



NIST Cybersecurity Framework

Assessing the Maturity of your Cybersecurity Program

April 21, 20120



@PeterMorin123



Peter Morin, CISSP

Director, Cybersecurity & Privacy Consulting

- Based out of Halifax, Nova Scotia, Canada
- Over 20 years of experience cyber security
- Part of PwC's Cyber Utilities Practice
- Specialize in security of critical infrastructure, incident response, threat hunting, etc.
- Worked in the past for the various military and government agencies
- Spoken at events run by BlackHat, FBI, DHS, ISACA, US DoD as well as lectured a numerous colleges and universities.
- CISSP, CISA, CRISC, CGEIT, GCFA



@PeterMorin123

Coming to you from the other coast!!




NOVA SCOTIA



@PeterMorin123

Agenda

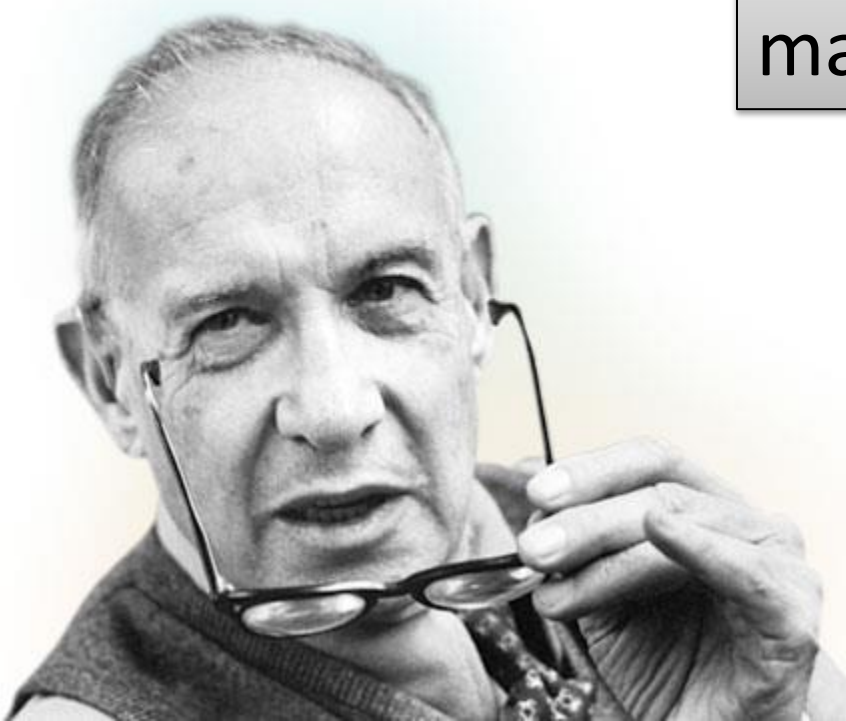
- **NIST CSF Framework: Assessing the Maturity of your Cybersecurity Program**
 - Background on the NIST CSF and its comparison with other maturity frameworks
 - Understanding the value proposition related to assessing the maturity of your cybersecurity program
 - Framework implementation guidance using a simplified process
 - Assessing the maturity of your cybersecurity program
 - Setting a target maturity goal
 - Developing a cybersecurity remediation roadmap
 - Tools to assist in the assessment and visualization of your cybersecurity maturity
 - Reporting maturity to executives and boards



Assumptions

- Every enterprise is increasingly aware of cyber risk, and is seeking to 'manage it' through:
 - Policies, procedures and other administrative controls
 - Technology-based controls
 - Insurance (aka, 'risk transfer')
 - Risk acceptance
- Cyber is an enterprise-wide risk management issue
 - It is much broader than the certification or compliance such as PCI DSS or HIPAA
 - It is a business issue, not only a technology issue
- Attendees may be looking for:
 - A place to start their cybersecurity programs, or
 - A way to communicate with stakeholders and set priorities & budgets
 - A way to measure progress
 - A way to get risk under (sufficient) control





“If you can't measure it, you can't manage it.”

Peter Drucker



@PeterMorin123

Why Measure Maturity?

- Identifying successes and highlighting opportunities for improvement
- Jump-starting improvement initiatives
- Energizing change initiatives
- Energizing the workforce
- Assessing performance against both the NIST CSF and benchmarking against your peers
- Better alignment of resources with organization objectives
- Could serve to provide validation of your cybersecurity posture to your clients, board, shareholders, etc.



Various Ways to Measure Maturity



Some can be self-delivered, some may require a third party



@PeterMorin123

NIST CSF

- National Institute for Standards and Technology (NIST) published version 1.0 of their Cybersecurity Framework (CSF) in February 2014
- In response to Executive Order 13636 as an effort to improve cybersecurity of critical infrastructure
- NIST released its most current version 1.1 of the Framework CSF in April 2018



The screenshot shows the White House website's briefing room page. The header includes the White House logo and navigation links for 'BRIEFING ROOM', 'ISSUES', 'THE ADMINISTRATION', and '1600 PENN'. Below the header, there are links for 'HOME', 'BRIEFING ROOM', 'PRESIDENTIAL ACTIONS', and 'EXECUTIVE ORDERS'. A sidebar on the left lists various content categories, with 'Executive Orders' highlighted in red. The main content area features the title 'Executive Order -- Improving Critical Infrastructure Cybersecurity' and the text 'EXECUTIVE ORDER' followed by 'IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY'. The text begins with 'By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:' and includes a section on policy regarding cyber intrusions into critical infrastructure.

Source: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>



@PeterMorin123

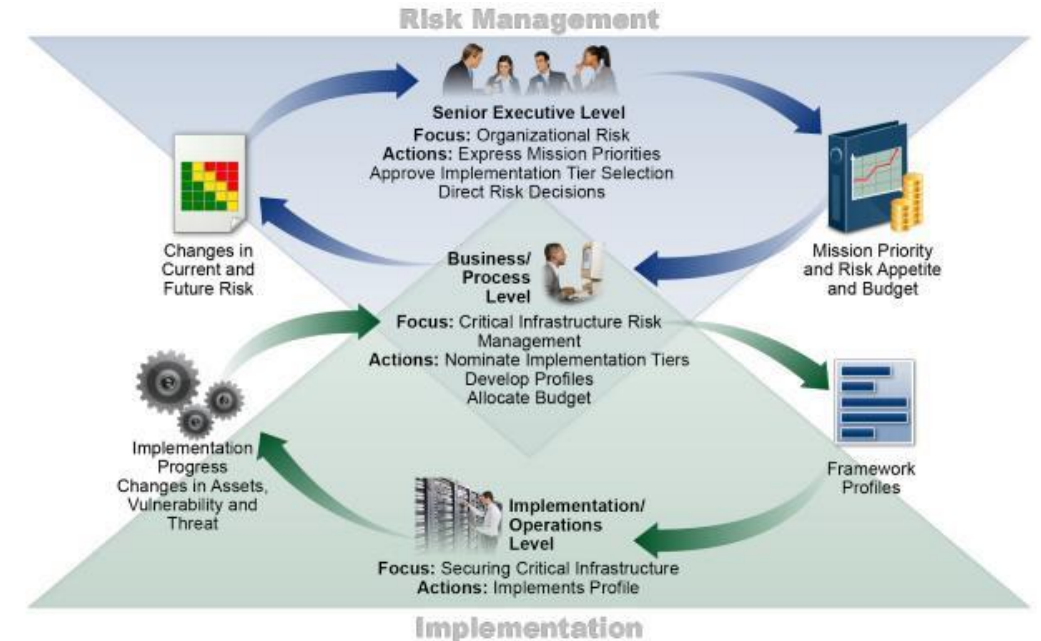
NIST CSF

- **Common language** for addressing and understanding cybersecurity risk management
- Especially helpful for communicating risks to stakeholders
- Establishing clear lines of communication to upper-management is an essential first step for incorporating cybersecurity into an organization's overall mission



Why NIST CSF?

- Intent
 - Voluntary
 - Adaptable and flexible
- Leverages standards, methodologies, and processes
 - Not a compliance checklist or control
- It's a framework
 - Not a law or regulatory mandate
- Risk-based approach
 - Focused on top-down high impact risks
 - Connects executive, business, and security operations



Source: <https://www.nist.gov/sites/default/files/documents/////draft-cybersecurity-framework-v1.11.pdf>



@PeterMorin123

Critical Infrastructure



ENERGY



HEALTH



TRANSPORT



FINANCIAL



ICT



WATER



FOOD



**PUBLIC & LEGAL
ORDER AND
SAFETY**



**CHEMICAL &
NUCLEAR
INDUSTRY**



**SPACE AND
RESEARCH**



Most Common Applications of CSF

- Evaluate an enterprise-wide cybersecurity posture and maturity by conducting an assessment against the CSF model
 - Determine the desired cybersecurity posture and plan and prioritize resources and efforts to achieve the target maturity.
- Evaluation of current and proposed products and services to meet security objectives aligned to CSF
 - Identify capability gaps and opportunities to reduce overlap/duplicative capabilities for efficiency.
- A reference for restructuring their security teams, processes, and training.



