CISO Insights to BEAD & E-ACAM Cybersecurity Requirements

nrtc

SILVERSKY

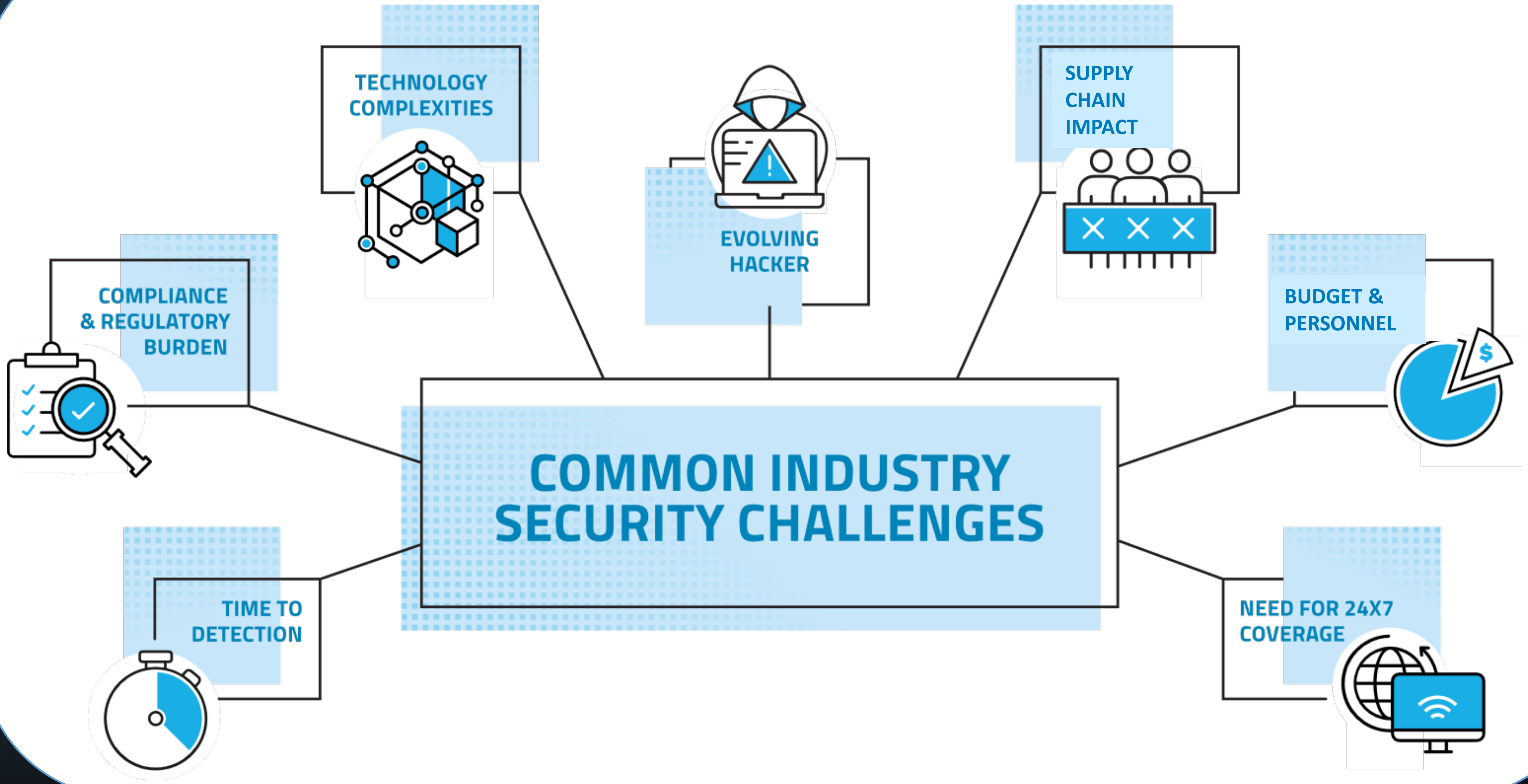
Tom Neclerio, SVP and CISO
CISSP, CGEIT, CRISC, CDPSE, CMMC-RP

