



New Mexico EO: Achieving Cybersecurity Resilience

Webinar

A graphic for a webinar. It features a purple trapezoidal shape on the left containing the Synopsys logo and text. To the right is the Great Seal of the State of New Mexico. The background is a light blue and white grid pattern.

SYNOPSYS

**New Mexico Executive Order:
Achieving Cybersecurity Resilience**

Chrissa Constantine, Sales Engineer, SIG
John Waller, Practice Principal, SIG
2024

The Great Seal of the State of New Mexico, featuring an eagle with wings spread, perched on a cactus, with a banner below it. The seal is circular with the text "GREAT SEAL OF THE STATE OF NEW MEXICO" and "1912" around the perimeter.

Thank You for Joining Our
Synopsis and Carahsoft Webinar:
**New Mexico EO: Achieving Cybersecurity
Resilience in State Agencies**

Welcome!

We will begin at the top of the hour.

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider. Carahsoft has built our reputation as a customer-centric organization dedicated to serving the needs of our technology manufactures, public sector end users, and reseller ecosystem.



Gavin Hockett

Team Lead

571-662-3247

Gavin.Hockett@Carahsoft.com



John Waller

*Cybersecurity Practice Lead
Synopsys*



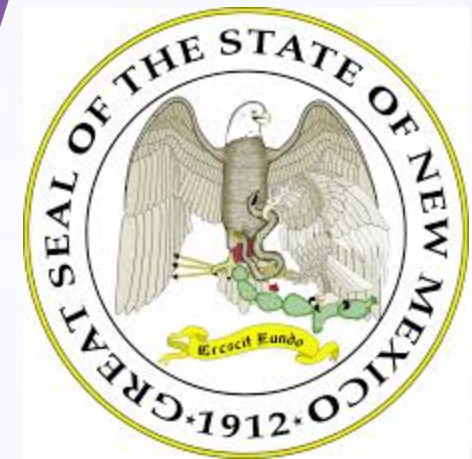
Chrissa Constantine

*Senior Sales Engineer
Synopsys*



New Mexico Executive Order: Achieving Cybersecurity Resilience

Chrissa Constantine, Sales Engineer, SIG
John Waller, Practice Principal, SIG
2024



CONFIDENTIAL INFORMATION

The information contained in this presentation is the confidential and proprietary information of Synopsys. You are not permitted to disseminate or use any of the information provided to you in this presentation outside of Synopsys without prior written authorization.

IMPORTANT NOTICE

In the event information in this presentation reflects Synopsys' future plans, such plans are as of the date of this presentation and are subject to change. Synopsys is not obligated to update this presentation or develop the products with the features and functionality discussed in this presentation. Additionally, Synopsys' services and products may only be offered and purchased pursuant to an authorized quote and purchase order or a mutually agreed upon written contract with Synopsys.

Agenda

- The New Mexico Executive Order 2024-11
- NIST Risk Management Framework (SP 800-53)
- Importance of Cybersecurity Resilience
- Aligning your Cybersecurity Program to NIST
- Building a Comprehensive Security Program
- Q & A

New Mexico Executive Order 2024-11

“The state faces increasingly sophisticated cyber campaigns that threaten our security and our privacy, and we are acting quickly to protect New Mexicans with a robust cyber security infrastructure,” said Governor Lujan Grisham.

Attacks Against Critical Infrastructure: NM Impacts

March 18, 2024:
Letter to State Governors

- [EPA and White House warning](#) to U.S. governors about cyberattacks capable of *disabling* water facilities
- Letter cited targeted attacks against critical infrastructure in the U.S.
- Ransomware Activity (2020-2023)
 - Targets critical infrastructure in New Mexico
- NM PRC Cybersecurity (2022)
26 utilities ranked 1-3
 - 16 level 1
 - 6 level 2
 - **4 out of 26: level 3 (likely to withstand threats)**

EXECUTIVE ORDER 2024-011

STRENGTHENING STATE AGENCY CYBERSECURITY

WHEREAS, a surge in cybersecurity breaches and hacks poses a severe threat to the integrity of sensitive information held by state agencies;

WHEREAS, recognizing the escalating nature of cyber threats, there is an urgent need to fortify the defenses of New Mexico's state agencies against potential cyber intrusions;

WHEREAS, the protection of citizen data and critical infrastructure requires immediate and comprehensive action to enhance cybersecurity measures; and

WHEREAS, implementing and enforcing strengthened cybersecurity requirements will bolster the overall resilience of state agencies in the face of evolving cyber threats.

