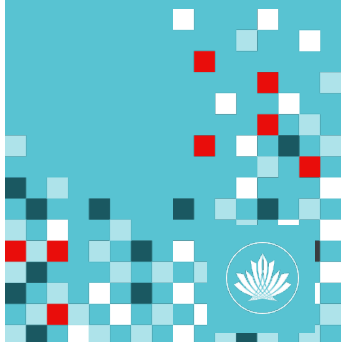
My girl friend thinks I don’t give her enough privacy ……..

…… At least that's what she writes in her diary



canarie

What you need to know about the NIST CSF

Jeff Gardiner, pMBA, BSc, BA, CISSP, CD | Compute Canada

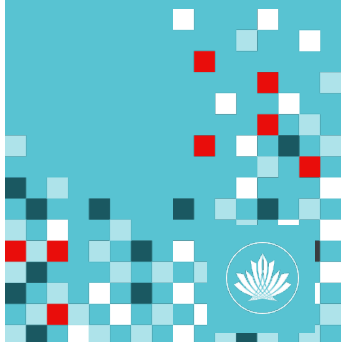
April 29, 2021

Event


© MARK ANDERSON, WWW.ANDERTOONS.COM
APPLESAUCE!
NO, WAIT...
ANDERSON

Recognizing the problem

- Technology Problem
- Process Problem
- Privacy Problem
- Threat Awareness Problem
- Security Control Problem
- Information Security Problem



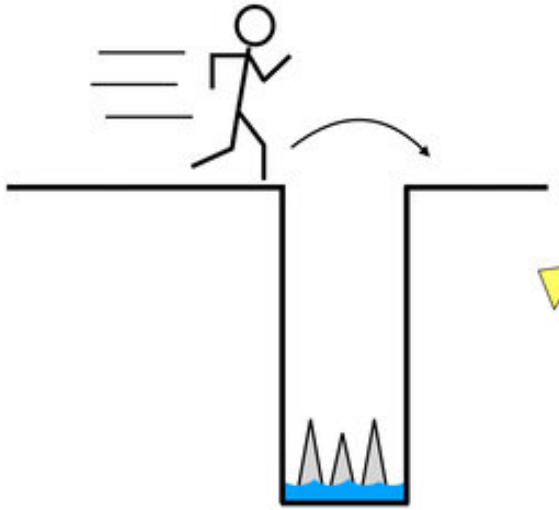
What problem does cybersecurity solve?


Orchidée
PARIS
SHOES
S.P.A

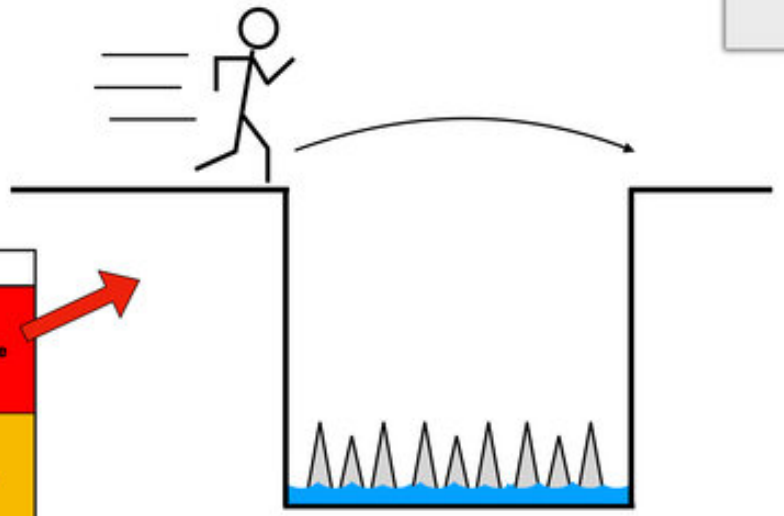
RISK = LIKELIHOOD x IMPACT

Assessment of Risk Exposure = Risk Probability x Impact

(Severity = Likelihood x Consequence)