BEAD Cyber Requirements

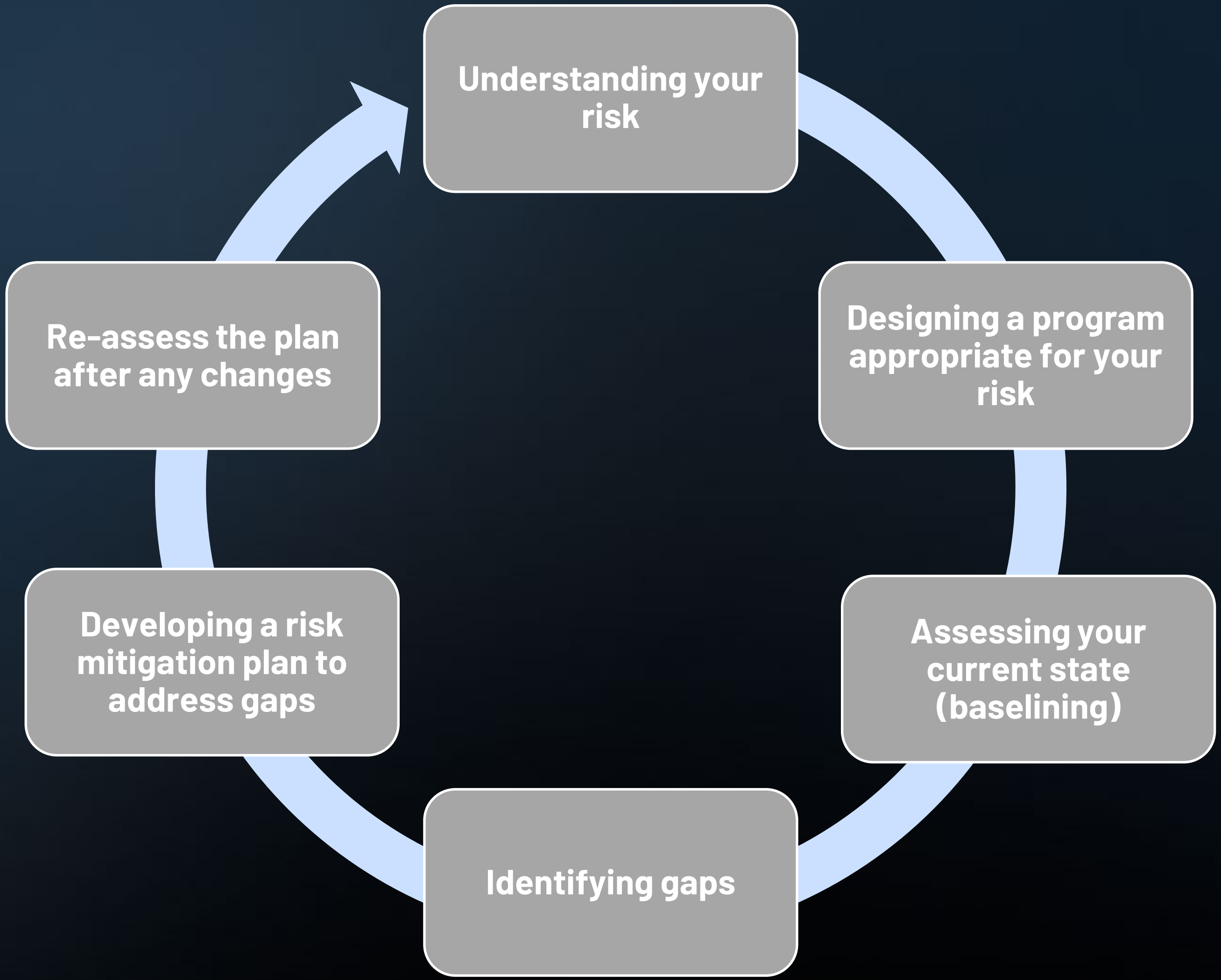
- Requires organizations have a cyber security strategy and risk management plan in place prior to receiving funding

Develop A Cyber Risk Management Plan	Develop A Supply Chain Risk Program
Plan must be operationalized or ready to be prior to grant	Plan must be operationalized or ready to be prior to grant
Plan must align with NIST Cyber Security Framework (CSF)	Plan must align with NIST NISTIR 8276: Supply Chain Risk Management
Plan must be submitted to entity prior to funding	Plan must be submitted to entity prior to funding
Plan should be re-evaluated on a regular basis	Plan should be re-evaluated on a regular basis
Any changes to the plan must be re-submitted within 30 days	Any changes to the plan must be re-submitted within 30 days

Why are they making us do this?