Impact of New Mexico Executive Order 2024-11

- The state's Department of Information Technology is directed to conduct thorough IT and security assessments on state agencies to detect security vulnerabilities
- Agencies **must** implement cybersecurity, information security & privacy policies that are *at least moderate impact* by the National Institute of Standards and Technology
- Agencies must **certify compliance by November 1, 2024 and Annually thereafter**
- From <https://statescoop.com/new-mexico-michelle-lujan-grisham-cybersecurity-executive-order-2024/>

2023 State of New Mexico Cybersecurity Plan

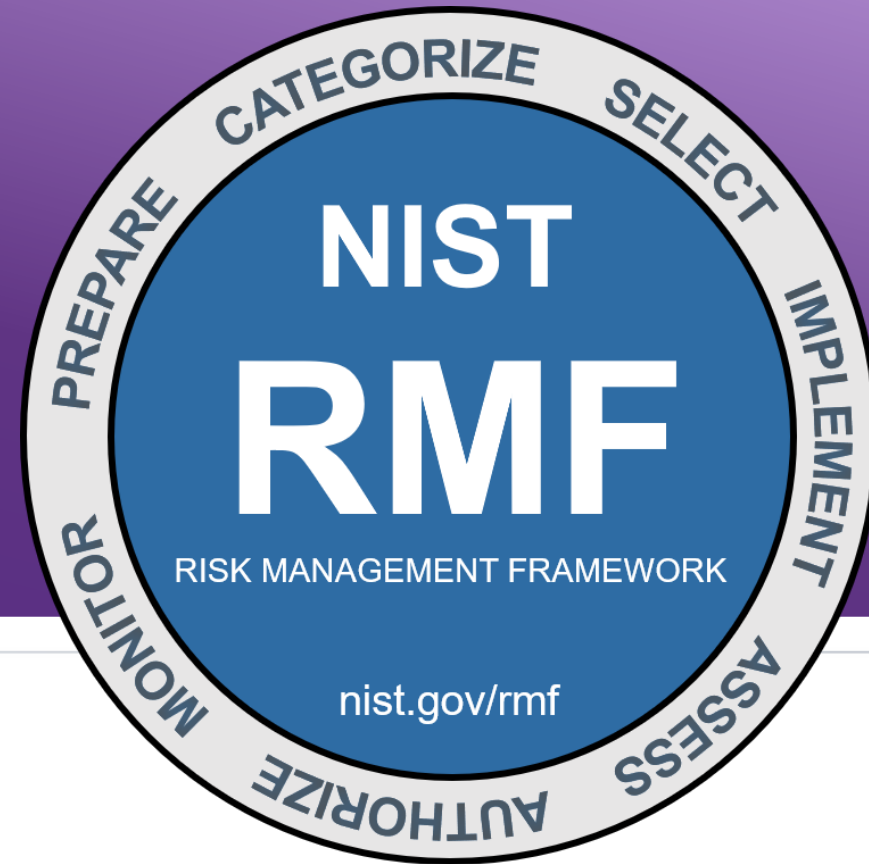
[Approved Cybersecurity Plan \(rtsclients.com\)](https://rtsclients.com) – Based upon CSF v1



Approved Cybersecurity Plan: Align to NIST CSF

- NIST Cybersecurity Framework (CSF) *does not specify impact levels directly*
- CSF is a comprehensive set of guidelines, best practices & standards to manage & reduce cybersecurity risk
- CSF references NIST publications that include impact levels, such as NIST SP 800-53 and FIPS 199; SP 800-37, SP 800-30, SP 800-161r1
- *CSF 2.0 - Feb 2024: Updates*
 - *Added the Govern function*
 - *Supply chain Risk Management expanded guidance and focus on Secure Software Development Practices*
 - *Move away from Critical Infrastructure to broaden scope to all organizations*

NIST Resiliency and Risk Management



Risk Management Framework Overview

The RMF provides a ***structured, yet flexible process*** for managing ***cybersecurity and privacy risk to information & systems*** that includes system categorization, control selection, implementation, assessment, authorization, and continuous monitoring.