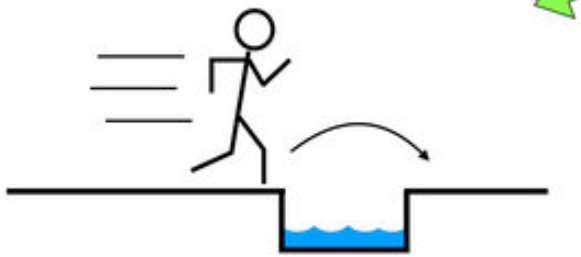


Low Probability & High Impact

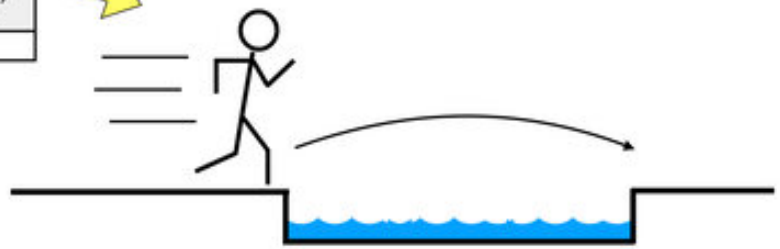


High Probability & High Impact

Risk Assessment Matrix				
Impact of Risk (Consequence)	Major Impact	Medium	High	Extreme
	Moderate Impact	Medium	Medium	High
	Minor Impact	Low	Medium	Medium
Risk Exposure = Impact x Probability		Unlikely (0-33%)	Moderately Likely (33%-66%)	Very Likely (66%+)
		Probability of Risk (Likelihood)		