How to build a Cyber Risk Management Plan?


Understanding your risk

Designing a program appropriate for your risk

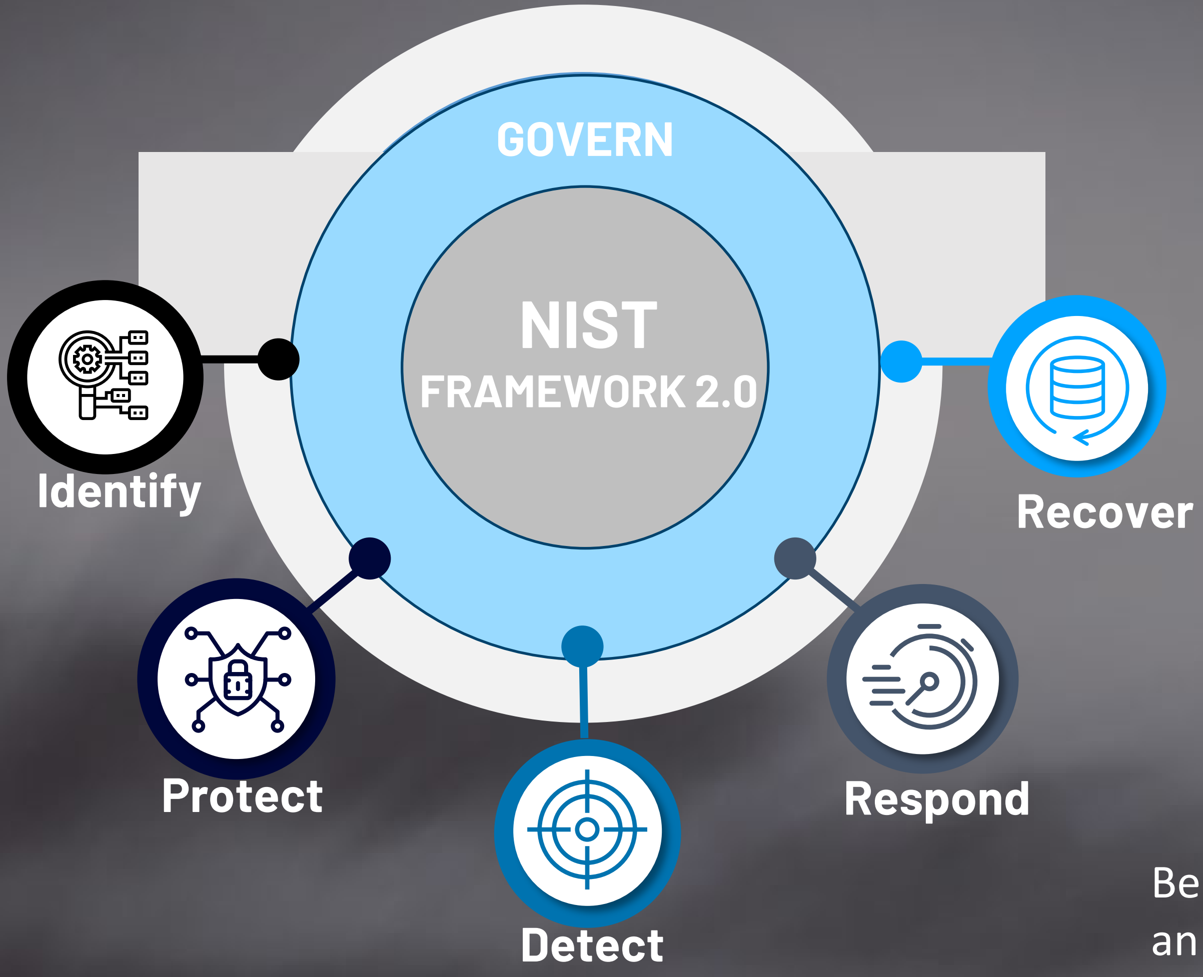
Assessing your current state (baselining)

