FCCMA

scarlett|group

Aligning with Florida's Cybersecurity Law: NIST CSF Assessments and Beyond

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

May 29, 2025

Tyler Chancey

Director of Cybersecurity at Scarlett Group, leading cybersecurity strategy and solutions development.

Experience: Worked in a Fortune 10 Security Operations Center, gaining expertise in auditing, consulting, and implementing tailored cybersecurity measures.

Certifications: GIAC Certified Forensics Analyst (GCFA) and multiple Microsoft security certifications, professional excellence in cybersecurity.

Joe Kynion

Director of Information Technology at the Hillsborough County Tax Collector, leading IT strategy and operations since 2021.

Experience: Joe boasts a remarkable 40-year career in IT, including nearly a decade as Vice President of Information Technology in the banking sector and 8 years as a U.S. Navy programmer. His versatile IT expertise spans healthcare, land development, and insurance industries, where he has developed a comprehensive understanding of technology solutions across diverse business environments.

Education: Bachelor’s Degree in Business from the University of Phoenix, actively pursuing advanced studies in AI and Cybersecurity.

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Join Us on Slido!

scarlett|group

Join at slido.com #4042579

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Cybersecurity Law Requirements

Learning Objective 1 - Understanding Florida's Cybersecurity Law Requirements

- Overview of the mandates and their implications for local governments.
- Explanation of Concepts and Requirements
- Importance of compliance and proactive cybersecurity measures.

Florida Cybersecurity Law Requirements

In the following slides, we will quickly review some of the relevant laws in Florida for Cybersecurity.

- Local Government Cybersecurity Act (Chapter 282 Section 3185)
- State Cybersecurity Act (Chapter 282 Section 318)
- Public Records Law (Chapter 119)
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- FLHSMV MOU for Partner Organizations
- HB 7055/7057

How familiar are you with Florida's cybersecurity laws and requirements?

Join at slido.com
#4042579

NIST 2.0 Alignment Overview

Security Control/Requirement
Governance Framework
Transparency and Accountability
Prohibition of Ransom Payments
Enhanced Threat Awareness
Liability Protections
Operational Standards
Annual Attestations
Data Protection
Adoption of NIST Standards
Incident Reporting
Mandatory Cybersecurity Training

Local Government Cybersecurity Act (Chapter 282 Section 3185)

Security Control/Requirement	Local Government Cybersecurity Act (Chapter 282 Section 3185)
Adoption of NIST Standards	X
Incident Reporting	X
Mandatory Cybersecurity Training	X

Purpose:

- Mandatory Cybersecurity Training
- Adoption of NIST Standards
- Incident Reporting

Public Records Law (Chapter 119)

Security Control/Requirement	Public Records Law (Chapter 119)
Transparency and Accountability	X
Data Protection	X

Purpose:

- Transparency and Accountability
- Electronic Records
- Custodial Responsibility

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

Security Control/Requirement	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
Enhanced Threat Awareness	X
Liability Protections	X
Incident Reporting	X

Purpose:

- Mandatory Reporting
- Enhanced Threat Awareness
- Liability Protections

scarlett|group

FLHSMV MOU for Partner Organizations

Security Control/Requirement	FLHSMV MOU for Partner Organizations
Operational Standards	X
Annual Attestations	X
Data Protection	X
Incident Reporting	X

Purpose:

- Legal and Regulatory Compliance
- Data Protection
- Operational Standards
- Annual Attestations

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

State Cybersecurity Act (Chapter 282 Section 318)

Security Control/Requirement	State Cybersecurity Act (Chapter 282 Section 318)
Governance Framework	X
Adoption of NIST Standards	X
Incident Reporting	X
Mandatory Cybersecurity Training	X

Purpose:

- Governance Framework
- Adoption of NIST Standards
- Incident Reporting
- Mandatory Cybersecurity Training

Do you believe your organization is adequately prepared to comply with the Local Government Cybersecurity Act?

Join at slido.com
#4042579

HB 7055/7057

Security Control/Requirement	HB 7055/7057
Prohibition of Ransom Payments	X
Adoption of NIST Standards	X
Incident Reporting	X
Mandatory Cybersecurity Training	X

Purpose:

- Prohibition of Ransom Payments
- Adoption of NIST Standards
- Incident Reporting
- Mandatory Cybersecurity Training

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Florida Cybersecurity Compliance Overview

Security Control/Requirement	All Relevant Florida Laws
Governance Framework	X
Transparency and Accountability	X
Prohibition of Ransom Payments	X
Enhanced Threat Awareness	X
Liability Protections	X
Operational Standards	X
Annual Attestations	X
Data Protection	X
Adoption of NIST Standards	X
Incident Reporting	X
Mandatory Cybersecurity Training	X

Compliance for Local Governments

Purpose:

- Safeguard sensitive data with strong compliance
- Governance through security frameworks
- Public trust grows with reinforced protections
- Meet regulations to ensure secure operations
- Maintain continuity despite cyberattack risks

Key Strategies for Florida Managers

1. Adhering to Florida Statute 282.3185
2. Mandatory Employee Training
3. Incident Reporting & Ransomware Prevention
4. Advanced Security Measures
5. Collaboration with Florida Digital Service

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

How to Align with New State Requirements

1. Adopting NIST-Based Standards
2. Mandatory Cybersecurity Training
3. Incident Reporting & Ransomware Prohibition
4. Annual Assessments

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Audience Q&A

Join at slido.com
#4042579

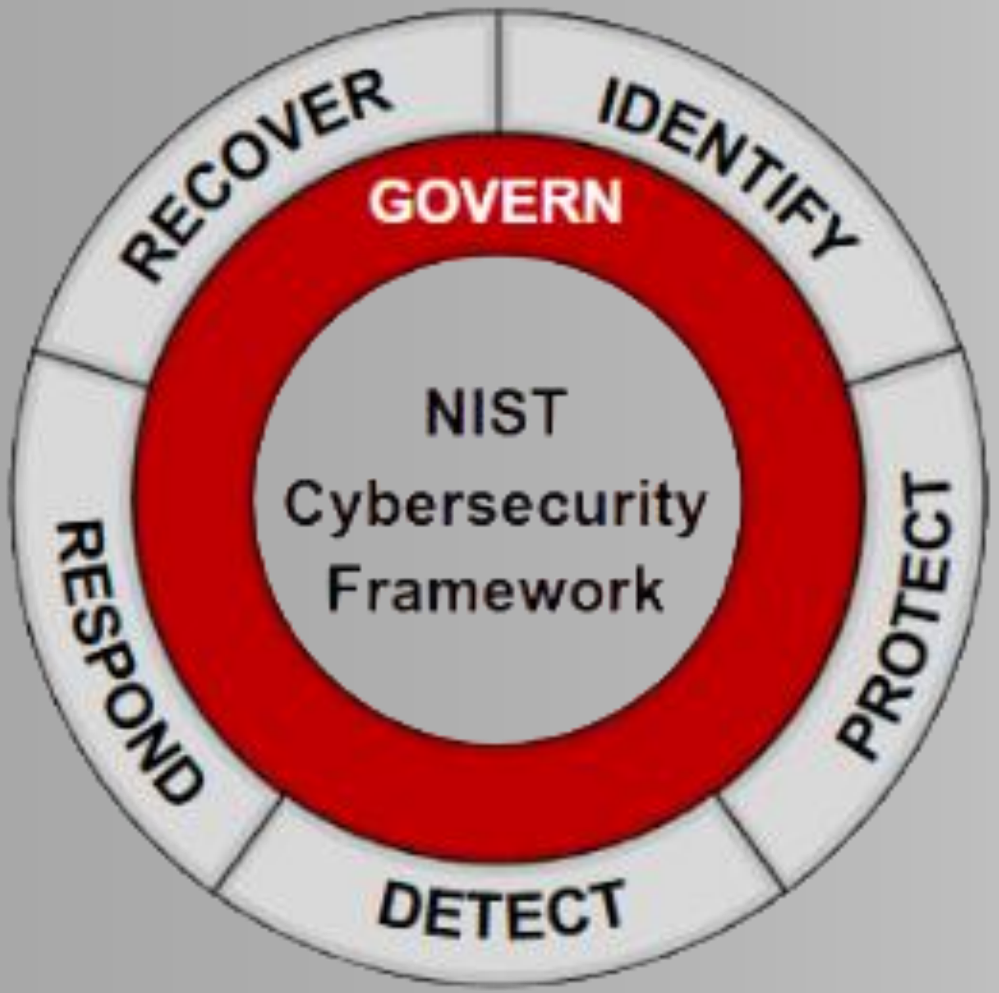
NIST CSF and Assessments

Learning Objective 2 - Understanding NIST CSF and the Value of Assessments

- How NIST CSF provides a structured approach to managing cybersecurity risks.
- Benefits of aligning with NIST CSF for compliance and security enhancement.
- Value of Assessments in understanding roadmap, budget, and risk.

