NIST Cyber Risk Scoring (CRS)

Program Overview

February 2021
Agenda

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

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

1. **Define Organization’s Risk Factors and Priorities**
   - Organization’s priorities and risk appetite is determined by receiving input from stakeholders to customize a security questionnaire that will best fit the organization’s security needs.
   - Output: Risk Profile Methodology

2. **Develop Business and Technical Characteristics**
   - Questionnaire is created to reflect organization’s business processes and technical environment. Likelihood and threat factors tied to these characteristics are quantified.
   - Output: Risk Profile Multiplier

3. **Determine Tailoring Logic & Apply Common Controls**
   - The Risk Profile leverages Common Control Providers and scoping considerations to reduce the number of controls to be assessed, narrowing the scope of work while maintaining security awareness.
   - Output: Applicable Controls and Total Potential Risk

4. **Incorporate Compliance and Vulnerability Data**
   - Assessment, compliance, and vulnerability data is continuously recorded in the Risk Profile to determine the risk posture of the information system.
   - Output: Total View of Risk

5. **Deploy Continuous Monitoring**
   - The Risk Profile makes it possible to perform Continuous Monitoring of all implemented security and privacy controls by using a **risk-based approach to prioritize control assessments**.
   - Output: Metric Reports
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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Baseline Risk Score</td>
<td>Every control is assigned an initial weighting (1-10) based on an analysis of its importance to the security and privacy posture.</td>
<td>• What is the potential security impact of this control to NIST?</td>
</tr>
<tr>
<td>Data Type Questionnaire Responses</td>
<td>Initial CIA ratings (1-10) are assigned to controls, based on criticality of the information type(s), upon completion of the Data Type Questionnaire.</td>
<td>• What is the impact of Confidentiality (C), Integrity (I), and Availability (A) to the types of information that are used within this component?</td>
</tr>
<tr>
<td>Risk Profile Questionnaire Responses</td>
<td>Additional adjustments are applied as indicated by responses to the Risk Profile Questionnaire, including business risks.</td>
<td>• What assets or applications are part of the component? • What is potential security impact of this component to the enterprise?</td>
</tr>
</tbody>
</table>
The following steps are completed in Archer for each system component to calculate potential risk.

**Complete Questionnaires**
- 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.

**Generate Risk Profile**
- 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.

**Calculate Risk Score**
- 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 and OA Overview

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)

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>17</td>
</tr>
<tr>
<td>In Process</td>
<td>14</td>
</tr>
<tr>
<td>Internal QA</td>
<td>7</td>
</tr>
<tr>
<td>CISO QA</td>
<td>10</td>
</tr>
<tr>
<td>Signatures</td>
<td>0</td>
</tr>
<tr>
<td>Authorized</td>
<td>0</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Scan Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>Weekly</td>
</tr>
<tr>
<td>Compliance Scans</td>
<td>Monthly</td>
</tr>
<tr>
<td>Web Applications</td>
<td>Annually and as needed</td>
</tr>
</tbody>
</table>

### Automated 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**

### Manual Assessments*

<table>
<thead>
<tr>
<th>Controls</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Year 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoC Volatile Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Risk Controls*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate Risk Controls*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Risk Controls*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Risk score ranges were determined by calculating baseline risk score multipliers.
Assessment Process
Archer captures system information that supports ongoing assessment and authorization efforts.

### System Level Data

<table>
<thead>
<tr>
<th>Division</th>
<th>Staff Office Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Director's Office, Office of the Chief Counsel, Executive Officer for Administration, Office of the Chief of Staff, Onboarding Office</td>
</tr>
<tr>
<td>101</td>
<td>Management and Organization Office</td>
</tr>
</tbody>
</table>

**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:** 100 Director's Office

**Compliant:**
- Operational

**System Operational Status (CSAM):** Operational

**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, and the three Associate Director's (AD) top level offices.

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

<table>
<thead>
<tr>
<th>Division Number</th>
<th>Staff Office Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Director's Office, Office of the Chief Counsel, Executive Officer for Administration, Office of the Chief of Staff, Onboarding Office</td>
</tr>
<tr>
<td>101</td>
<td>Management and Organization Office</td>
</tr>
</tbody>
</table>

**System Migrated To Archer:** Yes

**Overall System Security Category:** Moderate

**Overall Confidentiality:** Moderate

**Overall Integrity:** Moderate

**Overall Availability:** Low

**CSAM ID:** 2352
- Updated by Kiran, Santi on 7/27/2016 12:49:30 PM

**Last Authorization Date:** 10/30/2020

**ATO Expiration Date:** 10/30/2021

**PIA SAAP Authorized Date:**

**WebInspect VSA Start Date:**

**Contains PII:** No

**Contains BII:** No
Upon completion of the questionnaires, each component is provided with a tailored set of controls.
Assessors can document assessment results and supporting details in this interactive form.
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.
In Archer, role-based dashboards display task prioritization and management of A&A activities.

**Assessor Dashboard**

**Management Dashboard**
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
Privacy
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
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.
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.
The dashboard below summarizes the organization’s active vulnerability trends over the past year.
The dashboard below summarizes vulnerability scan results by system and categorizes vulnerabilities by severity exposure.
The dashboard below summarizes secure configuration scan results by system and categorizes findings by severity and exposure.
The dashboard below summarizes WebInspect scan results by system and indicates web application vulnerabilities by risk posture and severity.
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.
The dashboard below summarizes privacy risk metrics for system stakeholders.

System Privacy Dashboard

Select (click on) a System on another chart to engage the pie chart above.

Data as of 6/18/2019 9:01:59 AM
The dashboard below represents the organization’s performance against each function and category within the CSF.
Questions?
POCs

Chris Enloe
Christian.Enloe@nist.gov

Sheldon Pratt
Sheldon.Pratt@nist.gov

Santi Kiran
Santi.Kiran@nist.gov

John Cascio
John.Cascio@nist.gov