Identifying gaps

Developing a risk mitigation plan to address gaps

Re-assess the plan after any changes

Aligning your Program with NIST CSF



Understanding your risk and regulations

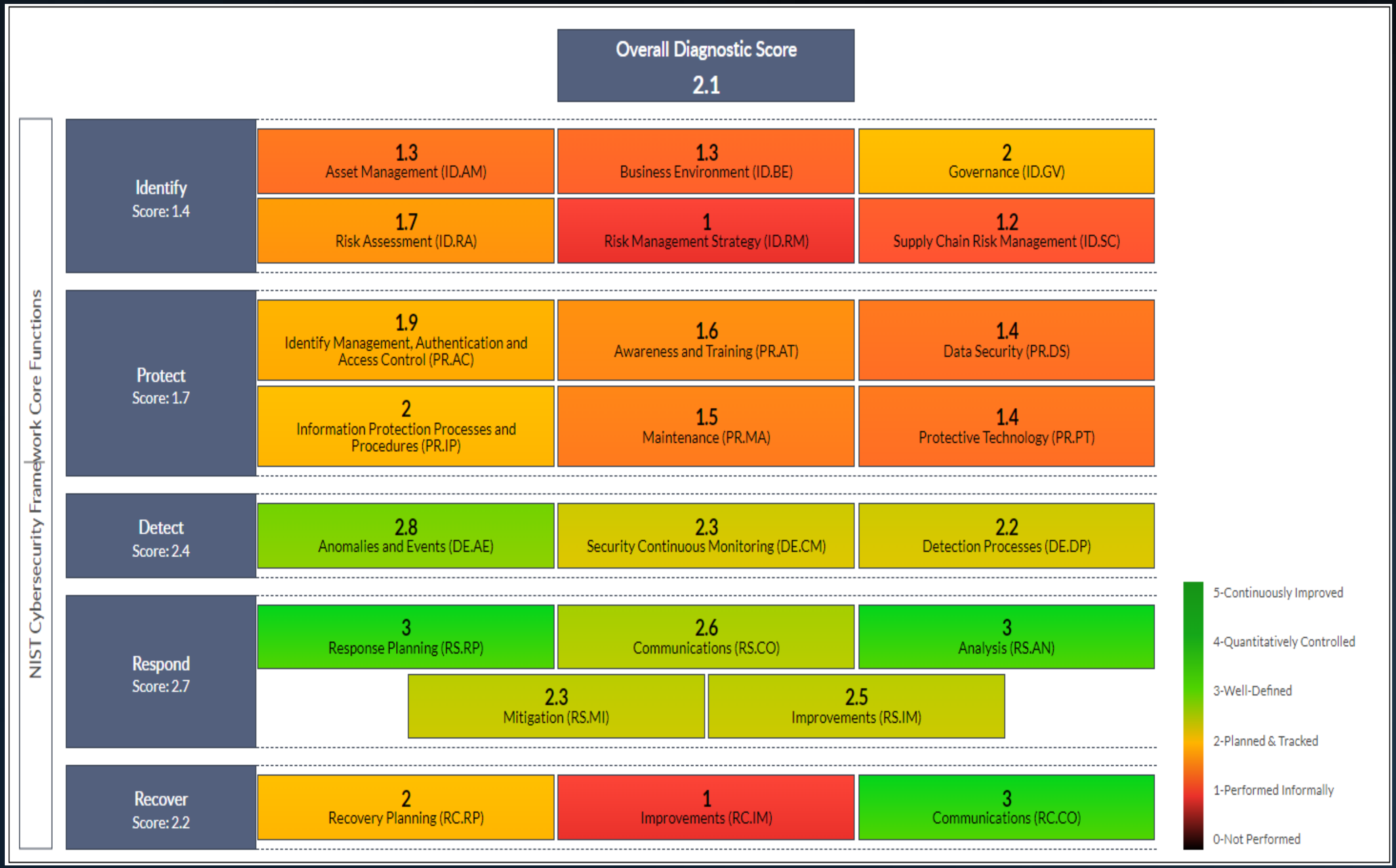
Reducing the likelihood of a damaging cyber intrusion