NIST CSF Overview & Guidelines

Cybersecurity Collaboration

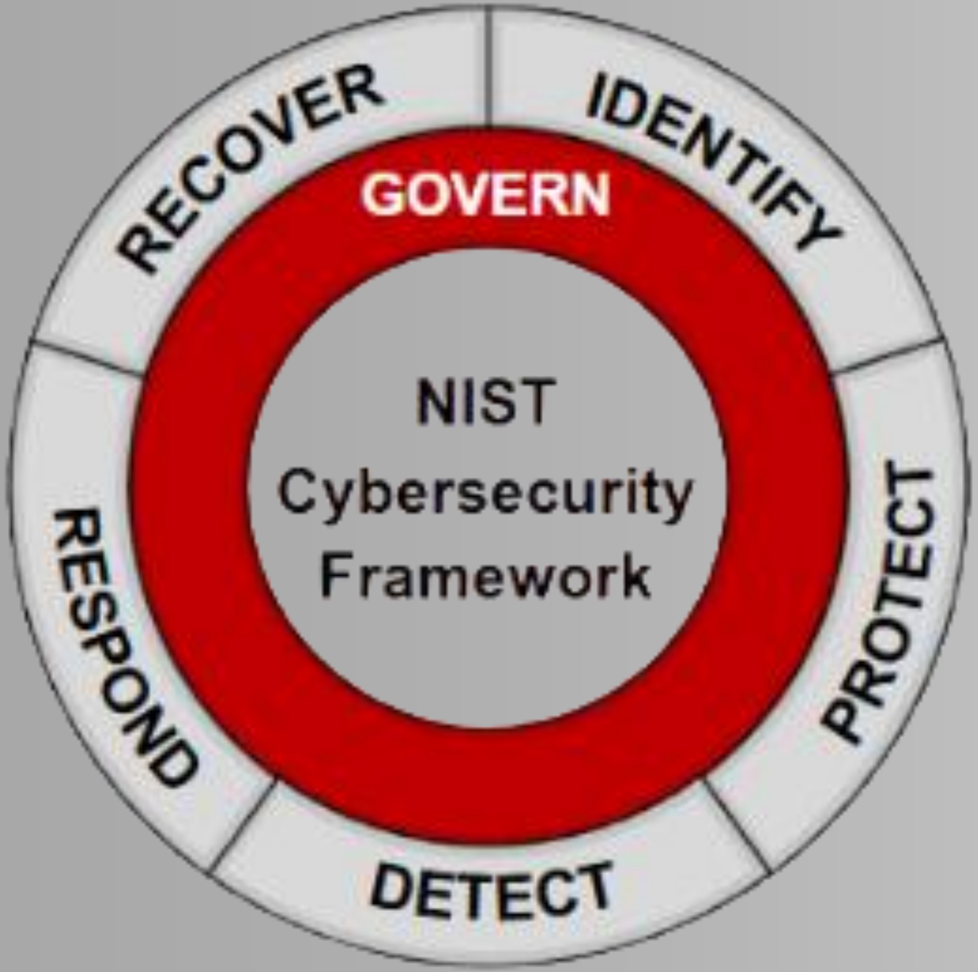


Core Functions

- **Identify:** Understanding the organization's cybersecurity risks and assets.
- **Protect:** Implementing safeguards to ensure the delivery of critical services.
- **Detect:** Developing and implementing activities to identify cybersecurity events.
- **Respond:** Deploying action regarding detected cybersecurity incidents.
- **Recover:** Maintaining plans for resilience and restoring capabilities after an incident.

What are NIST CSF Assessments?

Cybersecurity Framework



Purpose:

- Gap Analysis
- Risk Management
- Compliance Checks

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Most Common Assessment

Prioritized Heat Map

CATEGORIES WITH HIGHEST RISK BASED ON PROBABILITY AND IMPACT APPEAR IN THE UPPER RIGHT-HAND CORNER

Data Security

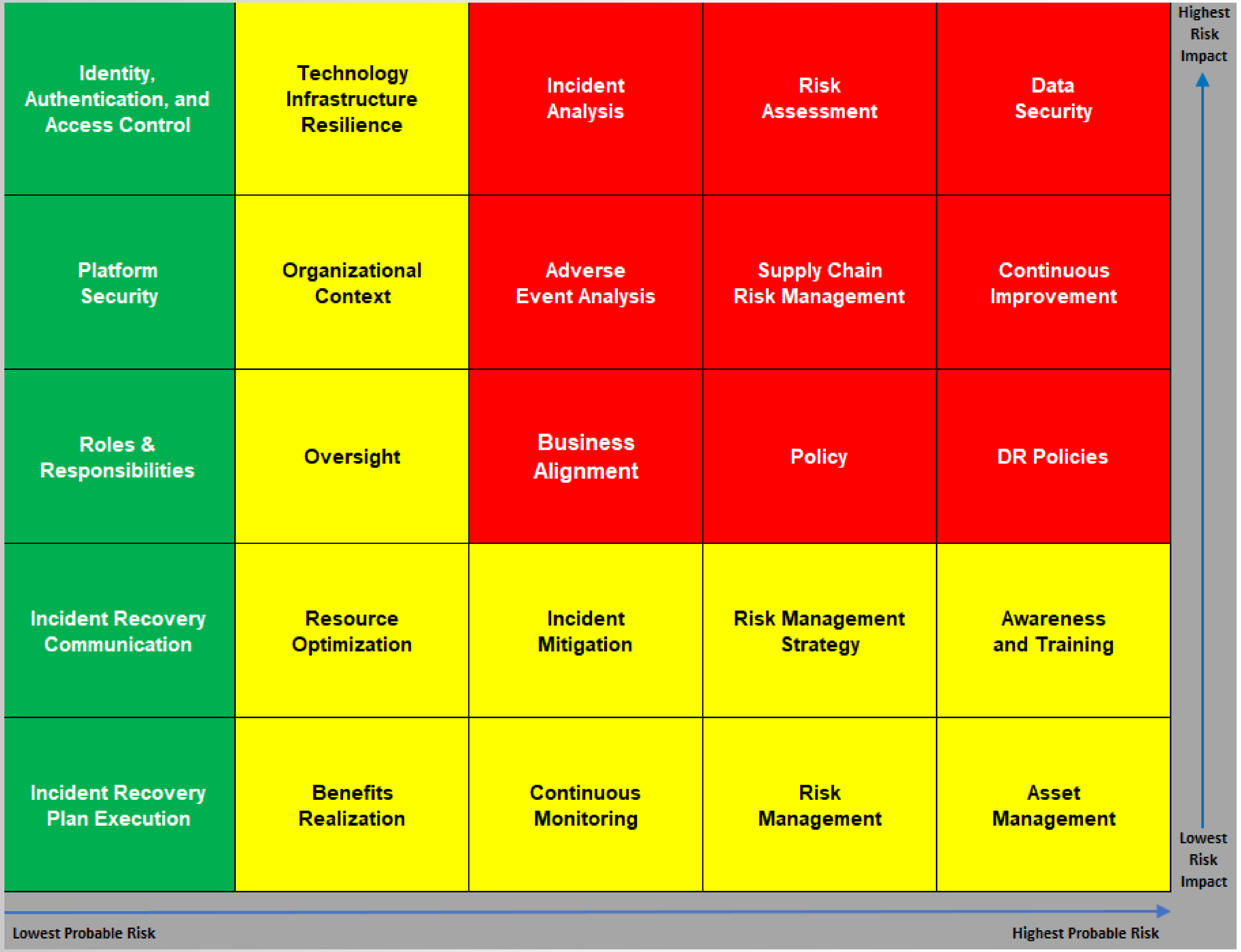
- Data Confidentiality, Integrity, Availability
- Data Classification & Labeling
- Data Encryption – In Use, At Rest, & In Transit

Business Alignment

- Governance
- Risk Management
- Policies and Procedures
- Event Analysis & Risk Assessment
- Supply Chain Risk Management

Continuous Improvement

- Lessons Learned
- Drills, Exercises, and Testing
- Documentation Updates
- Across all CSF Functions