NIST CSF vs. ISO 27001

- Both involve establishing cybersecurity controls
- ISO 27001 comes with a recognized certification and can be used to prove its abilities to its clients, partners, shareholders – but requires a third party to certify
- NIST Cybersecurity Framework is not certifiable and auditable – set of voluntary cyber security standards
- ISO 27001 focuses on protecting all types of information, not just information processed in IT systems (i.e. paper-based information)



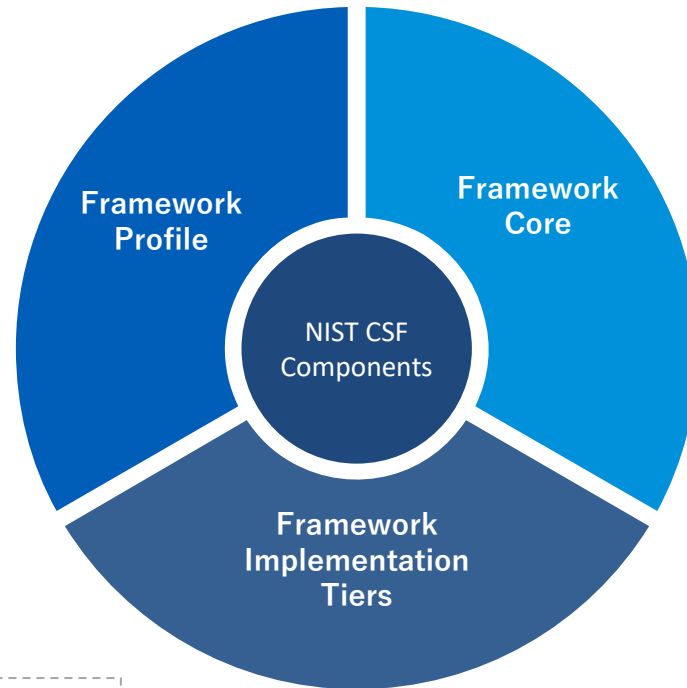
NIST CSF vs. ISO 27001

- ISO 27001 defines which documents and records are needed, and what is the minimum that must be implemented
- CSF is better structured when it comes to planning and implementation
- CSF enables both the top management but also engineers and other IT staff to understand easily what is to be implemented, and where the vulnerabilities are.



NIST CSF Components

Profiles are an organization's unique **alignment** of their **organizational requirements** and **objectives, risk appetite, and resources** against the desired outcomes of the Framework Core.



The Core is a set of **desired cybersecurity activities and outcomes** organized into Categories and aligned to Informative References.

Tiers describe the **degree to which an organization's cybersecurity risk management practices** exhibit the characteristics defined in the Framework.

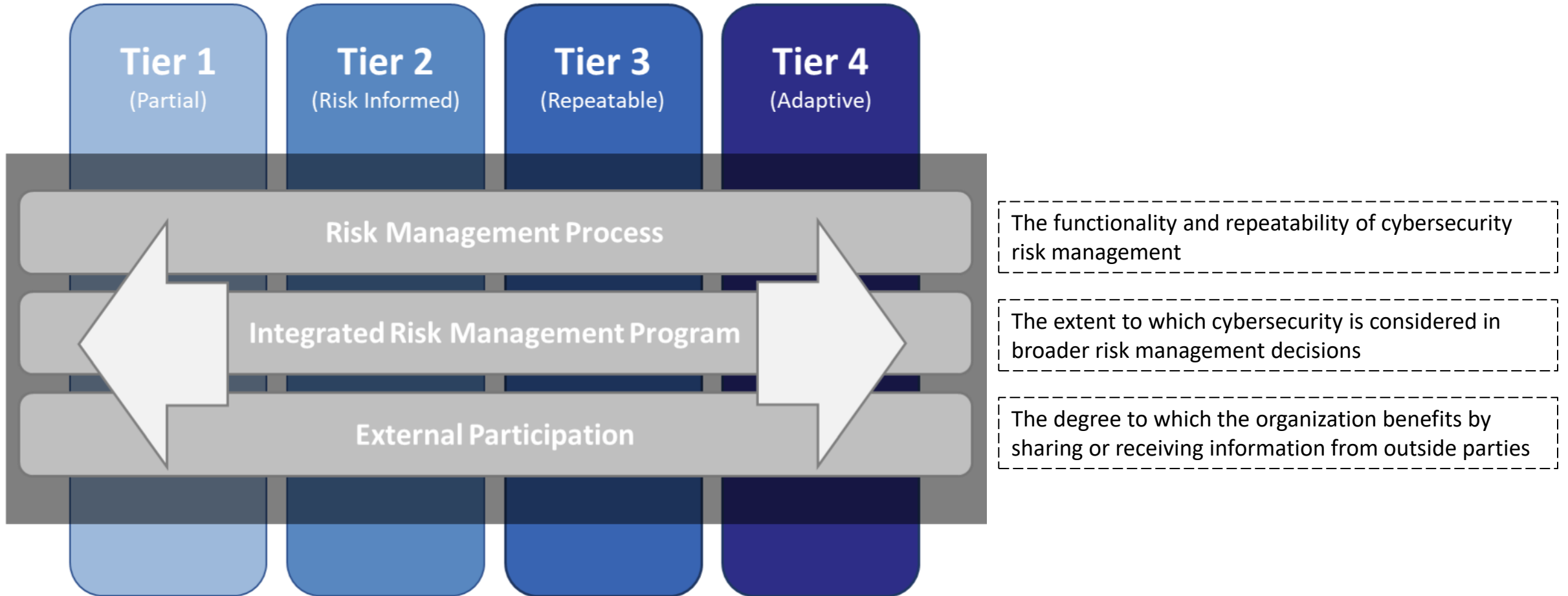


Framework Implementation Tiers

- Allow entities to **identify** their **priorities**
- Based on the assumption that different entities face different cybersecurity risks.
- Enterprises can read through the tier qualifications (i.e. level of budget, size of company) and identify which tier, and subsequent guidelines, best fit their businesses.



Framework Implementation Tiers



Framework Profiles

- Profiles guide entities through a self-assessment
- Optimizing the CSF to best serve the organization
- Assists in identifying:
 - How to best allocate resources
 - Priority threat vectors
 - How to design a unique plan for strengthening their organization's cybersecurity infrastructure.
 - These requirements and objectives can be compared against the current operating state of the organization to gain an understanding of the gaps between the two



Framework Profiles

- Ways to think about a Profile:
 - A customization of the Core for a given sector, subsector, or organization.
 - A fusion of business/mission logic and cybersecurity outcomes.
 - An alignment of cybersecurity requirements with operational methodologies.
 - A basis for assessment and expressing target state.
 - A decision support tool for cybersecurity risk management.