Developing the ability to quickly detect a potential intrusion

Be prepared to respond if an intrusion occurs

Maximize the ability to recover from a cyber incident

Assessing your current state – Baselining your Program

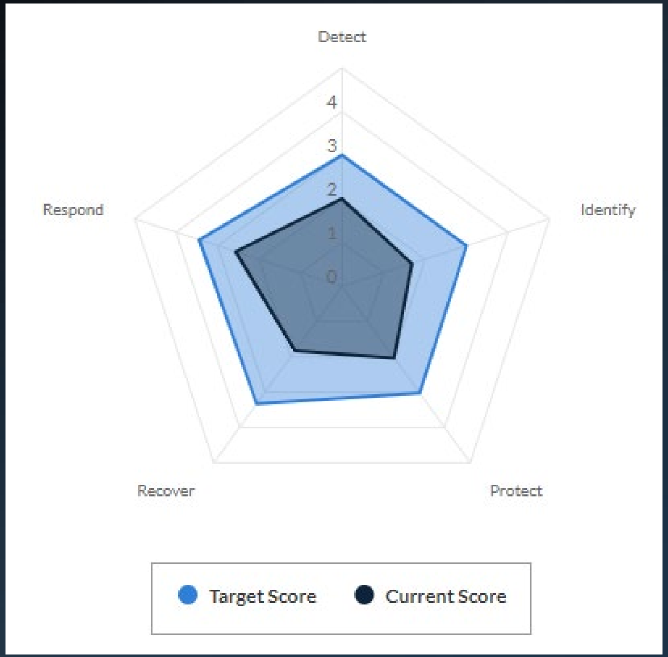


Overall Diagnostic Score
2.1

NIST Cybersecurity Framework Core Functions

Identify Score: 1.4	1.3 Asset Management (ID.AM)	1.3 Business Environment (ID.BE)	2 Governance (ID.GV)
	1.7 Risk Assessment (ID.RA)	1 Risk Management Strategy (ID.RM)	1.2 Supply Chain Risk Management (ID.SC)
Protect Score: 1.7	1.9 Identify Management, Authentication and Access Control (PR.AC)	1.6 Awareness and Training (PR.AT)	1.4 Data Security (PR.DS)
	2 Information Protection Processes and Procedures (PR.IP)	1.5 Maintenance (PR.MA)	1.4 Protective Technology (PR.PT)
Detect Score: 2.4	2.8 Anomalies and Events (DE.AE)	2.3 Security Continuous Monitoring (DE.CM)	2.2 Detection Processes (DE.DP)
Respond Score: 2.7	3 Response Planning (RS.RP)	2.6 Communications (RS.CO)	3 Analysis (RS.AN)
	2.3 Mitigation (RS.MI)	2.5 Improvements (RS.IM)	
Recover Score: 2.2	2 Recovery Planning (RC.RP)	1 Improvements (RC.IM)	3 Communications (RC.CO)

5-Continuously Improved
4-Quantitatively Controlled
3-Well-Defined
2-Planned & Tracked
1-Performed Informally
0-Not Performed