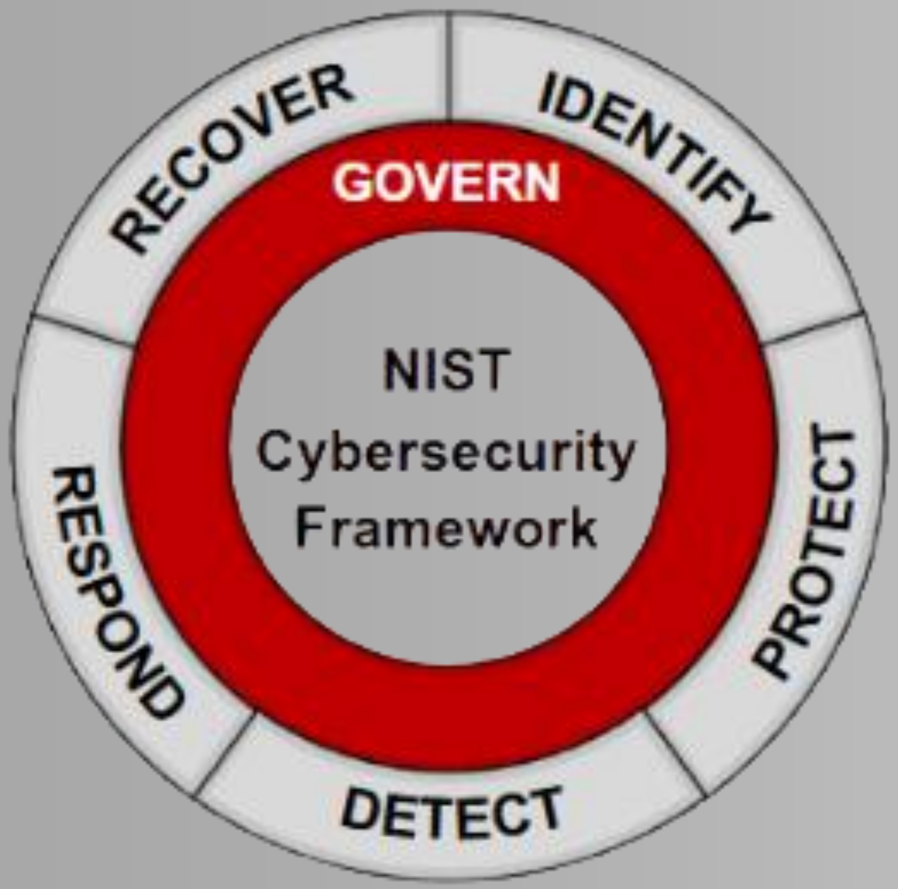


Identity, Authentication, and Access Control	Technology Infrastructure Resilience	Incident Analysis	Risk Assessment	Data Security
Platform Security	Organizational Context	Adverse Event Analysis	Supply Chain Risk Management	Continuous Improvement
Roles & Responsibilities	Oversight	Business Alignment	Policy	DR Policies
Incident Recovery Communication	Resource Optimization	Incident Mitigation	Risk Management Strategy	Awareness and Training
Incident Recovery Plan Execution	Benefits Realization	Continuous Monitoring	Risk Management	Asset Management

How effective do you think the NIST CSF assessments are in improving cybersecurity posture?

Join at slido.com
#4042579

Implementing Florida’s NIST CSF Requirements



Conduct Risk Assessments:

- Perform regular cybersecurity risk assessments to identify vulnerabilities.
- Use Cyber Florida’s NIST CSF 2.0 Risk Assessment tool to evaluate security gaps.
- Engage cybersecurity experts for consultation and compliance support.

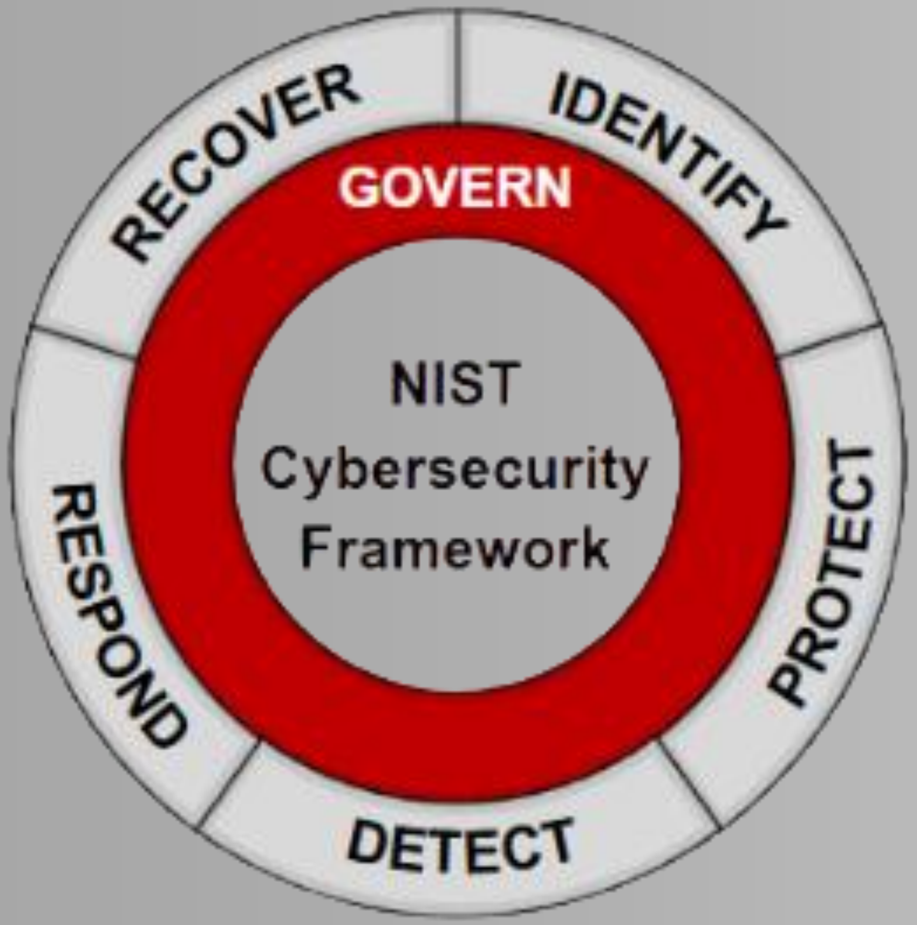
NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

How beneficial do you find mandatory cybersecurity training for employees in enhancing overall security?

Join at slido.com
#4042579

slido

Implementing Florida’s NIST CSF Requirements



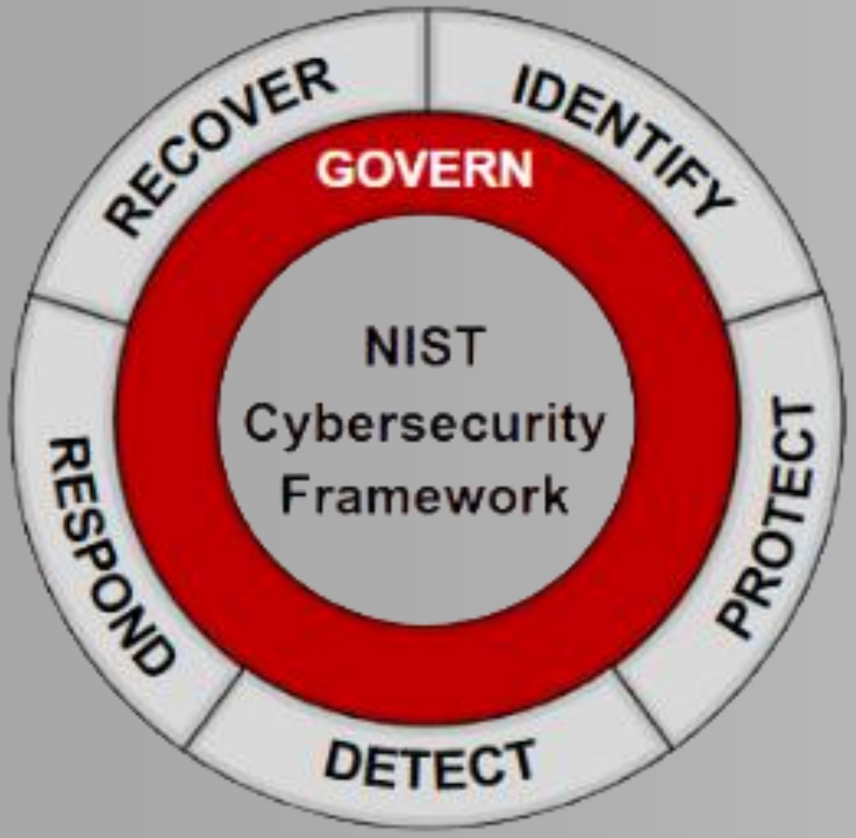
Strengthen Cybersecurity Training:

- Ensure all employees complete mandatory cybersecurity training within 30 days of employment and annually thereafter.
- Utilize Cyber Florida’s First Line Training for cost-effective security awareness.
- Implement phishing simulation exercises to reduce human error.

Do you think your organization has a robust incident reporting system in place?