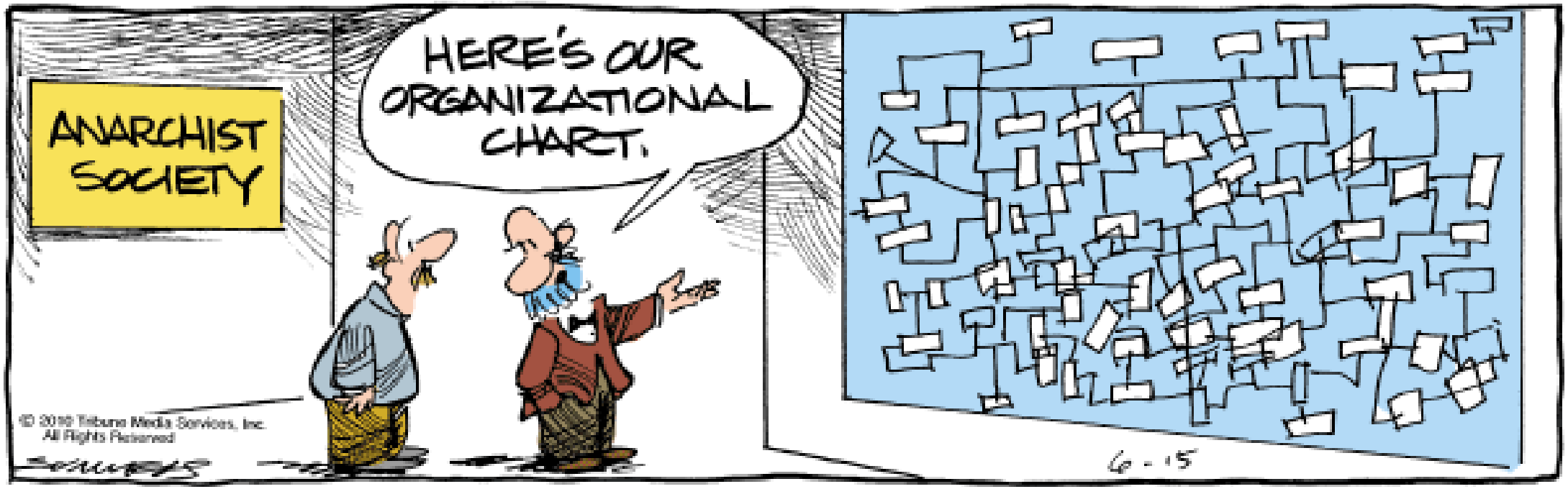


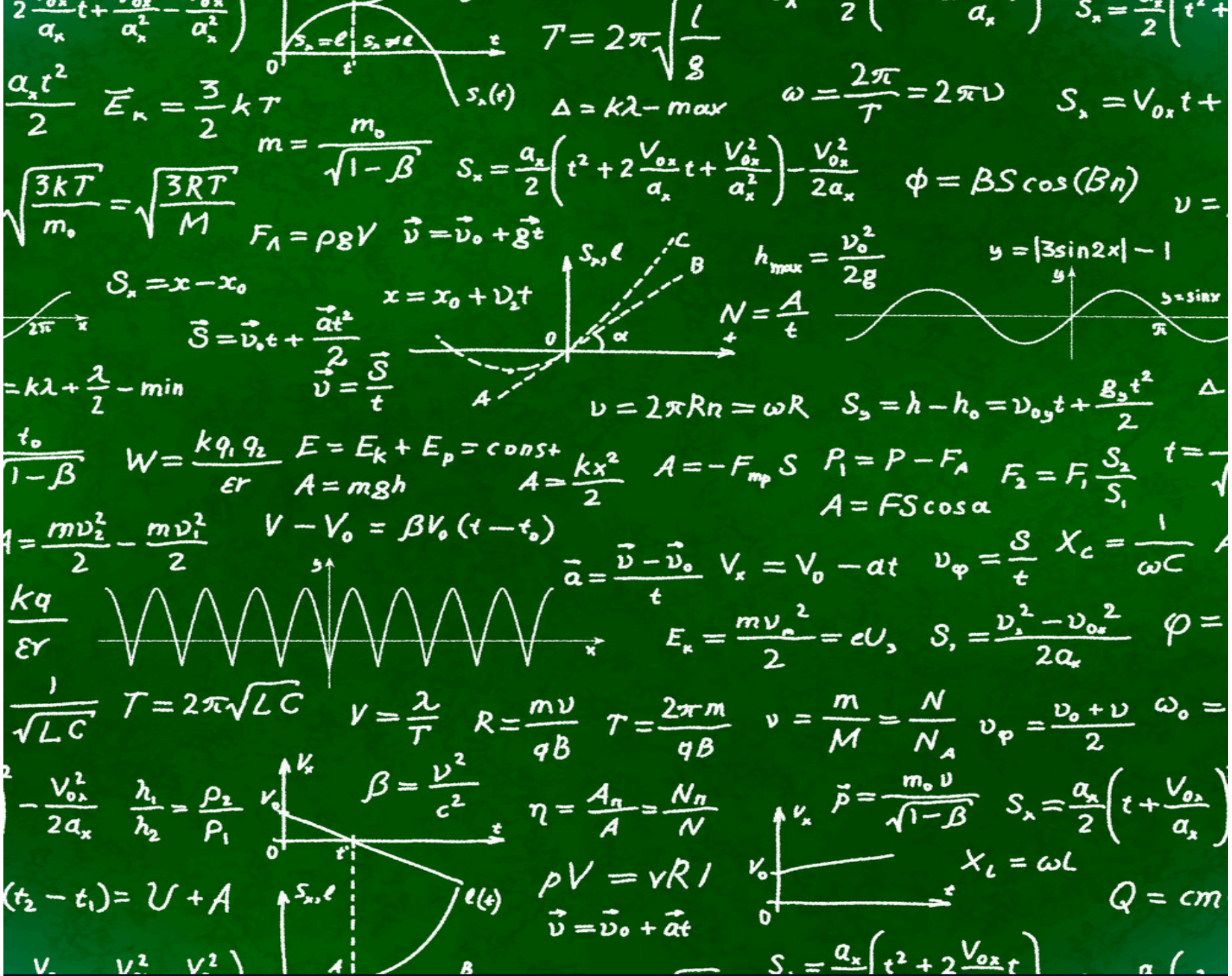
Low Probability & Low Impact



High Probability & Low Impact

Why is cybersecurity necessary?


ANARCHIST SOCIETY
HERE'S OUR ORGANIZATIONAL CHART.
© 2016 Tribune Media Services, Inc.
All Rights Reserved.
6-15