SILVERSKY™

Identifying gaps and creating a Risk Mitigation Plan

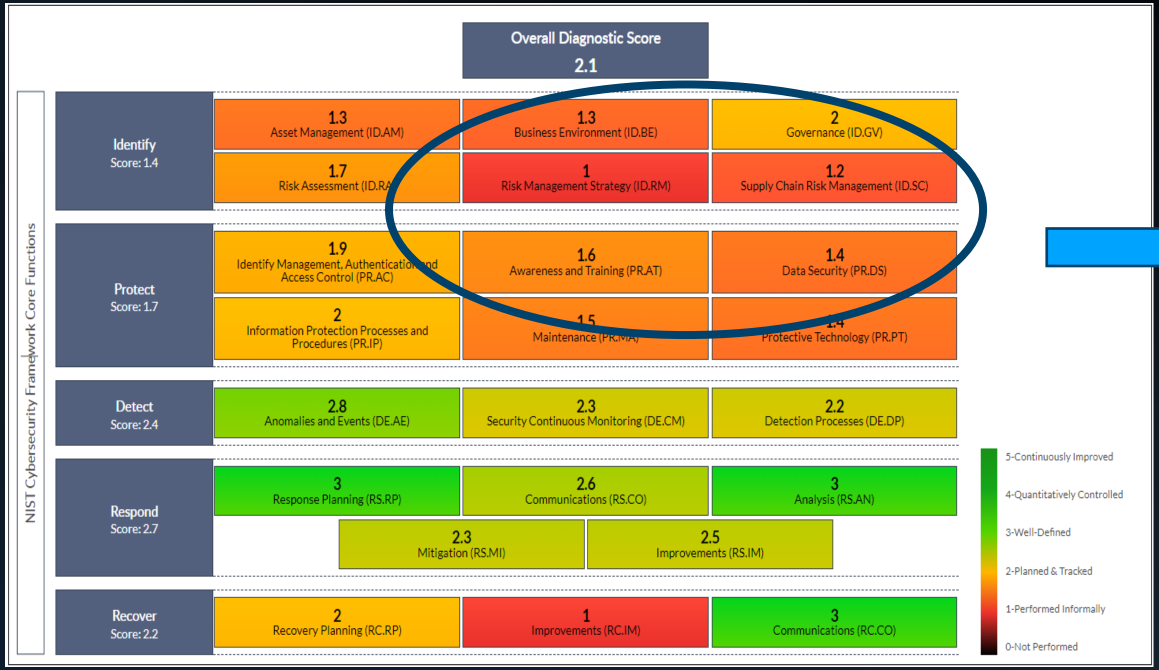
High Priority Actions (0-6 Months)

Control	Control Function	Recommended Action	Scheduled Completion Date	Assigned Party
ID.SC, ID.RM, ID.GV	Identify	**Establish a Supply Chain Risk Management Strategy.** A Secure Supply Chain Risk Management (SCRM) program is critical to ensure a holistic approach to risk identification and treatment. Globally, the supply chain remains a growing attack vector in recent years and establishing a program to protect against this risk is critical.	30th November 2024	IT Director

Medium Priority Actions (6-12 Months)

Control	Control Function	Recommended Action	Scheduled Completion Date	Assigned Party
ID.SC, ID.RM, ID.GV	Identify	**Recovery Plan testing and Lessons Learned**. Test the current Incident Response and Disaster Recovery Plan. Testing will inform if the plan isn't meeting recovery objective requirements and identify the necessary changes. Testing outcomes must be evaluated against required goals and improvements tracked and applied. Testing should include all Third Parties as required.	30th January 2025	IT Director