Join at slido.com
#4042579

Implementing Florida’s NIST CSF Requirements



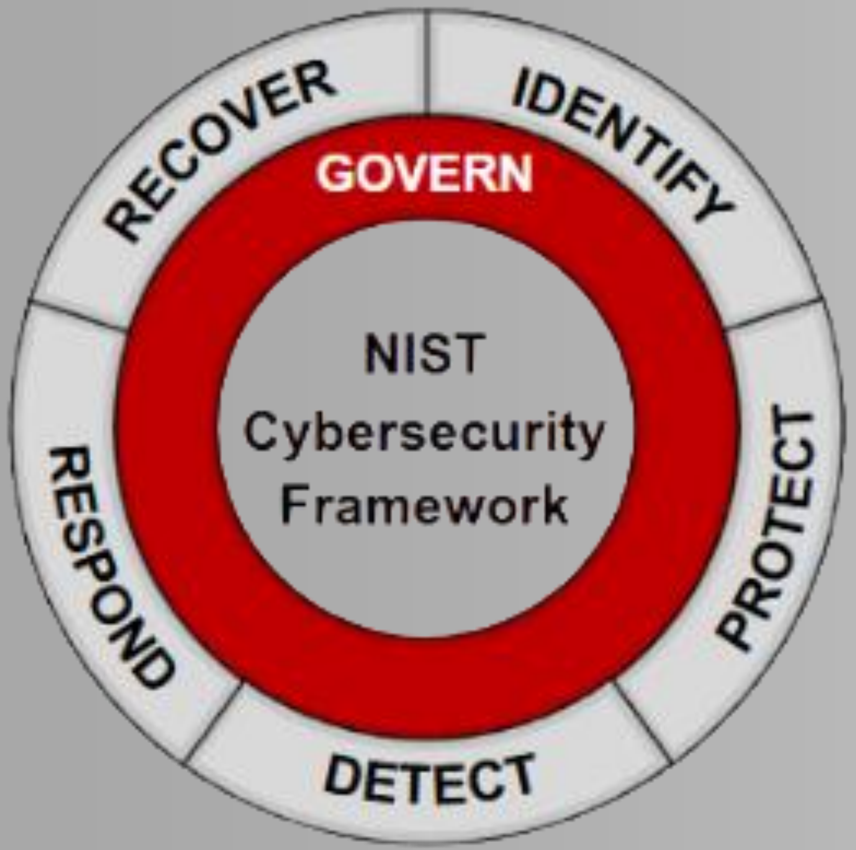
Enhance Incident Response & Compliance:

- Report major cybersecurity incidents within 48 hours and ransomware attacks within 12 hours.
- Notify the Florida Digital Service about cybersecurity progress and compliance efforts.
- Follow HB 7055/7057 mandates, including prohibiting ransom payments to cybercriminals

What is your level of confidence in your organization's ability to prevent ransomware attacks?

Join at slido.com
#4042579

Implementing Florida’s NIST CSF Requirements

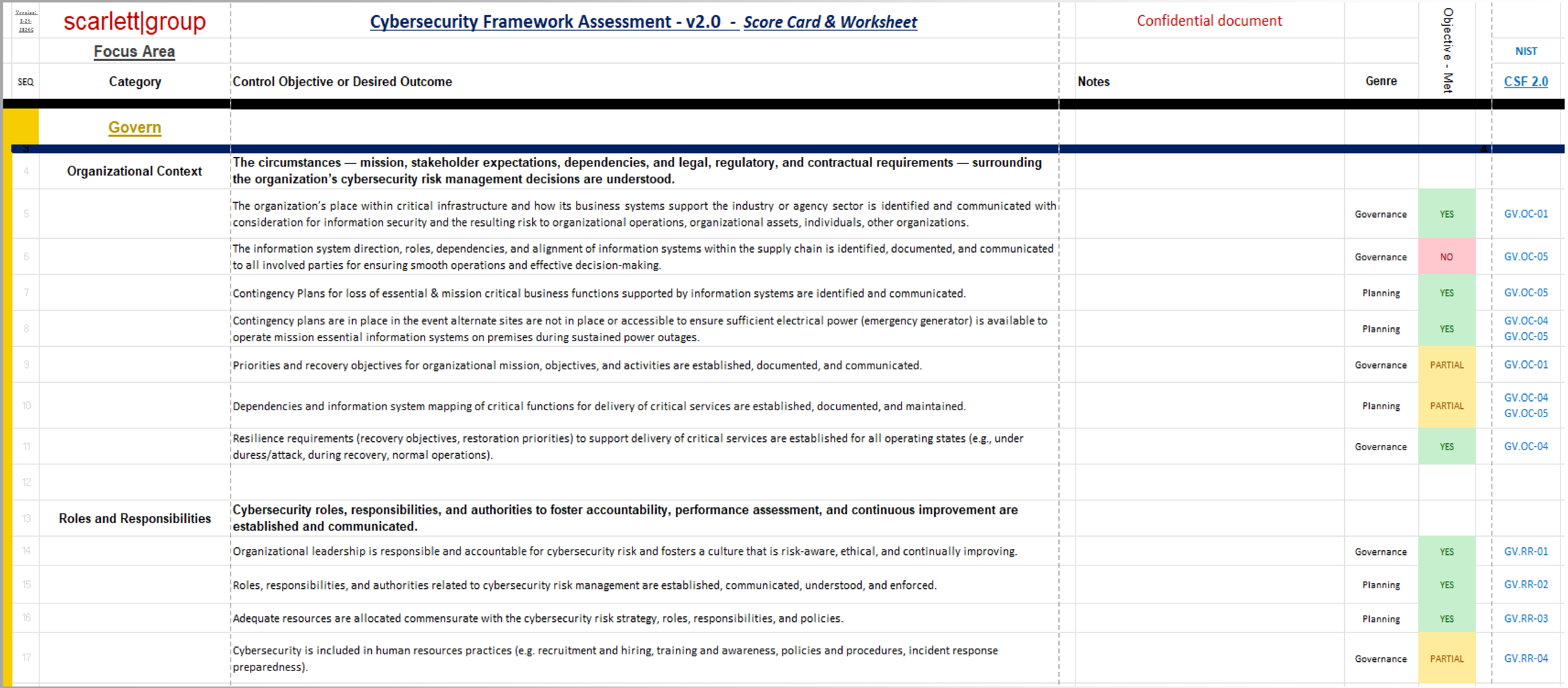


Align with NIST CSF 2.0:

- Implement NIST CSF’s five core functions: Identify, Protect, Detect, Respond, and Recover.
- Develop a cybersecurity governance framework tailored to Florida’s requirements.
- Use Cyber Florida’s workshops to stay updated on compliance best practices.

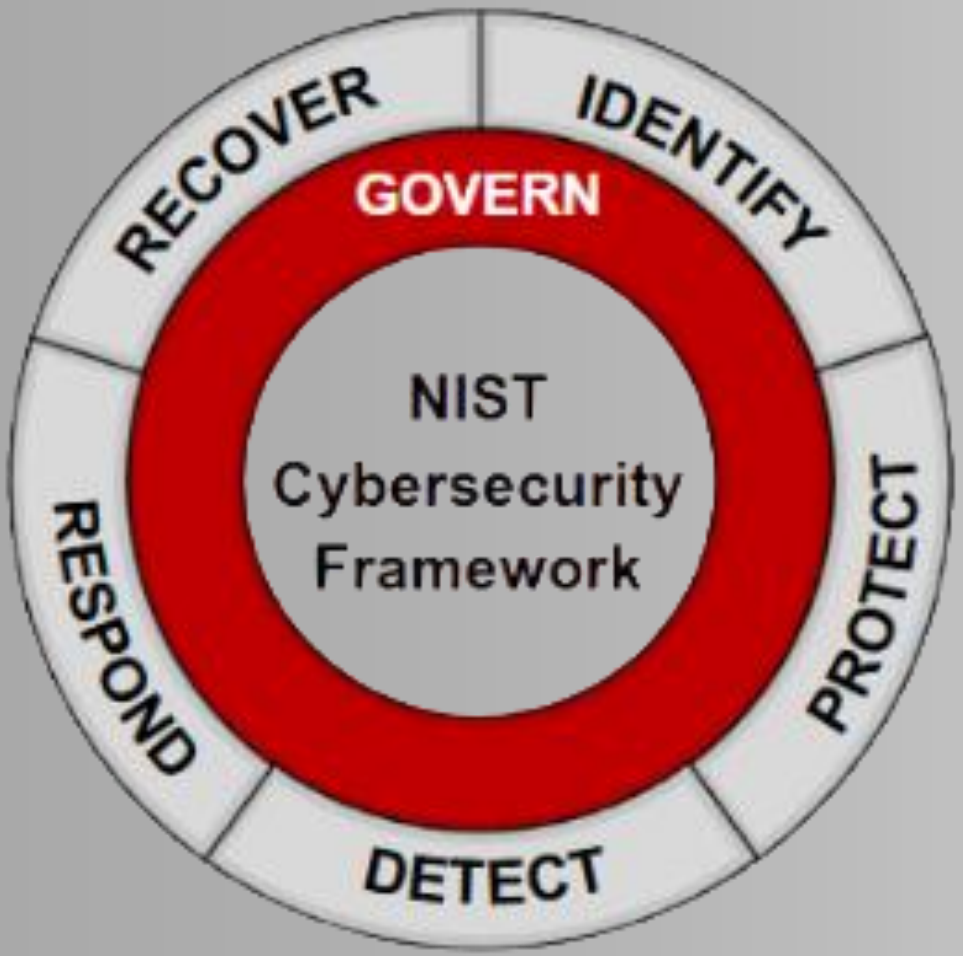
NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Annual Assessments