National Institute of Standards and Technology (NIST)

Important frameworks (FREE)

- **NIST Cybersecurity Framework (CSF)**
 - Generalized framework designed to be used voluntarily by any organization & can be integrated into established risk management & assessment programs.
 - *Complementary to the RMF approach to selecting & prioritizing controls from SP 800-53*
- **NIST Risk Management Framework (RMF)**
 - Help US Government Agencies & Federal Government Contractors comply with standards established in the Federal Information Security Management Act (FISMA) and the Federal Information Processing Standard Publication 200 (FIPS 200)
- **NIST Secure Software Development Framework (SSDF)**
 - NIST Special Publication (SP) 800-218
 - Set of secure software development practices



What is Cybersecurity Resilience?

Importance for State Agencies

- Definition

- *“The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” NIST*

- Key Benefits

- Protection against evolving threats
- Continuity of Operations (CONOPS)
- Trust and Credibility

- Key Aspects of Cybersecurity Resilience

- Identifying potential threats/vulnerabilities in advance
- Implementing robust security controls & defenses
- Developing Incident Response & Disaster Recovery Plans
- Adapting to threat landscape & continuous monitoring

Key Objectives to Obtain Cybersecurity Resilience

01

Conduct a Risk Assessment

02

Adopt & Implement
NIST SP
800-53
Controls

03

Develop &
Enforce
Security
Policies

04

Conduct
Security
Assessments
and Audits

05

Certification
& Reporting

06

Incident
Response,
Remediation &
Continuous
Monitoring

Align to NIST

Special Publication (SP) 800-53, Revision 5 & SP 800-37
& NIST Cybersecurity Framework (CSF)

Cybersecurity & Privacy Controls

Frameworks and Coverage to Protect an Organization



Weaker Coverage

Moderate Coverage

High Coverage

Risk Management Framework Steps

Prepare	Essential activities to prepare the organization to manage security and privacy risks
Categorize	Categorize the system and information processed, stored, and transmitted based on an impact analysis
Select	Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	Implement the controls and document how controls are deployed
Assess	Assess to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to authorize the system (to operate)
Monitor	Continuously monitor control implementation and risks to the system



RMF Prepare

Purpose: Carry out essential activities to help prepare all levels of the organization to manage its security and privacy risks using the RMF

Task	Step
P-1	Risk Management Roles
P-2	Risk Management Strategy
P-3	Risk Assessment - Organization
P-4	Organizationally-tailored Control Baselines & Cybersecurity Framework Profiles <i>(optional)</i>
P-5	Common Control Identification
P-6	Impact Level Prioritization <i>(optional)</i>
P-7	Continuous Monitoring Strategy –Organization
P-8	Mission or Business Focus



Related: SP 800-39, SP 800-30, SP 800-137

RMF Prepare

Purpose: Carry out essential activities to help prepare all levels of the organization to manage its security and privacy risks using the RMF

Task	Step
P-9	System Stakeholders
P-10	Asset Identification
P-11	Authorization Boundary
P-12	Information Types
P-13	Information Life Cycle
P-14	Risk Assessment -System
P-15	Requirements Definition
P-16	Enterprise Architecture
P-17	Requirements Allocation
P-18	System Registration



Related: SP 800-160, SP 800-30, SP 800-60

RMF Select Step

Purpose: select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, and the Nation.



- S-1:** Control Selection
- S-2:** Control Tailoring
- S-3:** Control Allocation
- S-4:** Documentation of Planned Control Implementations
- S-5:** Continuous Monitoring Strategy – System
- S-6:** Plan Review and Approval

Related:



What is NIST SP 800-53?