Framework Core

Recover: Maintaining plans for resilience, restore capabilities or services

Respond: Action regarding a detected cybersecurity event

Detect: Identify the occurrence of a cybersecurity event



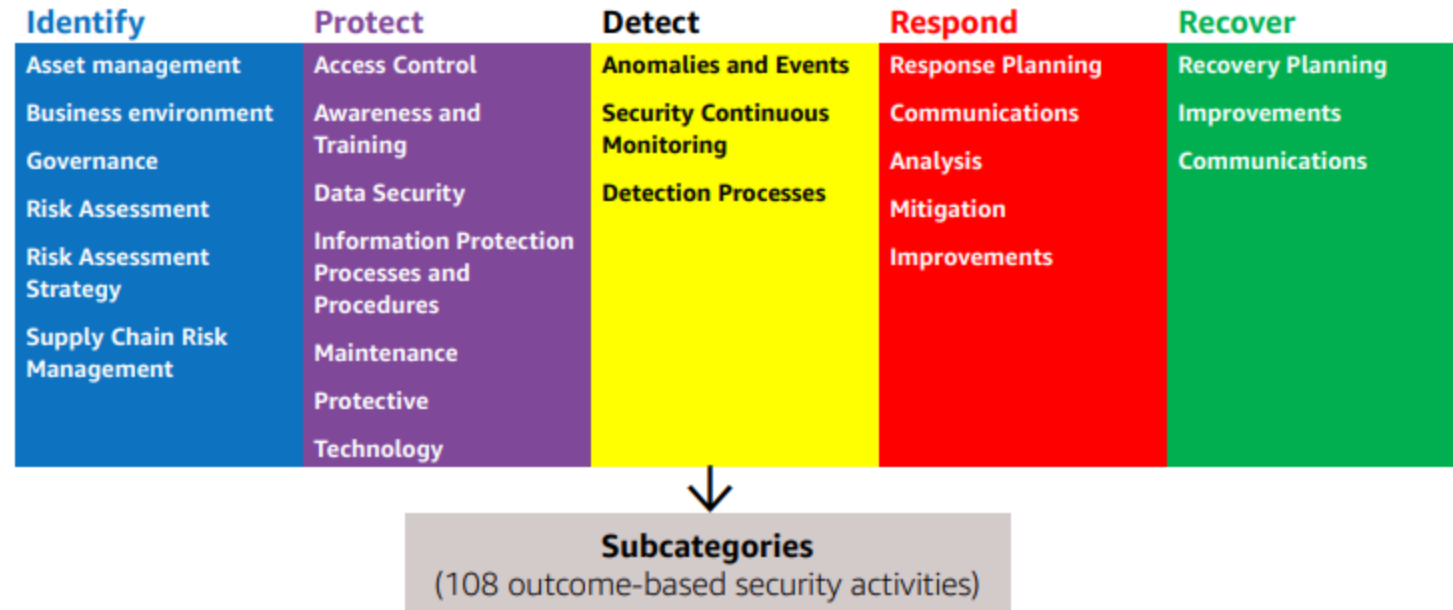
Identify: Understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Protect: Safeguards to ensure delivery of critical infrastructure services



Framework Core

- NIST CSF Core
 - Functional areas (i.e. Identify)
 - Categories (i.e. Asset Management)
 - Sub-categories (i.e. Physical devices and systems within the organization are inventoried)



Framework Core

Function ↓	Category ↓	Sub-Category ↓	Industry standards and alignment ↓
<p>PROTECT (PR)</p>	<p>Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<ul style="list-style-type: none"> · CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family
		<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</p>	<ul style="list-style-type: none"> · CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16



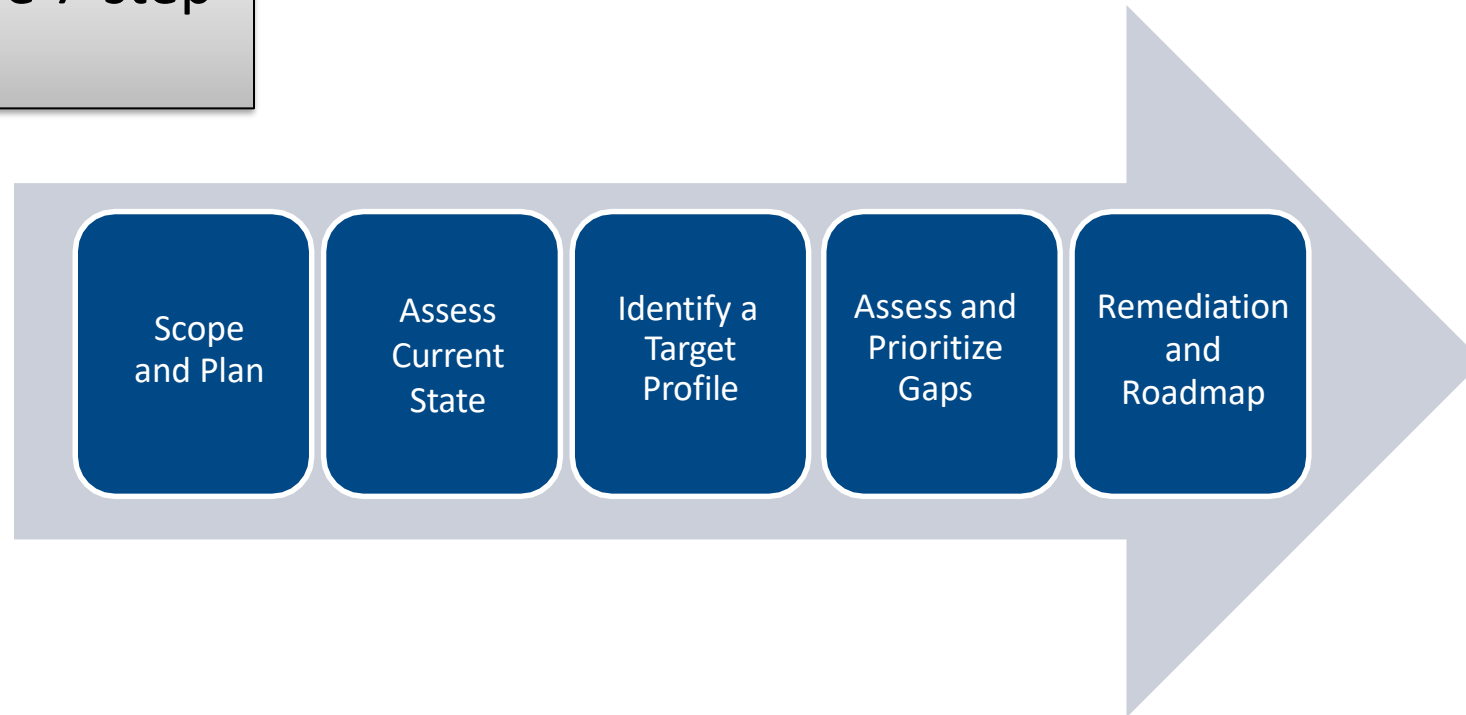
NIST CSF v1.0 vs. 1.1 (Core)

- 1 New Category (in the Identify Function area)
- 10 New Subcategories (in the Identify/Protect/Respond Function areas)
- 26 Subcategories Reworded from v1.0 — changes including:
 - Improved grammar
 - Added details
 - Removed extraneous words
 - Greater use of cyber security vs. information security
- v1.0 is still compatible with v1.1 (all items in v1.0 are in v1.1)



5-Step Assessment Process

Simplified from the 7-step
NIST CSF Process!



Step 1: Scope and Plan

- Identify **organization** or **mission objectives** along with high-level organizational **priorities**
- Allows the organization to make **strategic cybersecurity implementation decisions** and determine the scope of the systems (and other assets) that will support the organization
- Important to identify important systems and assets so that their protection can be prioritized



Step 1: Scope and Plan

- **What are you trying to assess?**
 - Enterprise
 - Business Unit
 - Business Process
 - Service for a client
- How does the assessment target align with overall goals and priorities?
- **You also should identify your top risks at this point**
 - Identify your **assets**;
 - Identify the **threats** to those assets;
 - Identify your **vulnerabilities** to those threats.



Threats, Assets, Vulnerabilities, & Risk Events

A process to identify, prioritize, and manage the cybersecurity risks that may prevent the organization from achieving corporate objectives and maintaining its reputation.

The process considers **threats**, **assets**, **vulnerabilities**, and **risk events**:

Threat



Anything that is capable, by its action or inaction, of compromising your organization. This includes users.

Asset



In cybersecurity, we concern ourselves with assets that are connected to a network, or assets that could be compromised by intentional or unintentional digital access.

Vulnerability



A weakness or flaw in a system that exposes it to intentional or unintentional compromise.





Risk Event



An occurrence that exploits one or more vulnerabilities, causing an impact on an asset(s). We intentionally include the word "event", since a risk requires that something happens.



