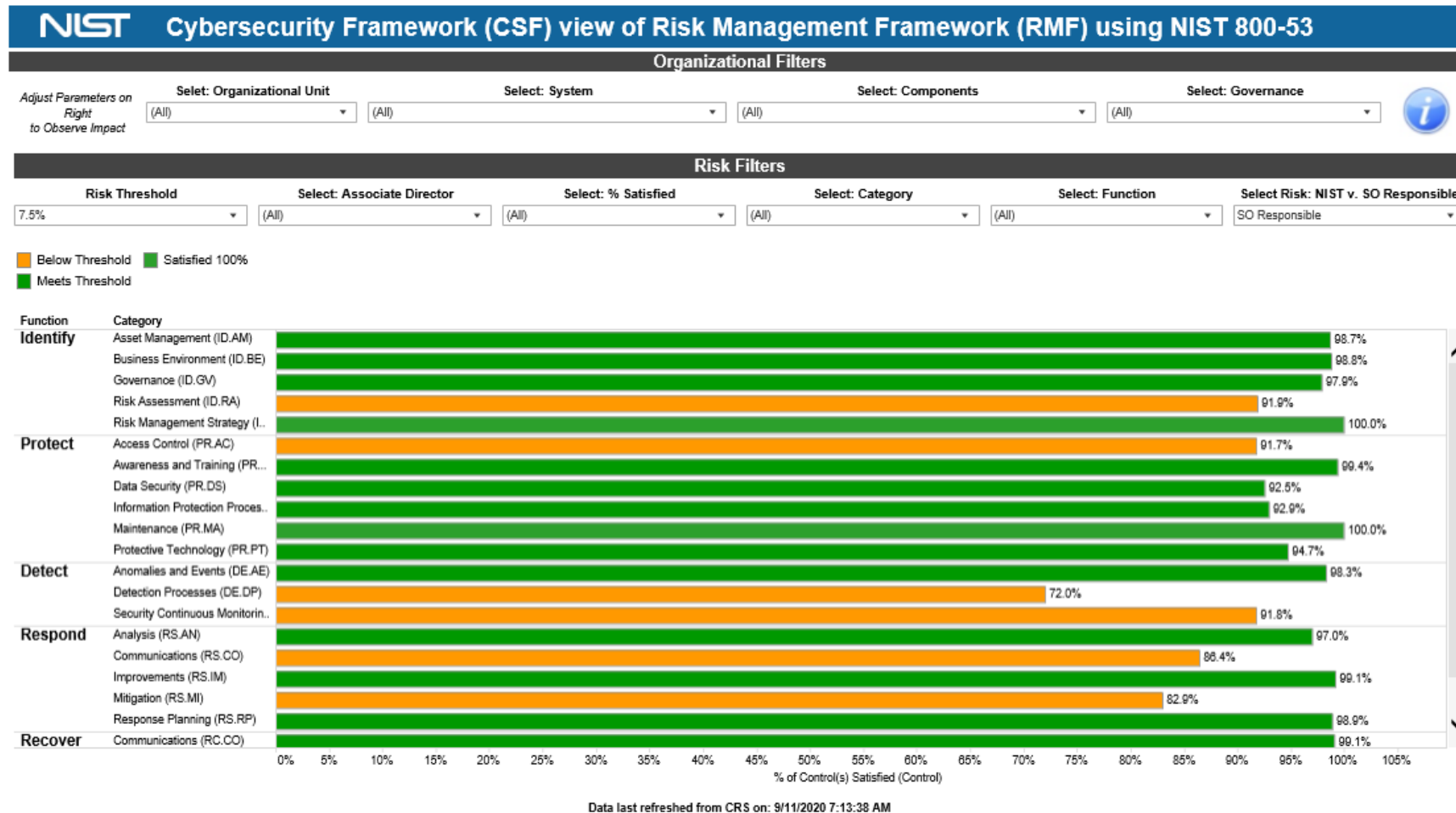
System Privacy Dashboard

The dashboard below summarizes privacy risk metrics for system stakeholders.



Cybersecurity Framework Dashboard

The dashboard below represents the organization's performance against each function and category within the CSF.



Questions?

Chris Enloe

Christian.Enloe@nist.gov

Sheldon Pratt

Sheldon.Pratt@nist.gov

Santi Kiran

Santi.Kiran@nist.gov

John Cascio

John.Cascio@nist.gov