Security and Privacy Controls for Information Systems and Organizations

Catalog of
**Security &
Privacy** Controls

Used as part of
**Risk
Management**
Process

Applicable to **all
types** of systems
& organizations

Assessment
Procedures
SP 800-53A

Control Baselines
SP 800-53B

NIST SP 800-53 R5 has 20 Control Families

Each family has base controls & Control Enhancements – More than 1,500 controls

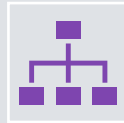
AC: Access Control	AT: Awareness and Training	AU: Audit and Accountability	CA: Assessment, Authorization, and Monitoring	CM: Configuration Management
CP: Contingency Planning	IA: Identification and Authentication	IR: Incident Response	MA: Maintenance	MP: Media Protection
PE: Physical and Environmental Protection	PL: Planning	PM: Program Management	PS: Personnel Security	PT: Personally Identifiable Information Processing and Transparency
RA: Risk Assessment	SA: System and Services Acquisition	SC: System and Communications Protection	SI: System and Information Integrity	SR: Supply Chain Risk Management

NIST RMF Takeaways



Manage

Using the Risk Management Framework provides a means to apply consistent and comprehensive security measures



Coordinate

Security & privacy risk management requires coordination between programs & resources



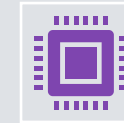
Regulations

Federal information & security programs are driven by legislation, regulations & policy



Wholistic

The NIST RMF is a wholistic, repeatable process to manage information security & privacy risk; it is not compliance or paperwork-based activity



Neutrality

The NIST RMF is tech neutral and can be applied to any type of information system without modification



Resources

There are numerous free NIST resources to support implementation of RMF steps & tasks

What does this mean for you?

<u>Prepare</u>	Essential activities to prepare the organization to manage security and privacy risks
<u>Categorize</u>	Categorize the system and information processed, stored, and transmitted based on an impact analysis
<u>Select</u>	Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
<u>Implement</u>	Implement the controls and document how controls are deployed
<u>Assess</u>	Assess to determine if the controls are in place, operating as intended, and producing the desired results
<u>Authorize</u>	Senior official makes a risk-based decision to authorize the system (to operate)
<u>Monitor</u>	Continuously monitor control implementation and risks to the system



The AppSec gap requires more than AST tools

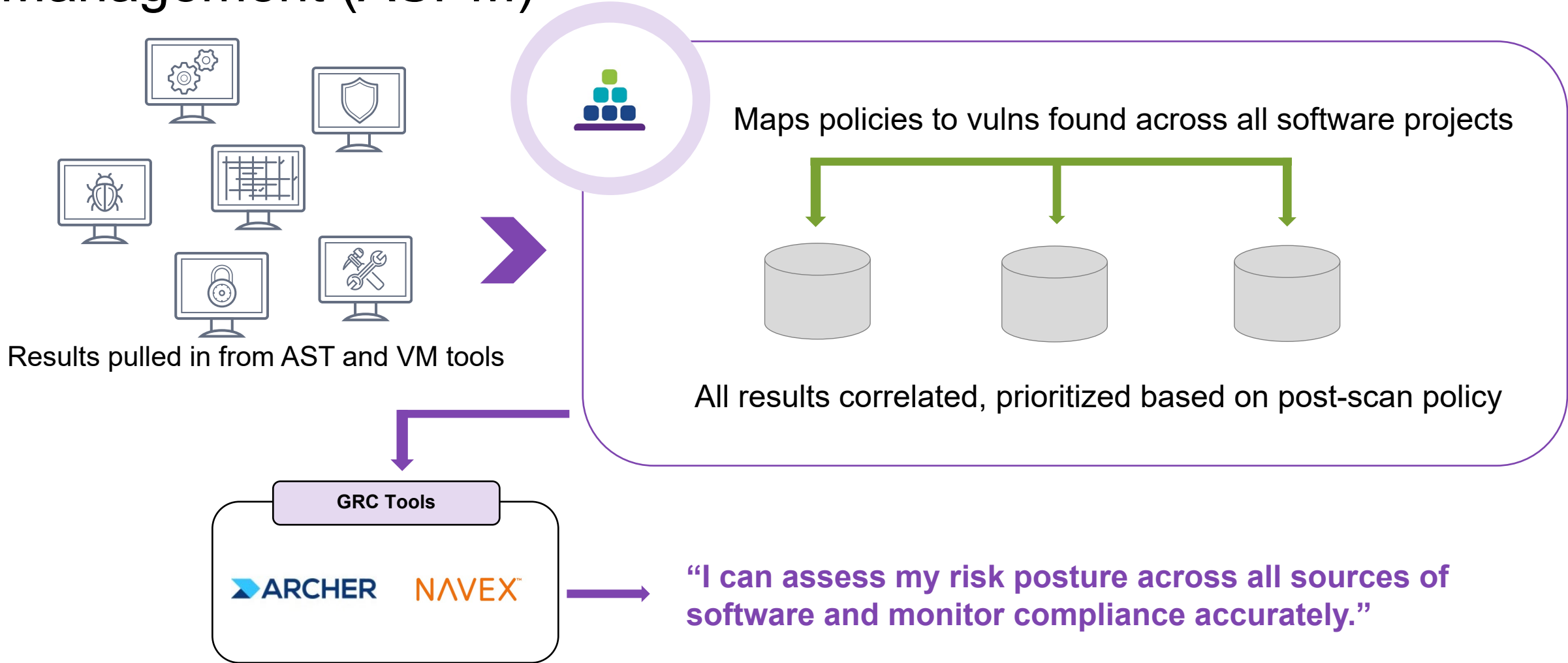
What are key questions to ask in assessing your cybersecurity program?