$T = 2\pi\sqrt{\frac{l}{g}}$
$\frac{a_x t^2}{2}$
$\vec{E}_к = \frac{3}{2}kT$
$m = \frac{m_0}{\sqrt{1-\beta}}$
$\Delta = k\lambda - max$
$\omega = \frac{2\pi}{T} = 2\pi\upsilon$
$S_x = V_{0x}t +$
$\sqrt{\frac{3kT}{m_0}} = \sqrt{\frac{3RT}{M}}$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t + \frac{V_{0x}^2}{a_x^2}\right) - \frac{V_{0x}^2}{2a_x}$
$\phi = BS\cos(Bn)$
$F_A = \rho g V$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{g}t$
$h_{max} = \frac{\upsilon_0^2}{2g}$
$y = |3\sin 2x| - 1$
$S_x = x - x_0$
$x = x_0 + \upsilon_x t$
$N = \frac{A}{t}$
$\vec{S} = \vec{\upsilon}_0 t + \frac{\vec{a}t^2}{2}$
$\vec{\upsilon} = \frac{\vec{S}}{t}$
$= k\lambda + \frac{\lambda}{2} - min$
$\upsilon = 2\pi Rn = \omega R$
$S_y = h - h_0 = \upsilon_{0y}t + \frac{g_y t^2}{2}$
$\frac{t_0}{\sqrt{1-\beta}}$
$W = \frac{kq_1q_2}{\varepsilon r}$
$E = E_k + E_p = const$
$A = mgh$
$A = \frac{kx^2}{2}$
$A = -F_{mp}S$
$P_1 = P - F_A$
$F_2 = F_1\frac{S_2}{S_1}$
$A = FS\cos\alpha$
$= \frac{m\upsilon_2^2}{2} - \frac{m\upsilon_1^2}{2}$
$V - V_0 = \beta V_0(t - t_0)$
$\vec{a} = \frac{\vec{\upsilon} - \vec{\upsilon}_0}{t}$
$V_x = V_0 - at$
$\upsilon_\varphi = \frac{S}{t}$
$X_C = \frac{1}{\omega C}$
$\frac{kq}{\varepsilon r}$
$E_к = \frac{m\upsilon_e^2}{2} = eU_з$
$S_1 = \frac{\upsilon_x^2 - \upsilon_{0x}^2}{2a_x}$
$\varphi =$
$\frac{1}{\sqrt{LC}}$
$T = 2\pi\sqrt{LC}$
$V = \frac{\lambda}{T}$
$R = \frac{m\upsilon}{qB}$
$T = \frac{2\pi m}{qB}$
$\upsilon = \frac{m}{M} = \frac{N}{N_A}$
$\upsilon_p = \frac{\upsilon_0 + \upsilon}{2}$
$\omega_0 =$
$\frac{V_{0x}^2}{2a_x}$
$\frac{h_1}{h_2} = \frac{\rho_2}{\rho_1}$
$\beta = \frac{\upsilon^2}{c^2}$
$\eta = \frac{A_n}{A} = \frac{N_n}{N}$
$\vec{p} = \frac{m_0\upsilon}{\sqrt{1-\beta}}$
$S_x = \frac{a_x}{2}\left(t + \frac{V_{0x}}{a_x}\right)$
$X_L = \omega L$
$(t_2 - t_1) = U + A$
$pV = \nu RT$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{a}t$
$Q = cm$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t\right)$

What is NIST?

- The **National Institute of Standards and Technology** (**NIST**) is a US based non-regulatory agency

- In Existence since 1901 (formerly *National Bureau of Standards*)

- Information Security and Privacy Advisory Board

- Publishes Standards & Frameworks

Who uses NIST Frameworks?

- US Government
- 50% of American Businesses
- Canadian Government - ITSG-33: Risk Management (based upon NIST 800-53 Rev 4)
- Recommended by Cdn Government for public sector