Cyber Threats and Adversaries (example)

Adversary	Motives	Organization Targets	Impact
 Organized crime	<ul style="list-style-type: none"> • Immediate financial gain • Collect information for future financial gains (i.e. CCs) • Sell intellectual property 	<ul style="list-style-type: none"> • Organization customer records • Employee personal and health information • Financial / payment systems • Financial information 	<ul style="list-style-type: none"> • Customer and shareholder lawsuits • Regulatory inquiry/penalty • Financial loss • Brand and reputation
 Hacktivists	<ul style="list-style-type: none"> • Influence political and /or social change • Pressure Organization to change your practices • Affect services to end customers 	<ul style="list-style-type: none"> • Sensitive business information • Personal information (board, executives, employees) • Operational assets • Customer data 	<ul style="list-style-type: none"> • Disruption of business activities • Brand and reputation • Loss of stakeholder confidence • Lawsuits
 Nation state	<ul style="list-style-type: none"> • Act of aggression as a political statement 	<ul style="list-style-type: none"> • Operational technologies • Intellectual property • Government assets 	<ul style="list-style-type: none"> • Disruption to operations • Regulatory inquiry/penalty • Brand and reputation
<hr/>			
 Insiders	<ul style="list-style-type: none"> • Personal advantage, monetary gain • Professional revenge • Bribery or coercion 	<ul style="list-style-type: none"> • Sensitive business/corporate information • Operational technologies • Intellectual property 	<ul style="list-style-type: none"> • Regulatory inquiry/penalty • Operational disruption • Disruption to operations • Loss of stakeholder confidence



Step 1: Scope and Plan

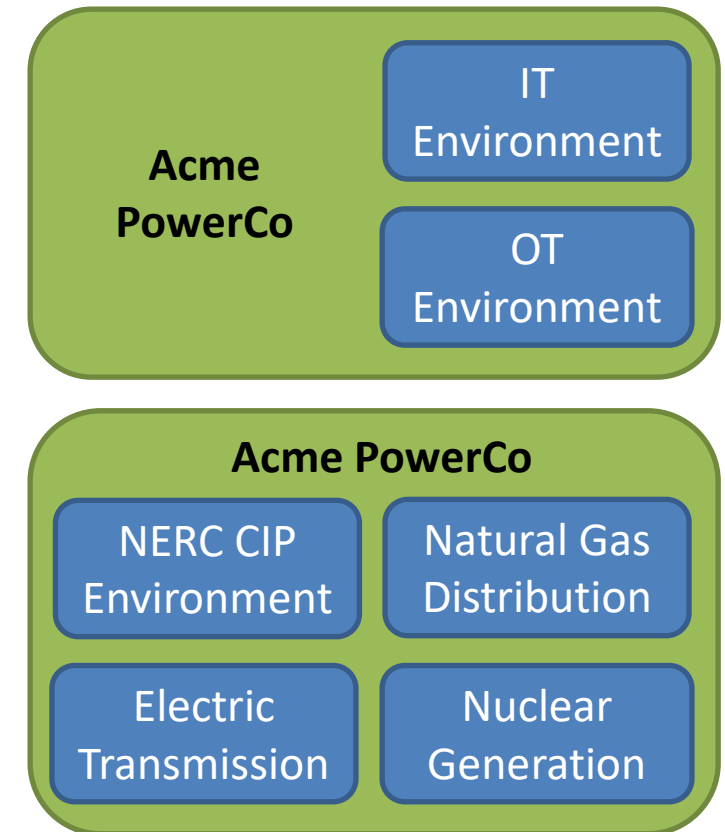
- Identify your **digital crown jewels**
 - The **digital** assets of greatest value and that would cause a material business impact if compromised.
 - Due to their value, the **Crown Jewels** are a top target of adversarial cyber threats and organizations must prioritize their protection
- What are the supporting IT systems and assets?
- Who are the relevant business owners, team leads, etc.?
- What are the relevant legal, regulatory, and contractual requirements?
- Has a risk strategy been developed and implemented?



Step 1: Scope and Plan

Asset Classes

- If you assess the controls from your high-security environment with you low-security environment, you may get an unrealistic maturity rating.
- Compliance-based environments: PCI-DSS, NERC CIP, SOX, etc.
- Think about where management, networks or applications could be very different (i.e. POS environment vs. corporate systems at a retailer).



Step 2: Assess Current State

- Developed by indicating which control outcomes (Category and Subcategory) of the Core are currently being achieved.
- Partially achieved controls should be noted so supporting baseline information regarding subsequent steps can be provided.
- The Current Profile should integrate every control found in the NIST CSF in order to determine which control outcomes are being achieved.



PR.AT-1: All users are informed and trained

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
		PR.AE	Anomalies and Events
DE	Detect	DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	<ul style="list-style-type: none"> • CIS CSC 17, 18 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 • NIST SP 800-53 Rev. 4 AT-2, PM-13
	PR.AT-2: Privileged users understand their roles and responsibilities	<ul style="list-style-type: none"> • CIS CSC 5, 17, 18 • COBIT 5 APO07.02, DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	<ul style="list-style-type: none"> • CIS CSC 17 • COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
	PR.AT-4: Senior executives understand their roles and responsibilities	<ul style="list-style-type: none"> • CIS CSC 17, 19 • COBIT 5 EDM01.01, APO01.02, APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	<ul style="list-style-type: none"> • CIS CSC 17 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13



PR.AT-1: All users are informed and trained



CIS Critical Security Controls No. 17

17.2 - Deliver Training to Fill the Skills Gap - Deliver training to address the skills gap identified to positively impact workforce members' security behavior.

17.3 - Implement a Security Awareness Program - Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

17.5 - Train Workforce on Secure Authentication - Train workforce members on the importance of enabling and utilizing secure authentication.

17.6 - Train Workforce on Identifying Social Engineering Attacks - Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.

17.7 - Train Workforce on Sensitive Data Handling - Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.

17.8 - Train Workforce on Causes of Unintentional Data Exposure - Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

17.9 - Train Workforce Members on Identifying and Reporting Incidents - Train employees to be able to identify the most common indicators of an incident and be able to report such an incident

ISO/IEC 27001:2013
A.7.2.2, A.12.2.1



NIST SP 800-53 Rev. 4
AT-2, PM-13



COBIT 5 APO07.03,
BAI05.07

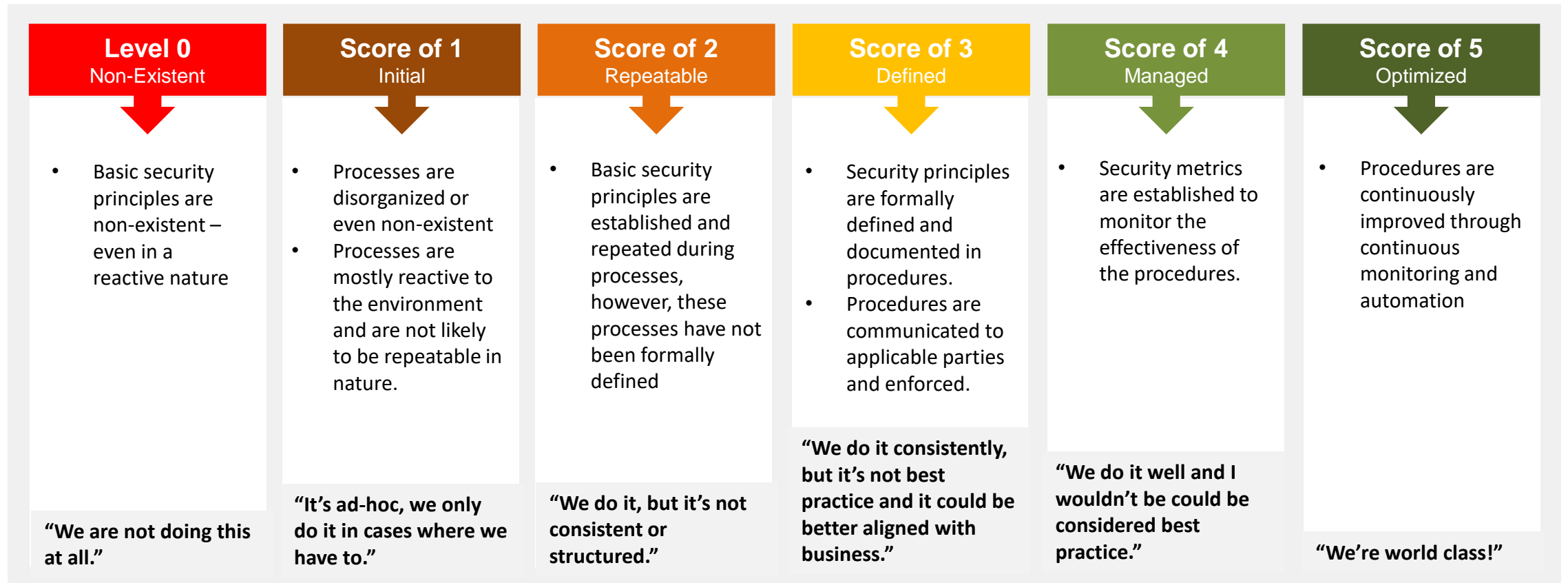


ISA 62443-2-1:2009
4.3.2.4.2, 4.3.2.4.3



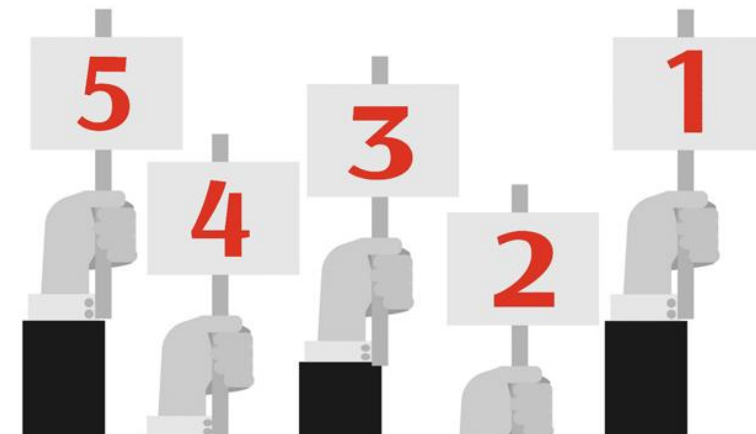
@PeterMorin123

Maturity Scoring



Step 2: Assess Current State

- **Some things to think about...**
 - You'll probably look at these subcategories and think "yeah, I'm kind of doing those things," which is good.
 - But how well are you doing them?
 - Remember, just running an ad-hoc process with governance (i.e. documentation, etc.) is not complete.
 - Also, don't assume things are being done in other departments without talking to those responsible
 - **Be honest with scoring.**