Do you have a way to orchestrate and verify testing?

Do you have a way to view all apps that you manage?

Do you have a way to report risk?

Monitoring Compliance with Application Security Posture Management (ASPM)



Strategies for orchestrating testing



Dynamic app-specific criteria
(business criticality, downtime risk)



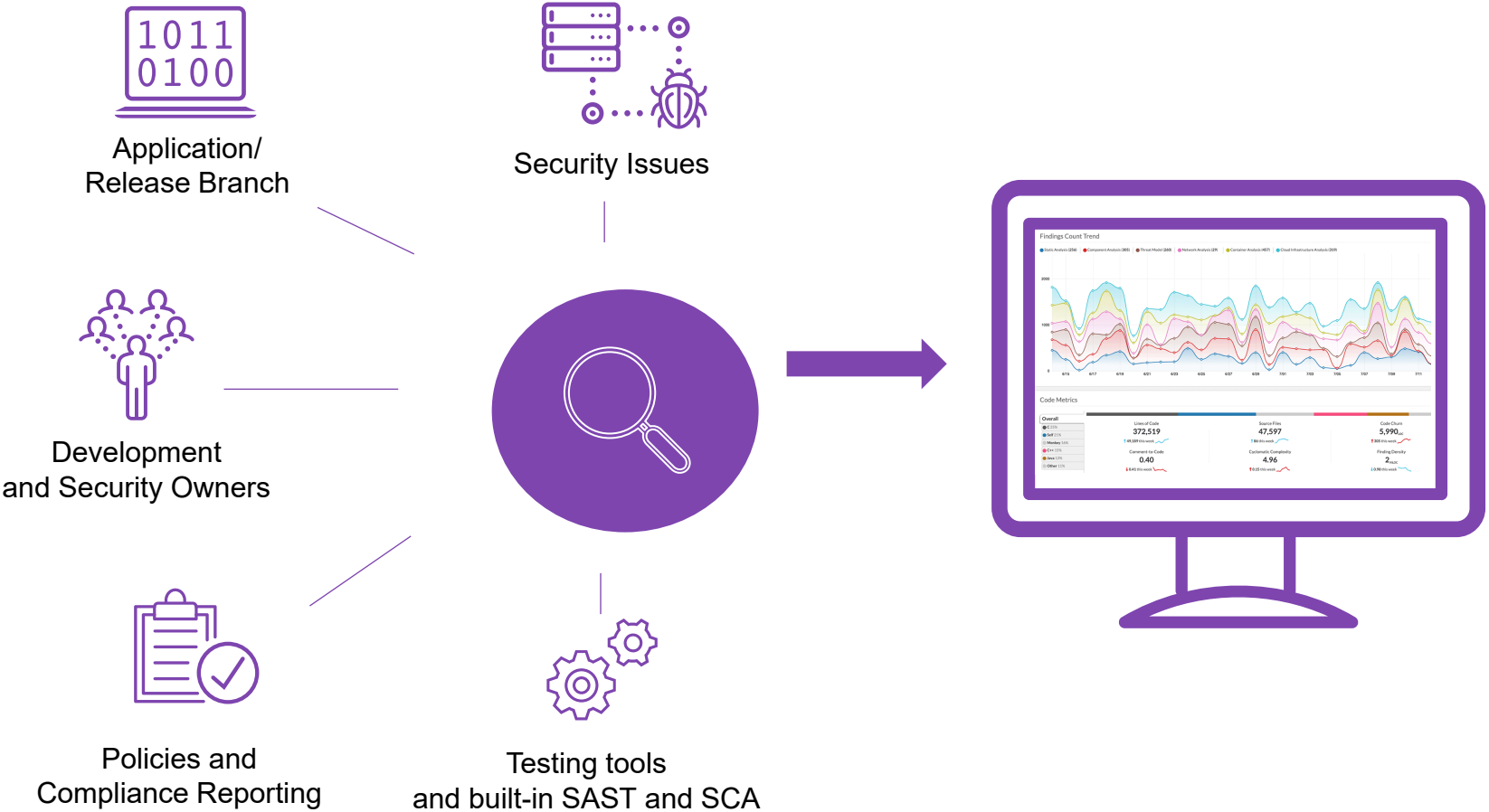
Type of testing needed
(automated or manual, time frame)