Version: 5-24-2024G	scarlett|group	Cybersecurity Framework Assessment - v2.0 - *Score Card & Worksheet*	Confidential document		Objective - Met	
	Focus Area					NIST
SEQ	Category	Control Objective or Desired Outcome	Notes	Genre		CSF 2.0
	Govern					
4	Organizational Context	**The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.**				
5		The organization's place within critical infrastructure and how its business systems support the industry or agency sector is identified and communicated with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations.		Governance	YES	GV.OC-01
6		The information system direction, roles, dependencies, and alignment of information systems within the supply chain is identified, documented, and communicated to all involved parties for ensuring smooth operations and effective decision-making.		Governance	NO	GV.OC-05
7		Contingency Plans for loss of essential & mission critical business functions supported by information systems are identified and communicated.		Planning	YES	GV.OC-05
8		Contingency plans are in place in the event alternate sites are not in place or accessible to ensure sufficient electrical power (emergency generator) is available to operate mission essential information systems on premises during sustained power outages.		Planning	YES	GV.OC-04 GV.OC-05
9		Priorities and recovery objectives for organizational mission, objectives, and activities are established, documented, and communicated.		Governance	PARTIAL	GV.OC-01
10		Dependencies and information system mapping of critical functions for delivery of critical services are established, documented, and maintained.		Planning	PARTIAL	GV.OC-04 GV.OC-05
11		Resilience requirements (recovery objectives, restoration priorities) to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).		Governance	YES	GV.OC-04
12						
13	Roles and Responsibilities	**Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.**				
14		Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.		Governance	YES	GV.RR-01
15		Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.		Planning	YES	GV.RR-02
16		Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.		Planning	YES	GV.RR-03
17		Cybersecurity is included in human resources practices (e.g. recruitment and hiring, training and awareness, policies and procedures, incident response preparedness).		Governance	PARTIAL	GV.RR-04

Why are Annual Assessments Crucial?



Benefits:

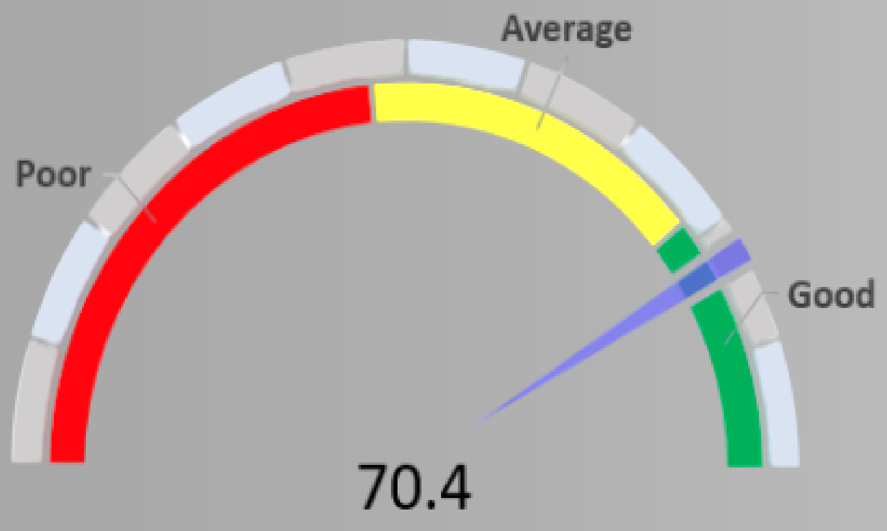
- Identify Vulnerabilities
- Regulate Compliance
- Prevent Costly Breaches
- Strengthen Incident Response
- Protect Public Trust

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

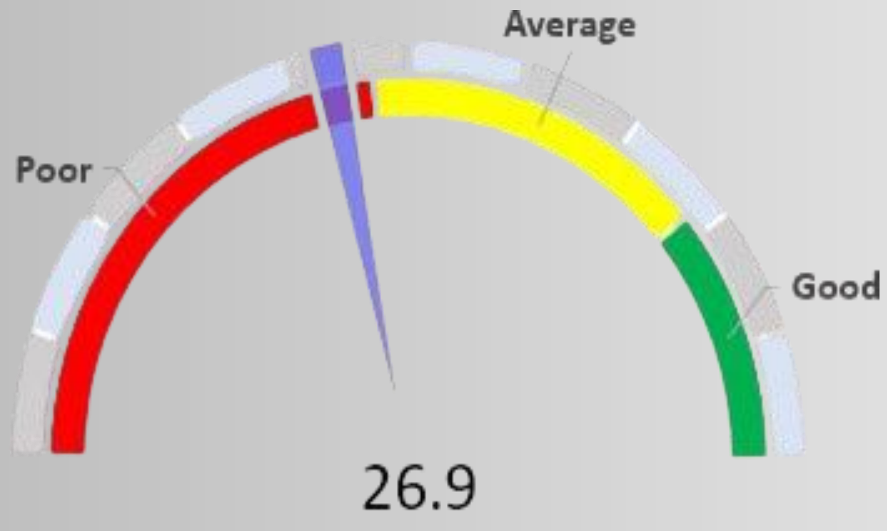
How can Third Party Assessments Help?
Starting the Roadmap

Purpose:

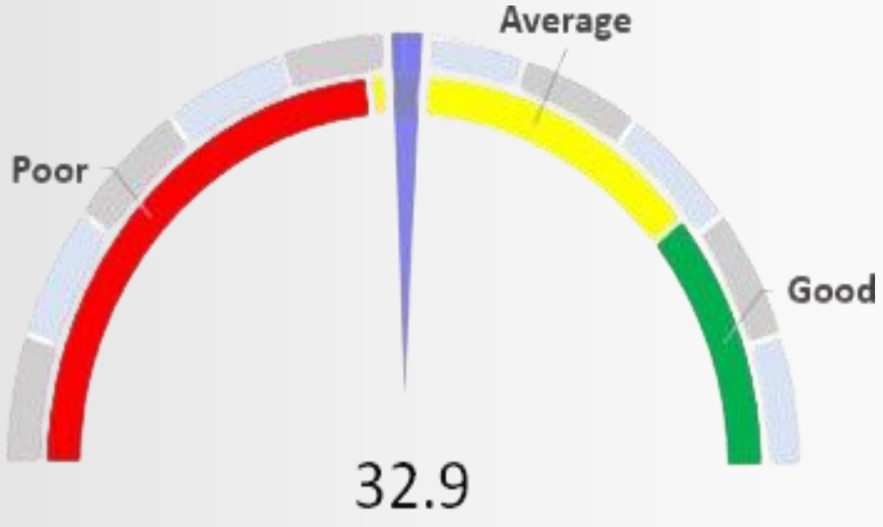
- Gap Discovery
- Align with Frameworks
- Results Focused
- Designed to be legible to Stakeholders and IT
- Risk-based approach