Step 2: Assess Current State

- Identify, Collect and Review
 - We gather all current documentation including policies, procedures, standards and guidelines
 - we review all information gathered and evaluate it based on industry best practice
 - Remember, this isn't an audit, so we aren't necessarily testing controls – so you don't need to collect certain data

Category	Document Examples
Identify / ID.GV (Governance)	Cybersecurity / IT governance framework
	Cybersecurity / IT committee – mandate/terms of reference and minutes of recent meeting
	Cybersecurity / IT reports/KRI/KPI/dashboard
	Cybersecurity / IT strategy
Protect / PR.AC (Identity Management and Access Control)	Access management policies and procedures (including remote access, segregation of duties and physical access)
	Guidelines or policies for sharing relevant security information with outside organizations or third-party support contractors.



Step 2: Assess Current State

- Workshops
 - We interview, discuss, and engage with relevant stakeholders to understand and document how your business and IT processes are aligned

Assessment Area	Workshop Attendee Examples
Executives	CIO, CISO, VP Operations, or similar
Legal	Chief Compliance Officer, VP Legal, General Counsel, or similar
Human Resources	Director of Human Resources, or similar
Audit	Internal Auditor, or similar
Networking Specialist	Network Engineer, or similar
IT Security Team	Director/Manager of IT, Information Security, or similar



Step 2: Assess Current State

- Start by looking at the sub-categories.
- For example, under **Anomalies and Events (AE)** in the **Detect (DE)** functional area, there are five subcategories:
 - **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
 - **DE.AE-2:** Detected events are analyzed to understand attack targets and methods
 - **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors
 - **DE.AE-4:** Impact of events is determined
 - **DE.AE-5:** Incident alert thresholds are established



Assessment Example

Functional Area	Category	Sub-category	Score
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	
		DE.AE-4: Impact of events is determined	
		DE.AE-5: Incident alert thresholds are established	

So what does “Impact of events is determined” mean?!



Assessment Example

Functional Area	Category	Sub-category
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

Internal control: The network management team monitors network traffic, utilizing solutions that alert the team to potentially abnormal traffic patterns



Assessment Example

Functional Area	Category	Sub-category
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods

Internal control: The network security team investigates alerts, escalating events, as appropriate, to the CISO, who may invoke the incident response plan



Assessment Example

Functional Area	Category	Sub-category
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-3: Event data are collected and correlated from multiple sources and sensors

Internal control: Logs are collected in a SIEM solution, which correlates and analyzes the logs to detect suspected intrusions



Assessment Example

Functional Area	Category	Sub-category
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-4: Impact of events is determined

Internal control: Events and incidents are investigated and triaged, based on the sensitivity of data and assets involved.



Assessment Example

Functional Area	Category	Sub-category
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-5: Incident alert thresholds are established

Internal control: The incident response plan is maintained by the CISO and contains thresholds used by team members to conclude whether an event must be declared an incident.



Functional Area	Category	Sub-category	Score
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	1
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	2
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	2
		DE.AE-4: Impact of events is determined	3
		DE.AE-5: Incident alert thresholds are established	4
(1 + 2 + 2 + 3 + 4 / 5) Average			2.4

Remember:

0 = non-existent

1 = Initial (some ad-hoc approaches)

2 = Repeatable (technology and/or procedures are in place where they may result in the same outcome when repeated.)

3 = Defined (complete set of policies and procedures are documented to support the security architecture)

4 = Managed (constant monitoring and measuring of policies, procedures and technology)

5 = Optimized (security architecture is fully aligned to business-driven objectives)



	B	C	D
	Current Maturity	Target Maturity	Summary Average
1 Asset Management (ID.AM)			
2 ID.AM-1: Physical devices and systems within the organization are inventoried	1	3	1.7
3 ID.AM-2: Software platforms and applications within the organization are inventoried	2	3	
4 ID.AM-3: Organizational communication and data flows are mapped	2	3	
5 ID.AM-4: External information systems are catalogued	2	3	
6 ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	2	3	
7 ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	1	3	
8 Business Environment (ID.BE)			
9 ID.BE-1: The organization's role in the supply chain is identified and communicated	0	3	1.4
10 ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	2	3	
11 ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	3	3	
12 ID.BE-4: Dependencies and critical functions for delivery of critical services are established	2	3	
13 ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	0	3	
14 Governance (ID.GV)			
15 ID.GV-1: Organizational information security policy is established	3	3	2.5
16 ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	4	3	
17 ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	2	3	
18 ID.GV-4: Governance and risk management processes address cybersecurity risks	1	3	
19 Risk Assessment (ID.RA)			
20 ID.RA-1: Asset vulnerabilities are identified and documented	3	3	2.3
21 ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	3	3	
22 ID.RA-3: Threats, both internal and external, are identified and documented	3	3	
23 ID.RA-4: Potential business impacts and likelihoods are identified	3	3	
24 ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	1	3	
25 ID.RA-6: Risk responses are identified and prioritized	1	3	
26 Risk Management Strategy (ID.RA)			
27 ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	1	3	1.0
28 ID.RM-2: Organizational risk tolerance is determined and clearly expressed	1	3	
29 ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	1	3	
30 Supply Chain Management (ID.SC)			
31 ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	3	3	3.0
32 ID.SC-2: Identify, prioritize and assess suppliers and third-party partners of information systems, components and services using a cyber supply chain risk assessment process	3	3	
33 ID.SC-3: Suppliers and 3rd-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan	3	3	
34 ID.SC-4: Suppliers and 3rd-party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted	3	3	
35 ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	3	3	
36			
37			
38			
39			
40			
41			
42			
43			
		Total Average	2.0



Step 3: Identify a Target Profile

Why set a target goal?

- Where do you want to be?
- When building your “to-be,” be aware that (with the rare exception) you don’t need to be a five.
- Being “world class” in anything takes a lot of effort and resources.
- Organizations that require world class security controls generally know it and are prepared to allocate a large budget to achieve it.
- In most cases you should probably be shooting for a four — sometimes a bit higher, sometimes a bit lower.