Conditions for triggering testing
(scope of code changes, defects)

Understand your application footprint

Dynamically map repositories, owners, and security data



Enrich software visibility by mapping findings, development and security owners, and policies to compliance violations.

Synopsys Cybersecurity Services – Detailed View

CYBERSECURITY STRATEGY AND ASSESSMENTS

ASSESS: Strategic Analysis

Service offerings based on comprehensive cybersecurity assessments to evaluate the current security posture, gap analysis, and develop a strategic roadmap drive overall Cybersecurity program maturity

- NIST CSF 2.0 Cybersecurity Assessment
- IAM Advisory and Program Services
- NIST AI RMF, NIST RMF and NIST 800-53 Assessment and Strategy
- Zero Trust Security Assessment and Strategy
- Platform Security Assessments

CYBERSECURITY GOVERNANCE, RISK & COMPLIANCE SERVICES

GOVERN: Compliance & Risk Management

Service offerings to assess cybersecurity capabilities to manage risk effectively, ensure compliance with evolving government and industry regulations, and integrate cybersecurity policies seamlessly into business operations.

- Cybersecurity Compliance Assessments
- CMMC and FedRAMP Advisory Services
- PCI-DSS Advisory Services
- SOC2, ISO 27001, HITRUST, HIPAA Advisory Services
- Cybersecurity Policy and Procedure Development

CYBERSECURITY RESILIENCY & TRAINING SERVICES

FORTIFY: Prevention & Preparation

Service offerings designed to enhance organizational Cybersecurity resilience through proactive incident response planning, disaster recovery strategies, and business continuity practices to minimize the impact of cyber threats and ensure rapid recovery.

- Security Operations Centre (SOC) Modernization Strategy
- Incident Response & Disaster Recovery Advisory Services
- Cybersecurity Tabletop Exercises

NIST CSF 2.0 Overview

Categories: For each function there are a set of categories & sub-categories that define cybersecurity outcomes & controls.

The NIST CSF Assessment reviews an organisations cyber security maturity against a set of functions which then forms recommendations under a set of categories.

KEY BENEFITS OF USING NIST CSF



International Standard

Globally recognized standard that promotes protection and resilience in an adaptable way.



Common Language

Provides a common ground and platform for executives and partners to discuss cybersecurity risks.



Long-term Risk Management

Build for future regulations and compliance requirements

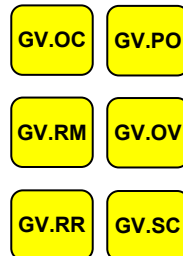
NIST CYBERSECURITY FRAMEWORK

Functions: The 'core' material of the NIST framework is split into 6 functions.



GOVERN

Informs what an organization may do to achieve and prioritize the outcomes of the other five Functions



IDENTIFY

Identification, inventory, assessment, and governance of enterprise assets and related risks



PROTECT

What is important to protect, why protection is necessary, and what protections are prudent



DETECT

Deployment and management of capabilities designed to monitor for potential security incidents



RESPOND

Analysis, implementation, and maintenance of methods to address and minimise impacts of security incidents



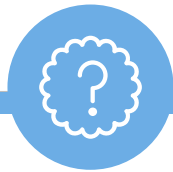
RECOVER

Maintaining or returning the business to normal operations following security incidents



NIST CSF 2.0 Assessment Approach (1/2)

Cybersecurity maturity assessment approach against the NIST CSF maturity framework



What?