NIST CSF 2.0 Alignment



Cyber Insurability Factor



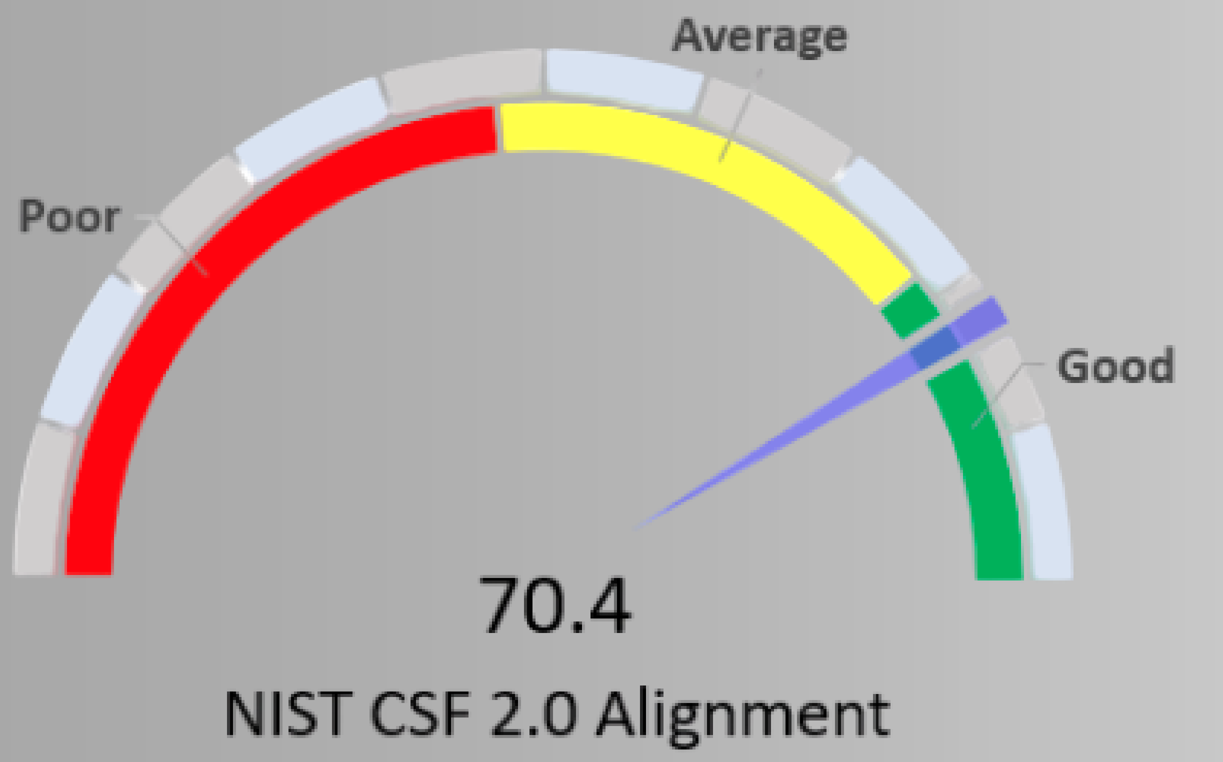
Ransomware Resilience Factor

How valuable do you find third-party assessments in identifying security gaps and improving compliance?

Join at slido.com
#4042579

slido

Align with State Requirements - Starting the Roadmap

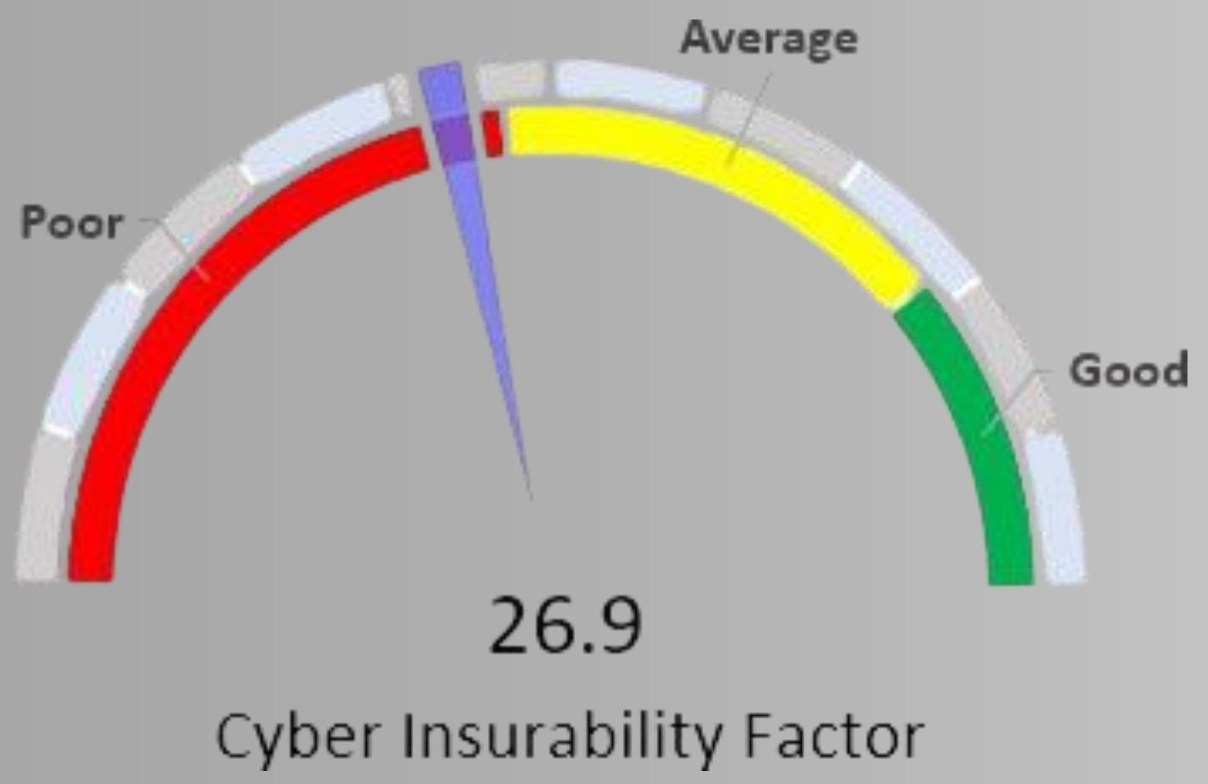


Core Functions:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Align with State Requirements - Starting the Roadmap

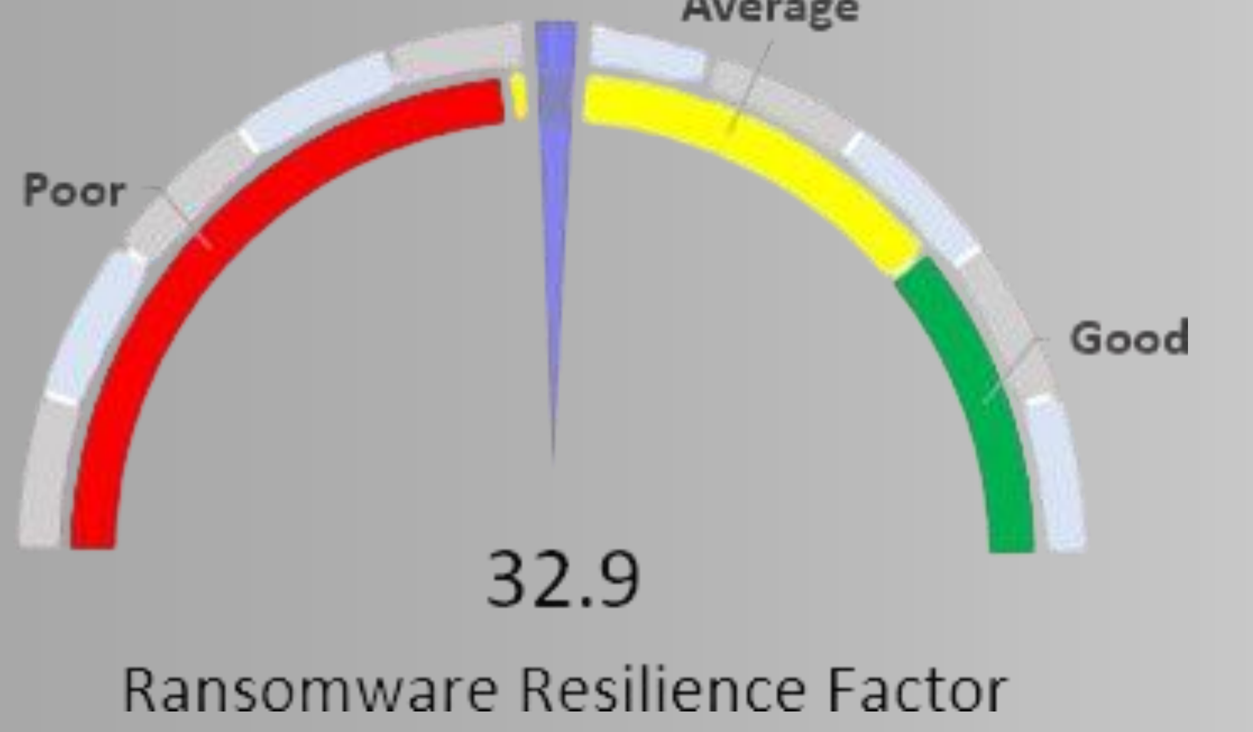


Policy and Procedure:

- How is governance being handled?
- Do policies exist?
- Are policies enabled via technical controls?
- Are policies being known and providing value?