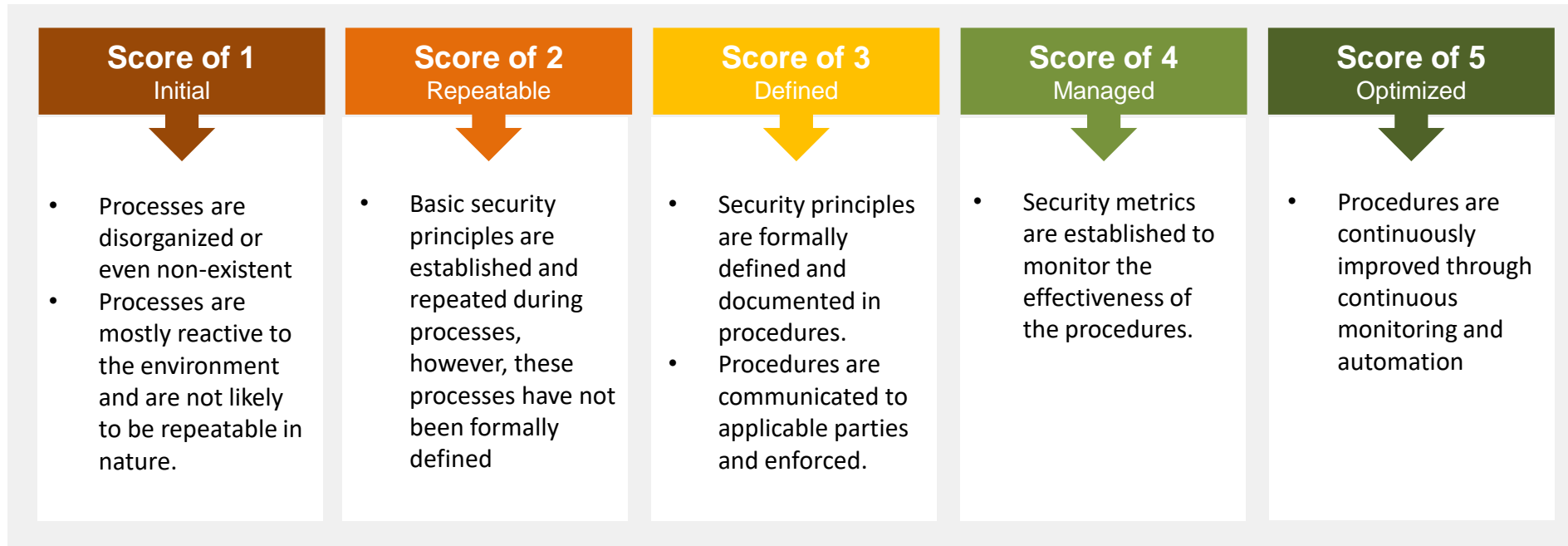


Step 3: Identify a Target Profile

- Create a target maturity score that focuses on the CSF Categories and Subcategories assessment and describes the desired cybersecurity outcomes.
- A cautious or rational approach should be taken when creating this profile.
- Risk appetite should be considered as well, where the organization determines which risk category or vector is appropriate to accept.
- **Do not dig yourself a hole you cannot get out of!**



Step 3: Identify a Target Profile

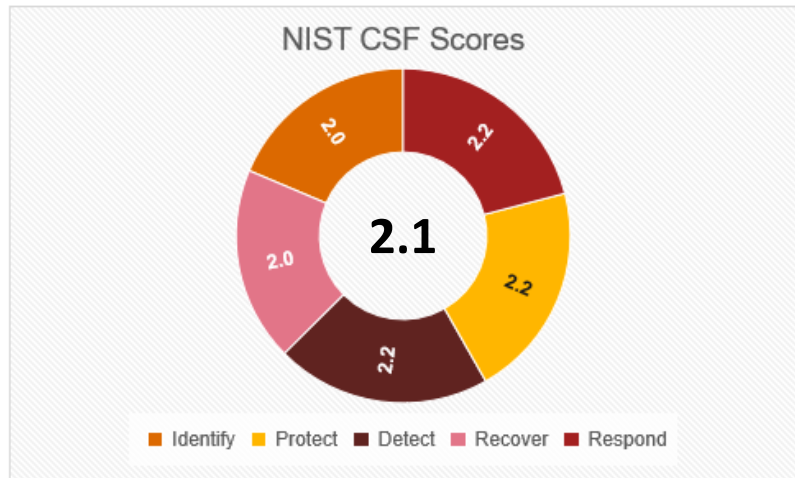
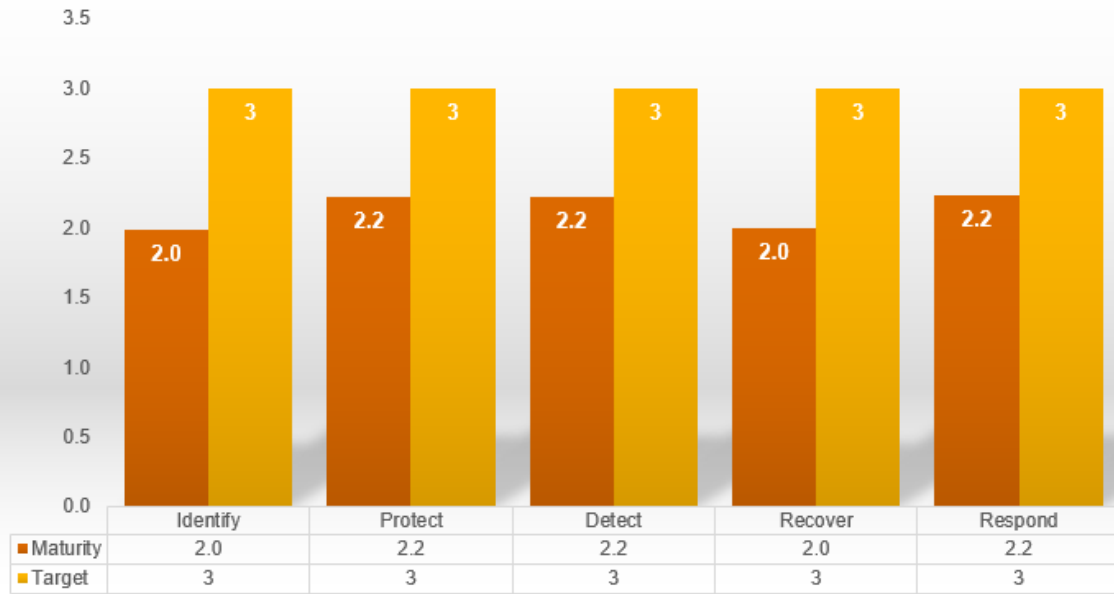


Step 4: Assess and Prioritize Gaps

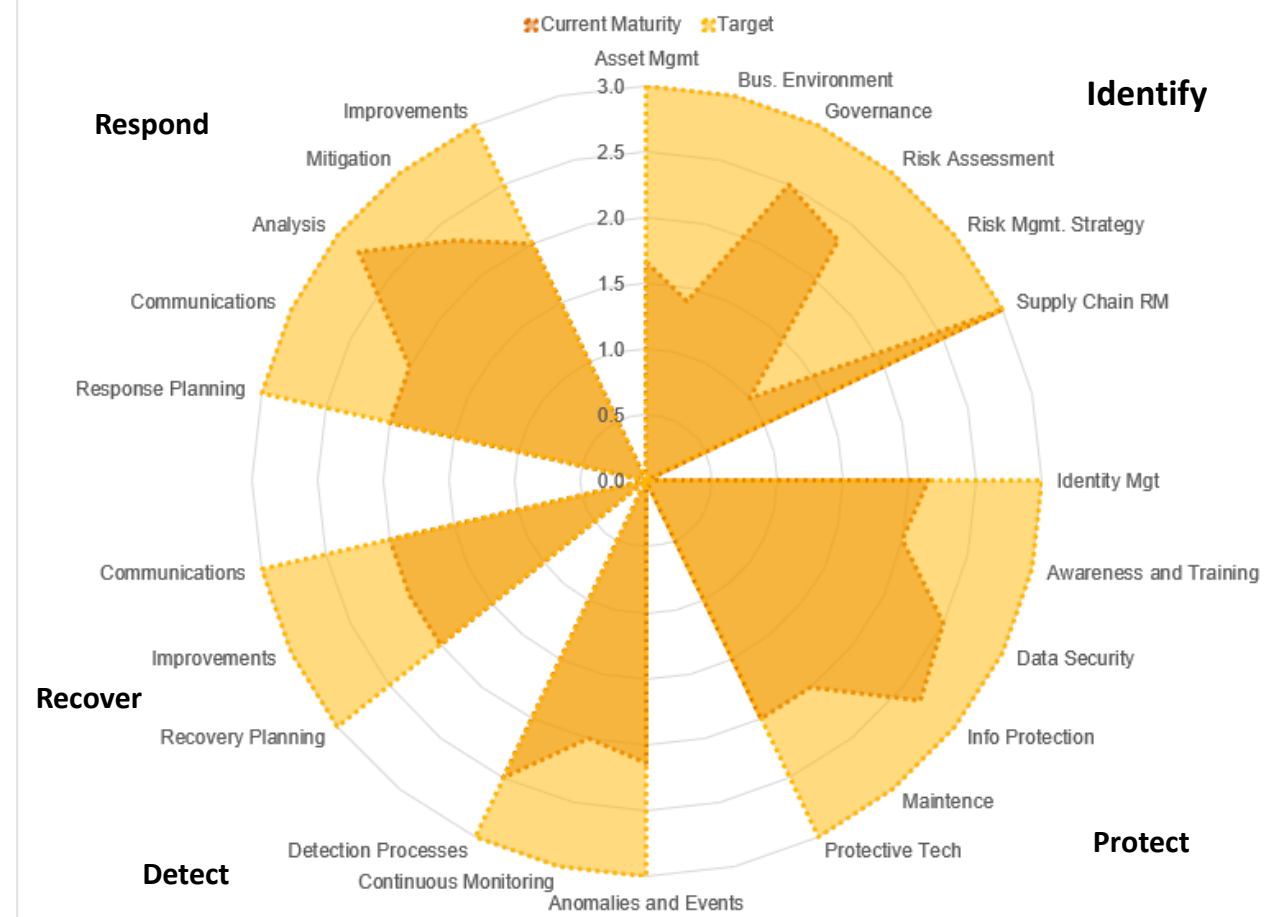
- Determine, analyze and prioritize any gaps that exist, based on the Current and Target Profiles previously enumerated.
- A prioritized action plan should address these gaps and use costs and benefits, risks and mission-driven considerations to achieve the desired Target Profile outcomes.
- The resources needed to address these gaps should be determined as well (FTEs).
 - Insource vs. outsource vs. co-source



Summary CSF Scores



NIST CSF SCORES BREAKDOWN



Factoring Risk into the Equation

- We assess maturity with CSF and not necessarily risk
- However, we should factor risk into our roadmap to assist in prioritizing projects
- Developing an understanding of its risk environment, including how it will be impacted if a threat becomes active and the risk is realized.