Re-assessing the plan after changes

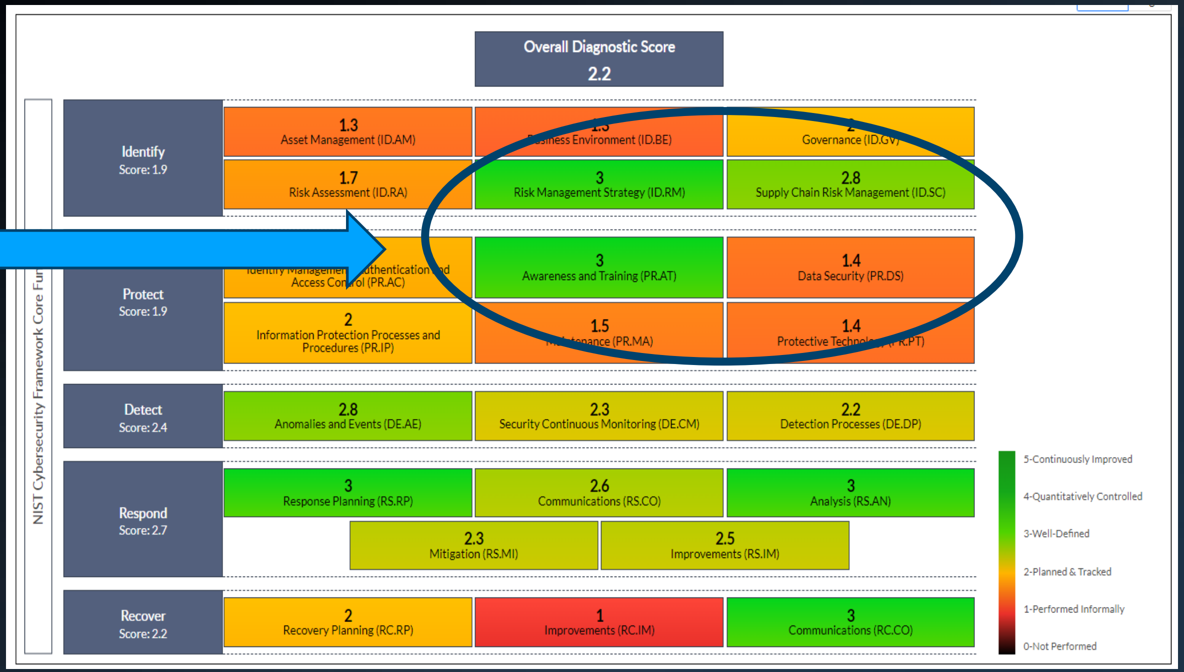


Overall Diagnostic Score
2.1

NIST Cybersecurity Framework Core Functions

Identify Score: 1.4	1.3 Asset Management (ID.AM)	1.3 Business Environment (ID.BE)	2 Governance (ID.GV)
	1.7 Risk Assessment (ID.RA)	1 Risk Management Strategy (ID.RM)	1.2 Supply Chain Risk Management (ID.SC)
Protect Score: 1.7	1.9 Identify Management, Authentication and Access Control (PR.AC)	1.6 Awareness and Training (PR.AT)	1.4 Data Security (PR.DS)
	2 Information Protection Processes and Procedures (PR.IP)	1.5 Maintenance (PR.MA)	1.4 Protective Technology (PR.PT)
Detect Score: 2.4	2.8 Anomalies and Events (DE.AE)	2.3 Security Continuous Monitoring (DE.CM)	2.2 Detection Processes (DE.DP)
Respond Score: 2.7	3 Response Planning (RS.RP)	2.6 Communications (RS.CO)	3 Analysis (RS.AN)
	2.3 Mitigation (RS.MI)	2.5 Improvements (RS.IM)	
Recover Score: 2.2	2 Recovery Planning (RC.RP)	1 Improvements (RC.IM)	3 Communications (RC.CO)

5-Continuously Improved
4-Quantitatively Controlled
3-Well-Defined
2-Planned & Tracked
1-Performed Informally
0-Not Performed



Overall Diagnostic Score
2.2

NIST Cybersecurity Framework Core Fun

Identify Score: 1.9	1.3 Asset Management (ID.AM)	1.3 Business Environment (ID.BE)	2 Governance (ID.GV)
	1.7 Risk Assessment (ID.RA)	3 Risk Management Strategy (ID.RM)	2.8 Supply Chain Risk Management (ID.SC)
Protect Score: 1.9	Identity Managemen uthentication nd Access Con ol (PR.AC)	3 Awareness and Training (PR.AT)	1.4 Data Security (PR.DS)
	2 Information Protection Processes and Procedures (PR.IP)	1.5 Maintenance (PR.MA)	1.4 Protective Technology (PR.PT)
Detect Score: 2.4	2.8 Anomalies and Events (DE.AE)	2.3 Security Continuous Monitoring (DE.CM)	2.2 Detection Processes (DE.DP)
Respond Score: 2.7	3 Response Planning (RS.RP)	2.6 Communications (RS.CO)	3 Analysis (RS.AN)
	2.3 Mitigation (RS.MI)	2.5 Improvements (RS.IM)	
Recover Score: 2.2	2 Recovery Planning (RC.RP)	1 Improvements (RC.IM)	3 Communications (RC.CO)