scarlett|group

Align with State Requirements - Starting the Roadmap

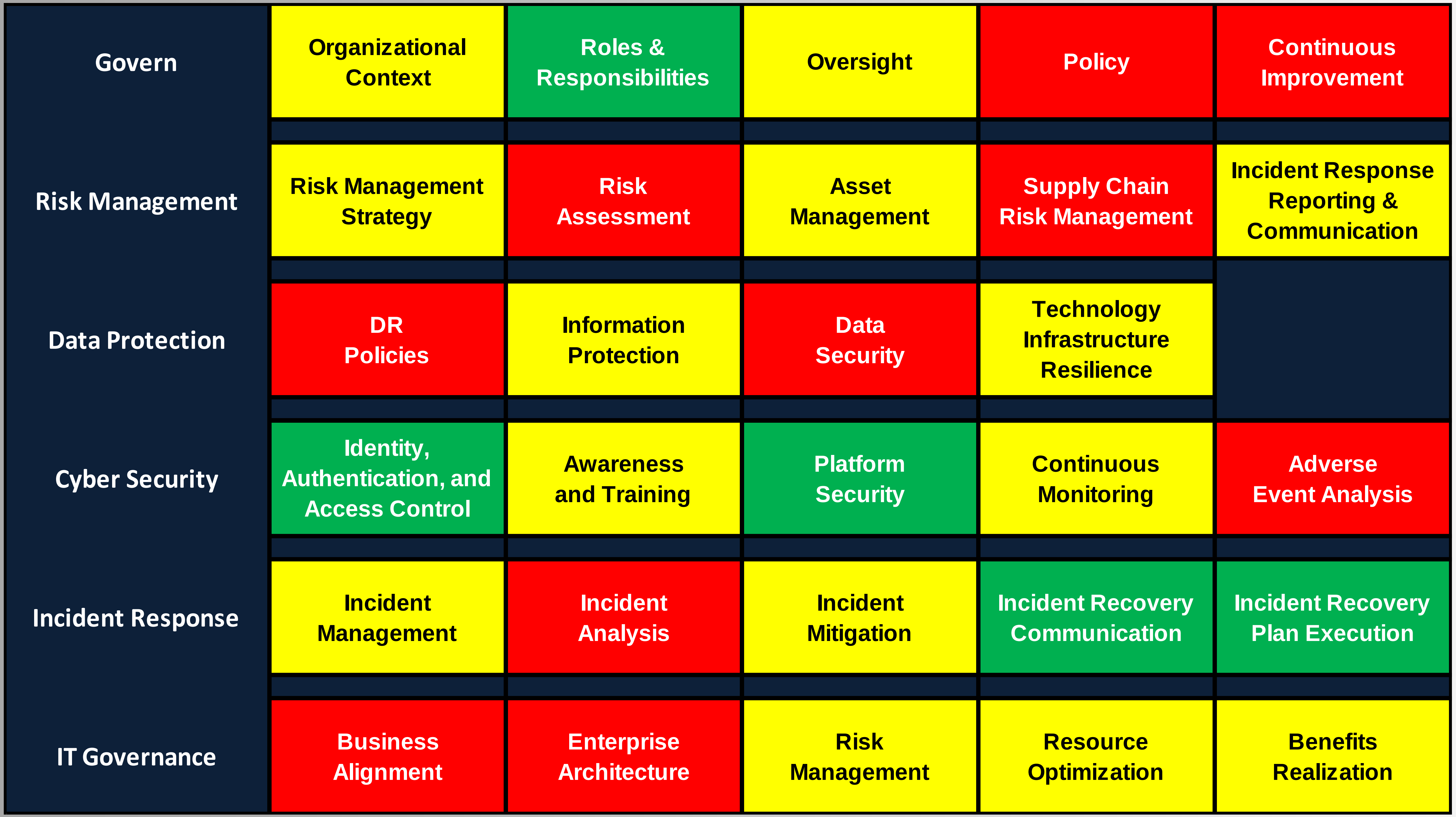


Technical Discovery:

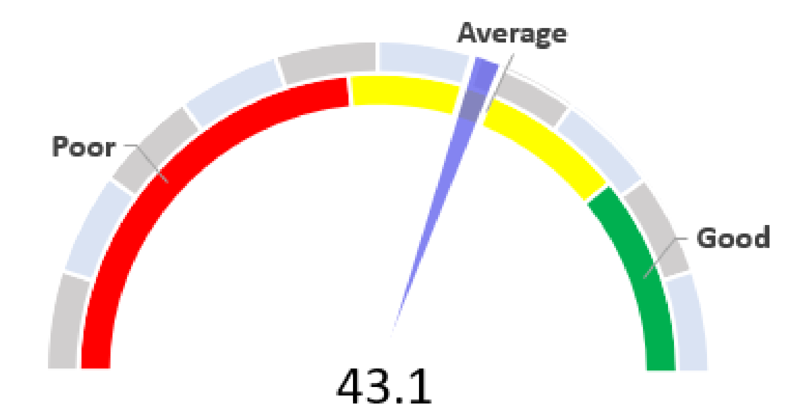
- Discover Assets
- Discover PII and Financial Data
- Discover Users and Applications
- Discover Vulnerabilities

scarlett|group

Align with State Requirements - Starting the Roadmap

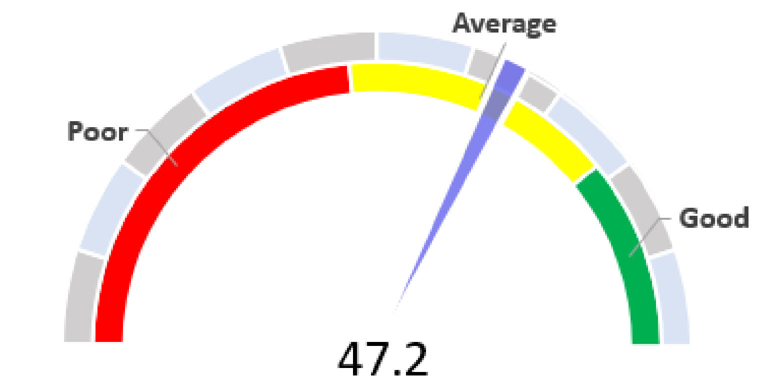


Govern	🟨 Organizational Context	🟩 Roles & Responsibilities	🟨 Oversight	🟥 Policy	🟥 Continuous Improvement
Risk Management	🟨 Risk Management Strategy	🟥 Risk Assessment	🟨 Asset Management	🟥 Supply Chain Risk Management	🟨 Incident Response Reporting & Communication
Data Protection	🟥 DR Policies	🟨 Information Protection	🟥 Data Security	🟨 Technology Infrastructure Resilience	
Cyber Security	🟩 Identity, Authentication, and Access Control	🟨 Awareness and Training	🟩 Platform Security	🟨 Continuous Monitoring	🟥 Adverse Event Analysis
Incident Response	🟨 Incident Management	🟥 Incident Analysis	🟨 Incident Mitigation	🟩 Incident Recovery Communication	🟩 Incident Recovery Plan Execution
IT Governance	🟥 Business Alignment	🟥 Enterprise Architecture	🟨 Risk Management	🟨 Resource Optimization	🟨 Benefits Realization