Cyber Security Maturity Current State

NIST CSF Overview
The industry-standard NIST Cybersecurity Framework (CSF) enables enterprises to evaluate security capabilities and measure risk. CSF contains six core functions, 22 categories, 112 subcategories and thousands of security control references (NIST, ISO, COBIT, etc.)

NIST CYBERSECURITY FRAMEWORK

- GOVERN**: Informs what an organization may do to achieve and prioritize the outcomes of the other five Functions.
- IDENTIFY**: Identification, inventory, assessment, and governance of enterprise assets and related risks.
- PROTECT**: What is important to protect, why protection is necessary, and what protections are prudent.
- DETECT**: Deployment and management of capabilities designed to monitor for potential security incidents.
- RESPOND**: Analysis, implementation, and maintenance of methods to address and minimize impacts of security incidents.
- RECOVER**: Maintaining or returning the business to normal operations following security incidents.

Key Benefits

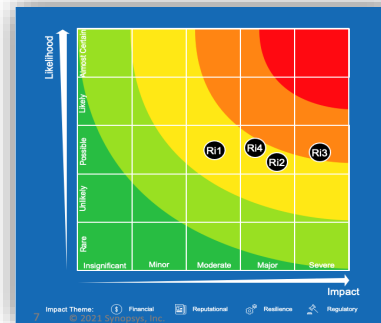
- INDUSTRY STANDARD**: Aligns Client_X to a standard that promotes protection and resilience in an adoptable way.
- COMMON LANGUAGE**: Provides talent and partners with a common language for discussing cybersecurity risks.
- MANAGED**: Enhances security by continuously updating the framework with the latest trends.

NIST CSF maturity assessment to evaluate the client's Cyber security posture.



So What?

Key Maturity and Security Gaps



Identify key security risks and associated impacts.



Now What?

Our Recommendations

DETAILED SECURITY RECOMMENDATIONS (1/5)
Recommendation statements are described as actionable items to aid Client in developing a strong cybersecurity program

ID	RECOMMENDATION	ACTIONABLE ITEMS	RISK ADDRESSED
R11	Consolidate standards for data security such as encryption (at rest and in-transit), hashing, retention, and destruction in one document such as "Data Security Standard".	<ul style="list-style-type: none">Define approved cryptographic algorithm, mode of operation, key size, nonce/IV size for symmetric encryption.Define the approved mechanism for encryption key management.Define approved hashing algorithms with configuration parameters such as work-factor for password hashing and signature.Define approved cipher suite for TLS protocol.Define base/extension and format-preserving encryption (FPE) standard, if applicable.Define standards for the protection of data-in-use such as standards for the display of sensitive data on the screen.	R11
R12	Enhance the "Identification and Authentication Standards" document to include standards for applicable authentication mechanisms such as OAuth 2.0, OIDC, SAML 2.0, and certificate-based authentication.	<ul style="list-style-type: none">For username/password-based authentication, also include requirements to reject breached passwords and provide guidelines to implement breached password detection.	R12
R13	Define remote maintenance policy, standards, and procedures.	<ul style="list-style-type: none">Define policies, standards, and procedures for remote maintenance.	R13

Provide recommendations and develop initiatives to mitigate key security risks and improve overall Cybersecurity program maturity.

Duration

4-6 weeks based on engagement scope

Thank You

Q&A

Thank You! Questions? Contact Us:

Gavin Hockett

571-662-3247


Gavin.Hockett@Carahsoft.com


Synopsys@carahsoft.com





Thank you for attending this Synopsys webinar! Carahsoft is the master distributor for Synopsys Open Source solutions available via NASA SEWP V, NJSBA, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Synopsys' solutions, please check out the following resources and information:

 For additional resources:
carah.io/SynopsysResources

 For additional Synopsys solutions:
carah.io/SynopsysSolutions

 To purchase, check out the contract vehicles available for procurement:
carah.io/SynopsysContracts

 For additional Open Source solutions:
carah.io/OpenSourceSolutions

 To set up a meeting:
Synopsys@carahsoft.com or 703-871-8570