Factoring Risk into the Equation

- A common problem with NIST CSF assessments are that they pull a risk team's focus down in to the weeds, then leaves them there, so to speak.
- Organizations really want to know “How much risk do we have?” and “Which of the NIST CSF activities reduces risk the most?” The CSF alone can't answer those questions.
- Identify and quantify your top risks to help prioritize your remediation
- How your maturity corresponds to that risk
- Prioritize investments where the business needs it most
 - Quick wins (low investment/high risk reduction, high investment/high risk reduction, low investment/low risk reduction, high investment/low risk reduction)



Factoring Risk into the Equation

- May be guided by previous risk assessment activities or the organization's overall enterprise risk management program
- Analyze the organization's operational environment to determine the likelihood of cybersecurity events and their related impact.
- This risk assessment should not be narrowly focused on problem areas but also include what is working well too.



Factoring Risk into the Equation

The steps below give a high level overview of an example cybersecurity risk assessment process

1. Identify cyber risks and business impacts

- **Objective:** Identify organizational cyber risks across various business segments and determine potential business impacts associated with each cyber risk
- **Output:** Identified cyber risks and total business impact scores for each risk

2. Determine likelihood

- **Objective:** Evaluate likelihood of cyber risks based on the frequency at which the organization observes threat scenarios
- **Output:** Likelihood scores, inherent risk scores, and inherent risk levels for each identified cyber risk

3. Identify and score cyber controls via NIST CSF

- **Objective:** Evaluate the strength of controls
- **Output:** Control strength scores for identified cyber controls, threat scenarios, and cyber risks

4. Determine residual risk and risk targets

- **Objective:** Compute current residual risk and target residual risk for each identified cyber risk using the business impacts, threat scenario likelihoods, and cyber control strength scores from previous steps
- **Output:** Current and target residual risk scores and levels for identified cyber risks and dashboard graphics to facilitate executive conversations and decision-making



Step 5: Remediation and Roadmap

- After determining which steps need to be taken to address the gaps identified, determine which actions to take and carry out to remediate.
- Cybersecurity practices should then be adjusted to achieve the Target Profile.



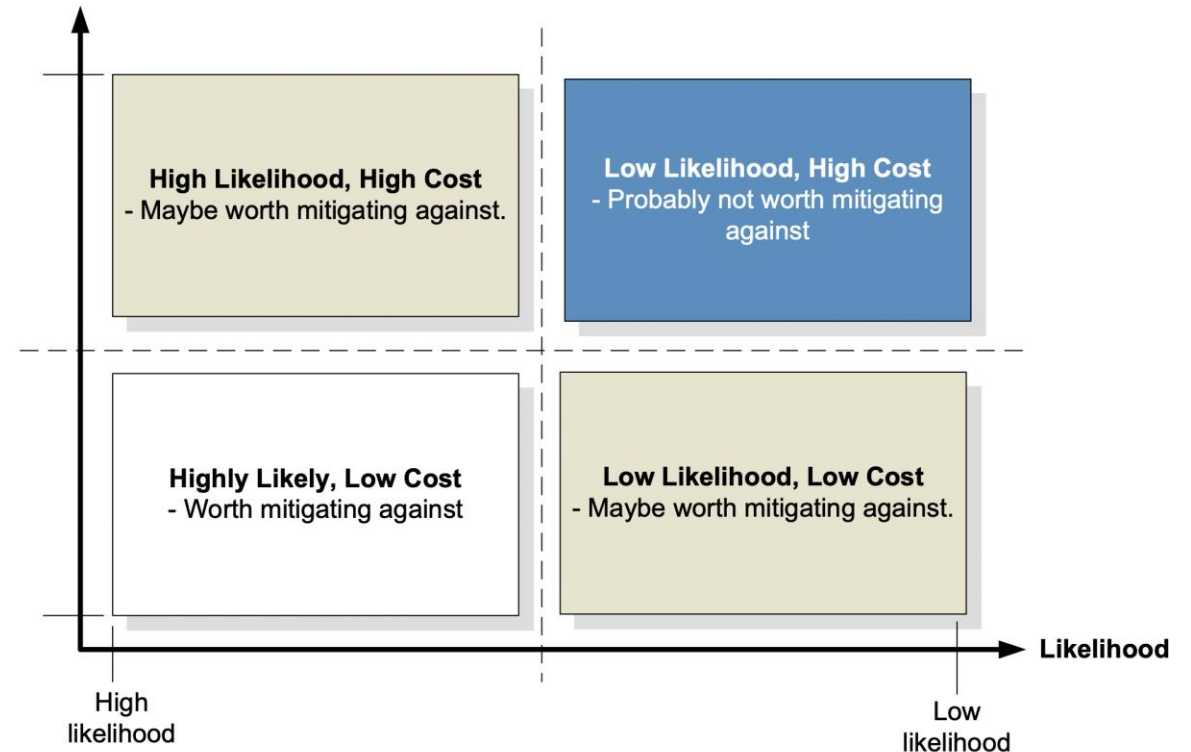
Detection Processes (DE.DP)

Short description	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Subcategories	<p>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</p> <p>DE.DP-2: Detection activities comply with all applicable requirements</p> <p>DE.DP-3: Detection processes are tested</p> <p>DE.DP-4: Event detection information is communicated</p> <p>DE.DP-5: Detection processes are continuously improved</p>
Observations	Recommendations
<p>DE.DP-1: Roles and responsibilities for detection are defined to ensure accountability. Duty Team acts as a Tier 1, notify accountable process owners (developers) who are Tier 2.</p>	<p>Keep roles and responsibilities for Duty team up-to-date. Provide security training activities which would involve coordination across all organizational elements.</p>
<p>DE.DP-2: Duty Team noted that there are no formal procedures which obligate engineers/developers to configure monitoring of service with the Team before deploying service into production. Developer can bypass this process, Therefore Duty Team is not aware of services which should be monitored.</p>	<p>Define, document, implement and communicate procedures describing configuring monitoring of services before deploying into production</p>
<p>DE.DP-3: We have found no evidence whether detection processes are tested on regular basis.</p>	<p>Implement formal procedures which would describe how the organization:</p> <ul style="list-style-type: none"> • Creates a process for ensuring that organizational plans for conducting security testing, monitoring activities and training associated with organizational information systems; • Ensures that detection testing is executed in a timely manner • Reviews detection testing and monitoring plans for consistency with • the organizational risk strategy.
<p>DE.DP-4: Duty Team noted that event detection information is communicated in relevant Jira workflow.</p>	<ul style="list-style-type: none"> • Ensure that event detection information is communicated to defined personnel; • Update list of events which must be detected on regular basis. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal

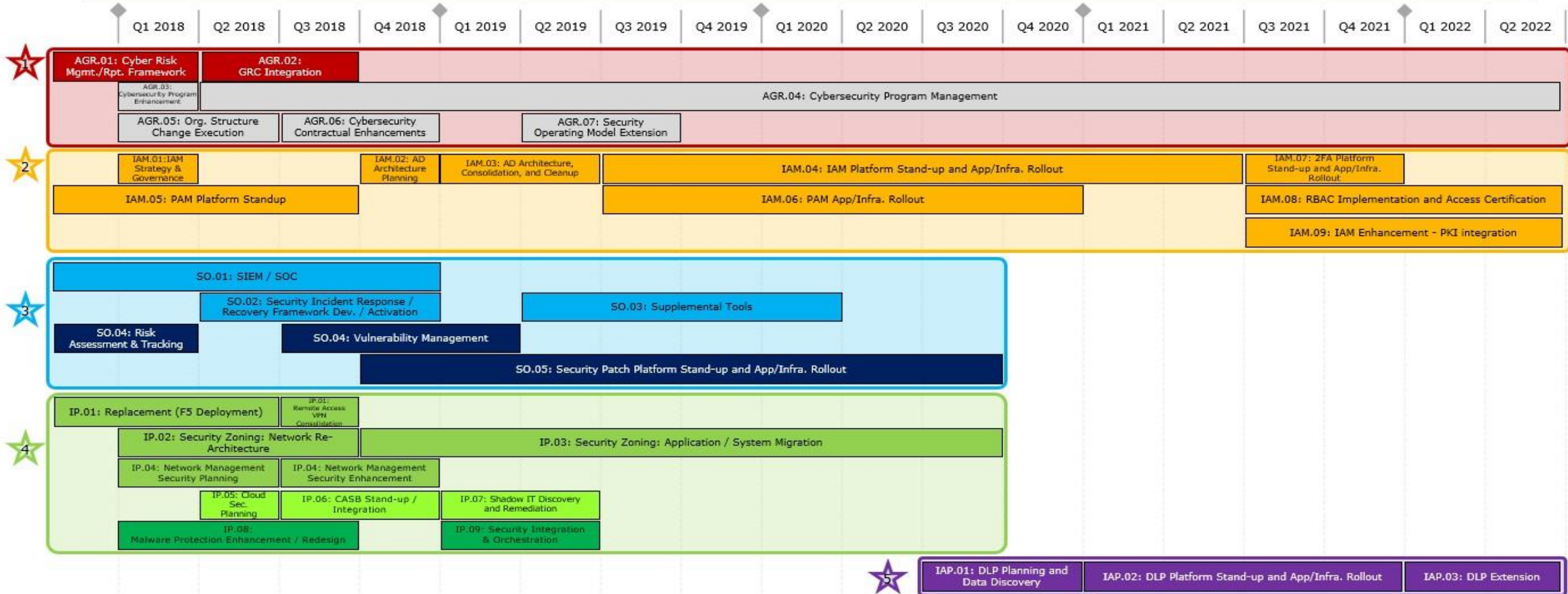


Step 5: Remediation and Roadmap

- Remember governance alone may not be a good indicator (if I document, I am good)
- Low hanging fruit is not always the way to go
- Low maturity does not mean you will be breached



Cybersecurity Roadmap

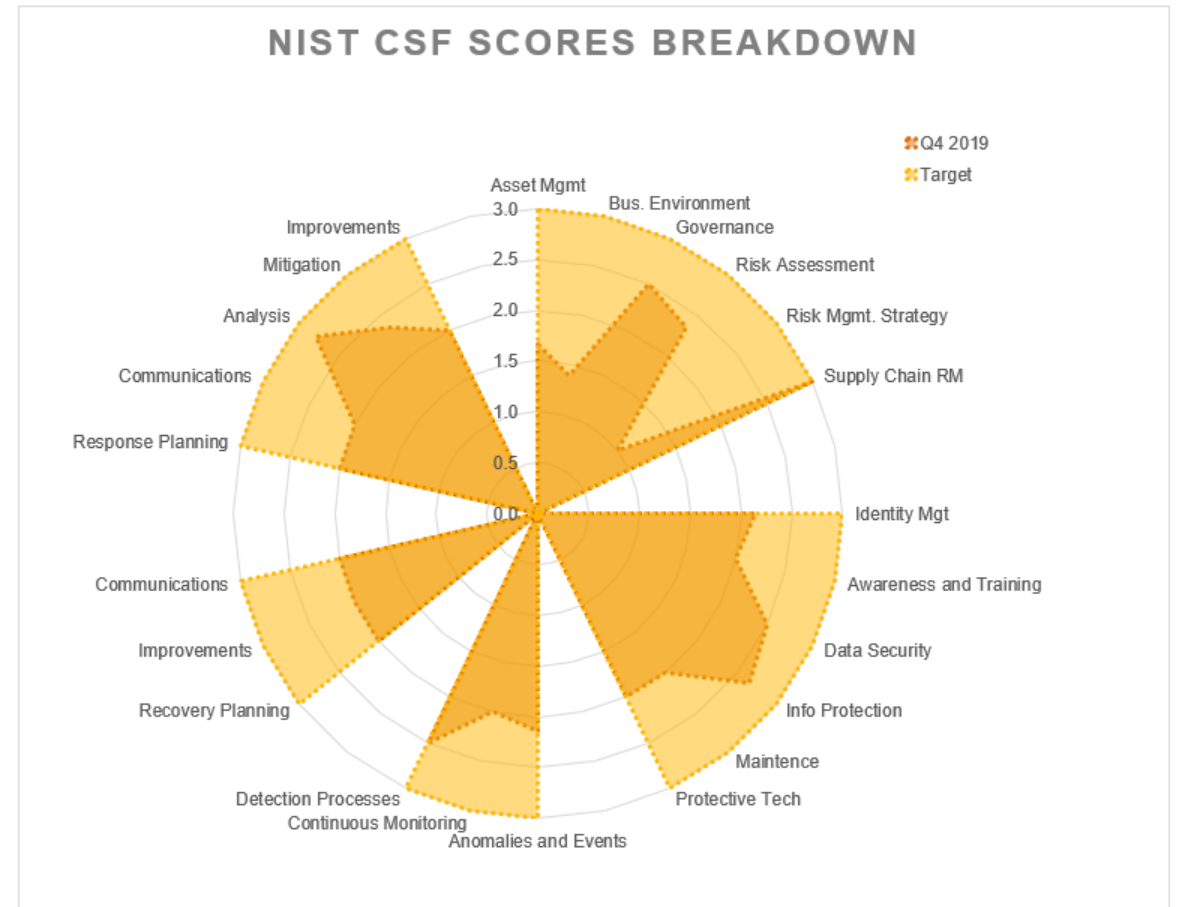


Legend

- Initiative**
 - ★ Architecture, Risk, Governance
 - ★ Identity & Access Management
 - ★ Security Operations
 - ★ Infrastructure Protection
 - ★ Information & Appl. Protection
- Project Bundle**
 - Bundle 1: Architecture / Governance
 - Bundle 2: Risk Management
 - Bundle 3: IAM
 - Bundle 4: SIEM/SOC
 - Bundle 5: Vuln./Patch Management
 - Bundle 6: Network Protection
 - Bundle 7: Cloud Security
 - Bundle 8: Endpoint/Malware Pro.
 - Bundle 9: Data Loss Protection

Keeping up to date...

- Try to evaluate quarterly
- At a minimum, yearly
- Changes to maturity may affect changes to your roadmap
- Remember, adding documentation (governance) may increase scores, but doesn't necessarily reduce risk.



CSF Use Cases

- Healthcare
 - U.S. Department of Health and Human Services completed a mapping of HIPAA to the NIST CSF
 - Under HIPAA, covered entities and business associates must comply with the HIPAA Security Rule to ensure the confidentiality, integrity and availability of protected health information
 - Mapping between the NIST CSF and HIPAA promotes an additional layer of security
 - Assessments performed for certain categories of the NIST CSF may be more specific and detailed than those performed for the corresponding HIPAA requirement.



CSF Use Cases

- Financial Services

- U.S. Financial Services Sector Coordinating Council (FS-SCC) developed a custom version of the NIST CSF that addresses unique aspects of the sector and regulatory requirements
- Financial Services Sector Specific Cybersecurity profile, drafted collaboratively with regulatory agencies, is a means to harmonize cybersecurity-related regulatory requirements.
- For example, the FS-SCC mapped the “Risk Management Strategy” category to nine different regulatory requirements and determined that the language and definitions, while different, largely addressed the same security objective



International Adoption

- Outside of the U.S., many countries have leveraged the NIST CSF for commercial and public sector use.
 - Italy was one of the first international adopters of the NIST CSF and developed a national cybersecurity strategy against the five Functions.
 - In June 2018, the UK aligned its Minimum Cyber Security Standard, mandatory for all government departments to the five Functions.
 - Israel and Japan localized the NIST CSF into their respective languages with Israel



International Adoption

- Outside of the U.S., many countries have leveraged the NIST CSF for commercial and public sector use.
 - Uruguay performed a mapping of the CSF to ISO standards to strengthen connections to international frameworks.
 - Switzerland, Scotland, Ireland, and Bermuda are also among the list of countries that are using the NIST CSF to improve cybersecurity and resiliency across their public and commercial sector organizations.



In Closing

- Form a team (e.g., a security governance process)
- Get the buy in from your executive
- Important components
 - Scope statement (remember asset classes)
 - “Crown jewels” inventory (systems, suppliers, assets)
 - Risk assessment (likelihood/impact of named risks)
- Don't get too bogged down by scores
 - Documentation will improve scores, but not necessary security
 - If I do this, how does it affect my score?

Conclusion



Peter Morin

petermorin123@gmail.com

Twitter: @PeterMorin123

<http://www.petermorin.com>



@PeterMorin123