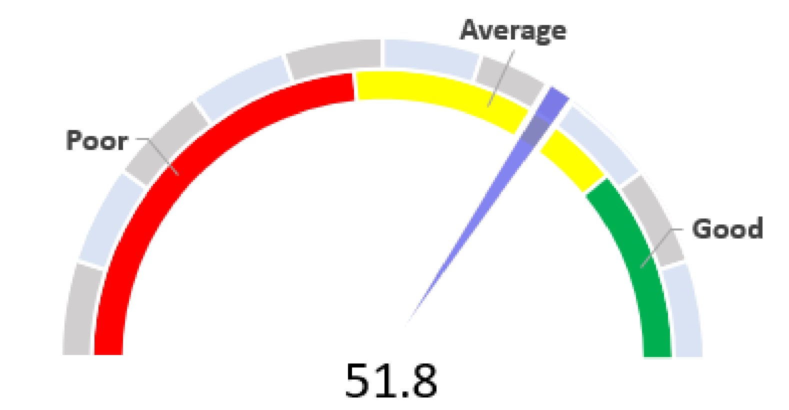
43.1

NIST CSF Alignment



47.2

Ransomware Resilience Factor



51.8

Cyber Insurability Factor

scarlett|group

Audience Q&A

Join at slido.com
#4042579

Recurring Assessment and Risk Evaluation

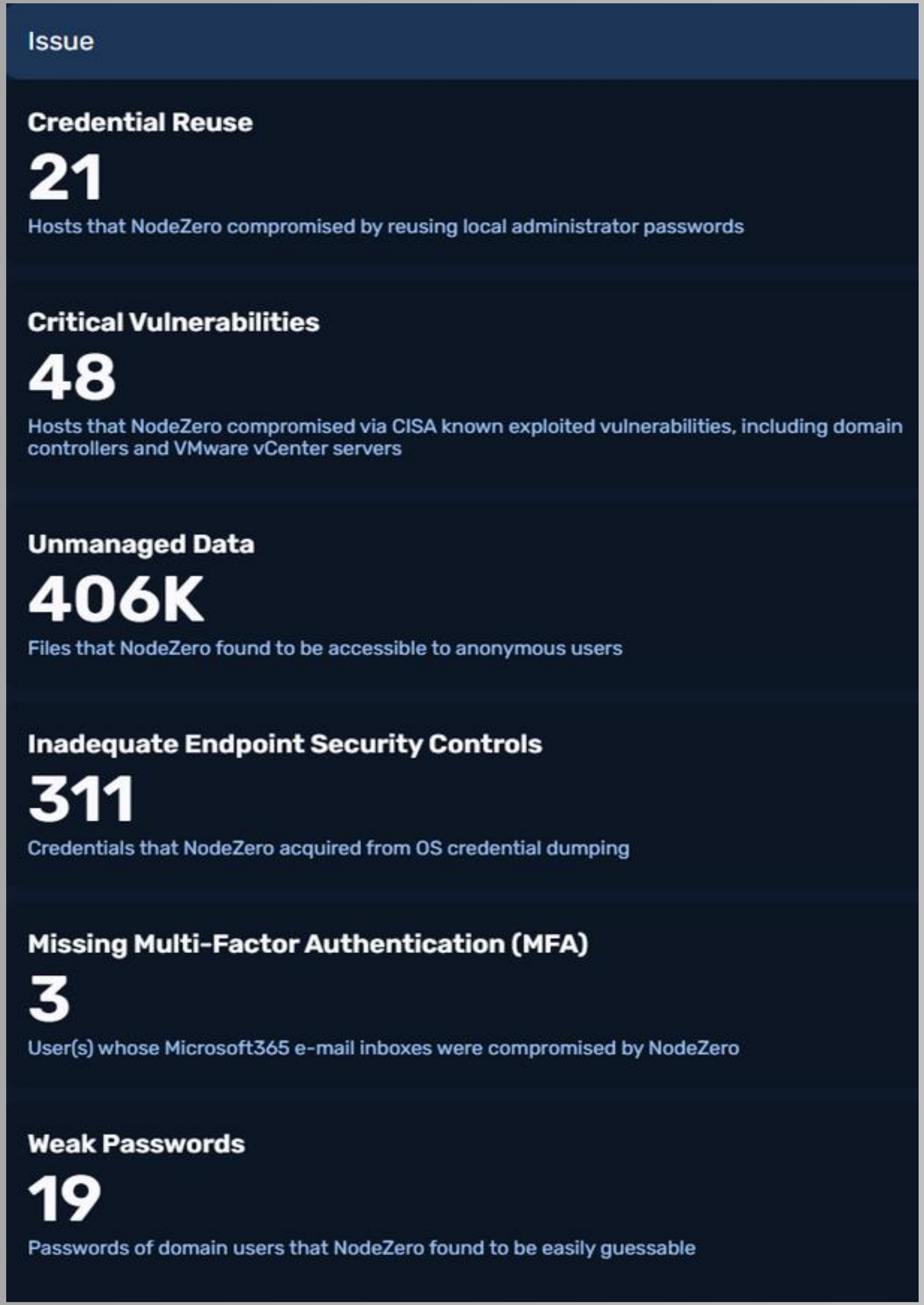
Learning Objective 3 - Importance of Recurring Assessments and Penetration Testing

- Annual assessments to re-align new controls with NIST CSF.
- Monthly autonomous penetration testing to ensure continuous security improvements.
- Risk Governance is a “living” process, evaluated continuously.

How important do you think regular penetration testing is for maintaining cybersecurity?

Join at slido.com
#4042579

Monthly Autonomous Penetration Testing



Issue

Credential Reuse
21
Hosts that NodeZero compromised by reusing local administrator passwords

Critical Vulnerabilities
48
Hosts that NodeZero compromised via CISA known exploited vulnerabilities, including domain controllers and VMware vCenter servers

Unmanaged Data
406K
Files that NodeZero found to be accessible to anonymous users

Inadequate Endpoint Security Controls
311
Credentials that NodeZero acquired from OS credential dumping

Missing Multi-Factor Authentication (MFA)
3
User(s) whose Microsoft365 e-mail inboxes were compromised by NodeZero

Weak Passwords
19
Passwords of domain users that NodeZero found to be easily guessable

Continuous Security Improvements:

- Perform monthly autonomous penetration testing to identify and address vulnerabilities in real-time.
- Utilize AI and cutting-edge tools to simulate attacks and test defenses.
- Ensure continuous improvement of security measures through regular testing.

scarlett|group

Risk Governance – A Living Process

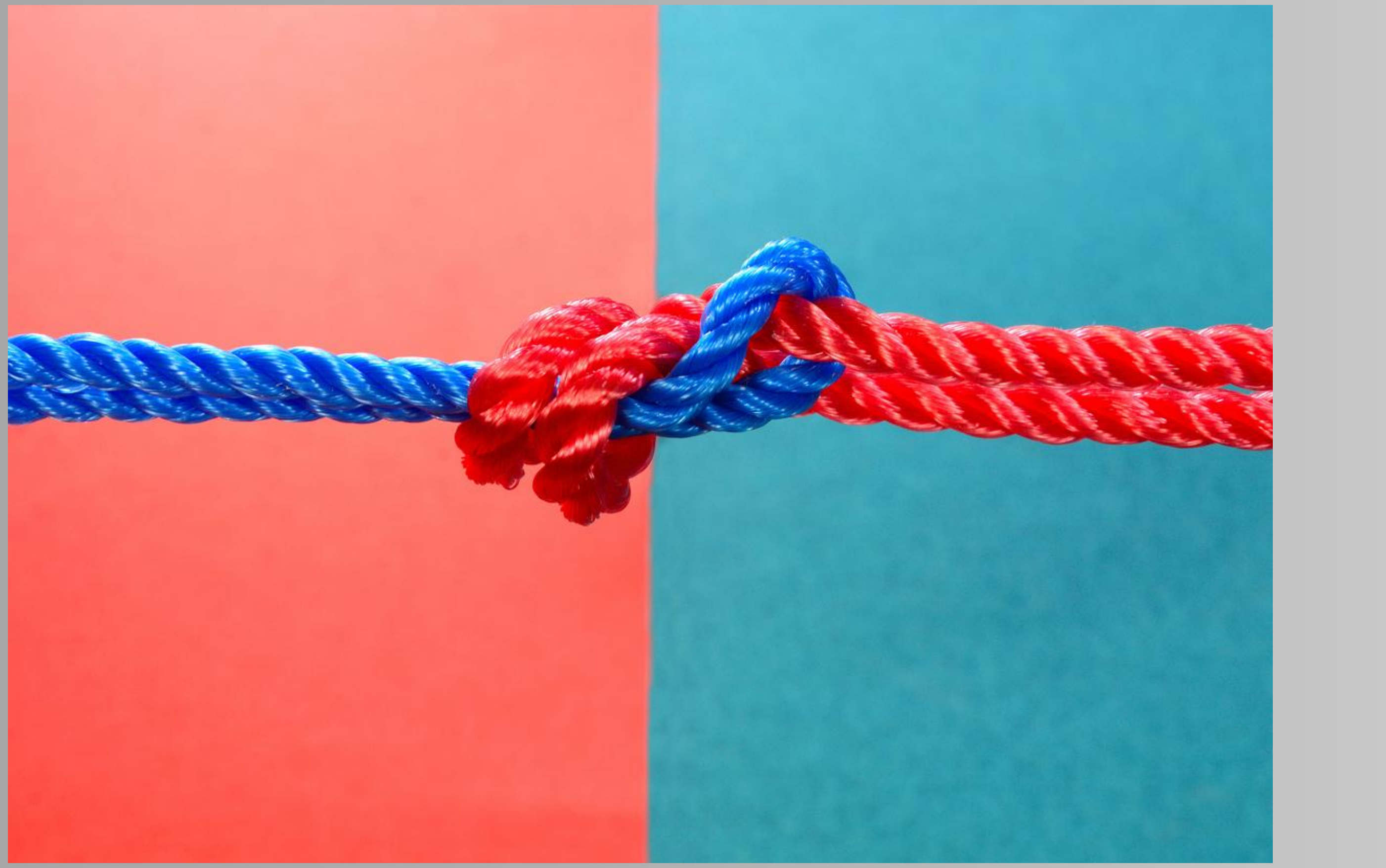
Continuous Evaluation:

- Treat risk governance as a dynamic and ongoing process.
- Regularly evaluate and update risk management strategies to adapt to new threats.
- Ensure that governance frameworks are flexible and responsive to changes in the cybersecurity landscape.

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR

Integration of Assessments and Testing

Holistic Approach



- Combine annual assessments and monthly penetration testing for a comprehensive security strategy.
- Use assessment findings to inform penetration testing scenarios and vice versa.
- Ensure that both processes are integrated into the overall risk management framework.

scarlett|group

Audience Q&A

Join at slido.com
#4042579

slido

Contact Us!

Tyler Chancey
Director of Cybersecurity
tchancey@scarlettgroup.com
Phone: 904.688.2211

Joe Kynion
Director of Information Technology
kynionj@hillstaxfl.gov
Phone: 813.612.6769

scarlett|group

NANCY C. MILLAN
HILLSBOROUGH COUNTY
TAX COLLECTOR