5-Continuously Improved
4-Quantitatively Controlled
3-Well-Defined
2-Planned & Tracked
1-Performed Informally
0-Not Performed

- Update your plan to show improvements or completed tasks
- Any changes to the plan must be re-submitted within 30 days

SILVERSKY™

Supply Chain Risk Management

Establishing A Program

Key Phases:

1. **Developing the Foundation**

    - SCRM charter document – establishes committee of different business unit stakeholders

    - SCRM policy – establishes requirements of what must be done

    - SCRM standard operating procedure – establishes how it should be done

SILVERSKY™

Supply Chain Risk Management

Establishing A Program

Key Phases:

2. **Assessing Vendors**

   - Establish a list of key vendors (those that perform critical functions or store critical data)
   - Assess vendors base on some metric - data sensitivity, data exposure, data volume
   - Rank vendors based on criticality (tier 1, 2, 3)
   - Establish review guidelines, contract/legal language and frequency based on tier levels

Legal Contract Clauses

- Third Party Audit Requirement
- Right to Audit
- Breach Notification
- Data Handling
- Security Questionnaire
- Indemnification

SILVERSKY

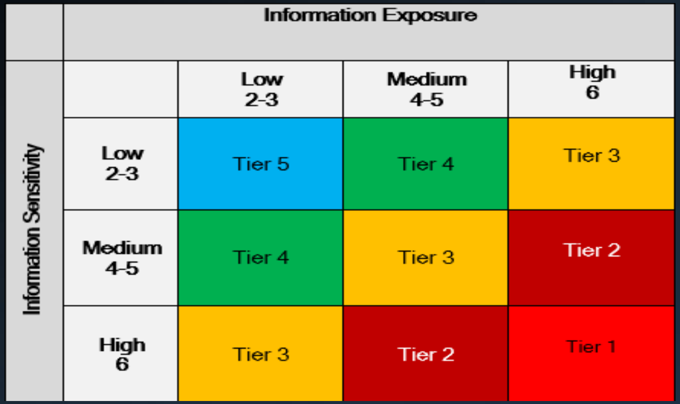
Supply Chain Risk Management

Establishing A Program

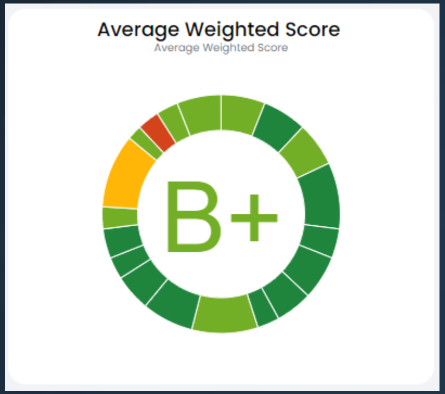
Key Phases:

3. Continuous Monitoring

- Establish a program to review vendors on a regular interval based on criticality tiers
- Security questionnaires, audit reports, third party risk monitoring platforms



		Information Exposure		
		Low 2-3	Medium 4-5	High 6
Information Sensitivity	Low 2-3	Tier 5	Tier 4	Tier 3
	Medium 4-5	Tier 4	Tier 3	Tier 2
	High 6	Tier 3	Tier 2	Tier 1



Average Weighted Score

More than Checking the Box: Key Takeaways

Understand your risk. “The Who and What”

- Build a Cyber Program that is appropriate to your risk

Evaluate your current state and build a plan of action

- Baseline current state and a build a roadmap for future state

Security is Continuous

- Measure success towards your plan

Don’t take the Journey Alone!

- Find a good partner and resources to help

Questions?

Sign up for your FREE
Dark Web Account Compromise
Assessment

nrtc

SILVERSKY™

Tom Neclerio
SVP of Security Services, CISO

nrtc

SILVERSKY™

Thank You!

For more information visit: www.nrtc.coop

Or email: managedservices@nrtc.coop