https://cyber.gc.ca/en/path-enterprise-security

- Canarie & many Canadian universities

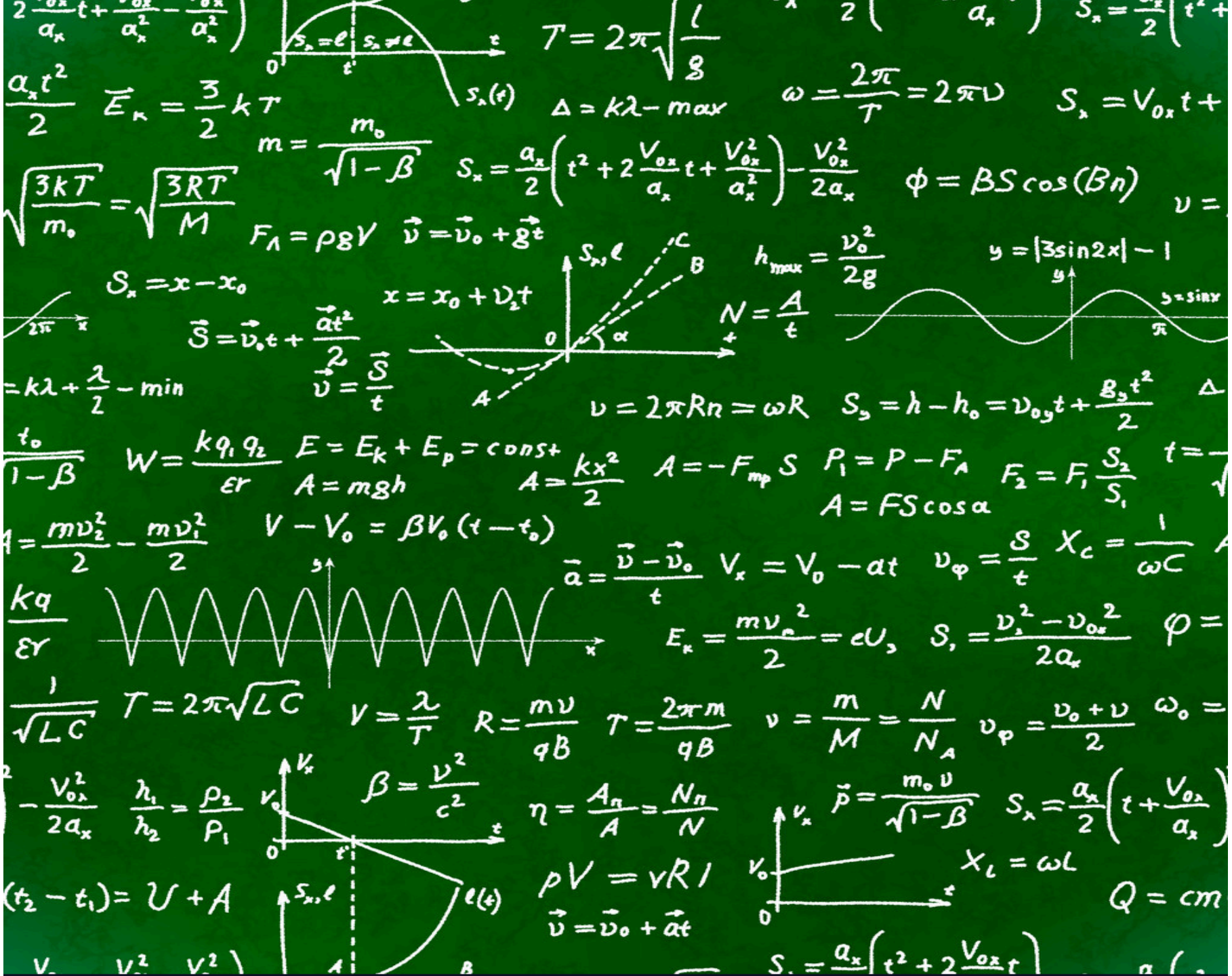
The Framework for Improving Critical Infrastructure Cybersecurity

Ver 1.1

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

cyberframework@nist.gov


$T = 2\pi\sqrt{\frac{l}{g}}$
$\frac{a_x t^2}{2}$
$\vec{E}_к = \frac{3}{2}kT$
$m = \frac{m_0}{\sqrt{1-\beta}}$
$\Delta = k\lambda - max$
$\omega = \frac{2\pi}{T} = 2\pi\upsilon$
$S_x = V_{0x}t +$
$\sqrt{\frac{3kT}{m_0}} = \sqrt{\frac{3RT}{M}}$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t + \frac{V_{0x}^2}{a_x^2}\right) - \frac{V_{0x}^2}{2a_x}$
$\phi = BS\cos(Bn)$
$F_A = \rho g V$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{g}t$
$h_{max} = \frac{\upsilon_0^2}{2g}$
$y = |3\sin 2x| - 1$
$S_x = x - x_0$
$x = x_0 + \upsilon_x t$
$N = \frac{A}{t}$
$\vec{S} = \vec{\upsilon}_0 t + \frac{\vec{a}t^2}{2}$
$\vec{\upsilon} = \frac{\vec{S}}{t}$
$= k\lambda + \frac{\lambda}{2} - min$
$\upsilon = 2\pi Rn = \omega R$
$S_y = h - h_0 = \upsilon_{0y}t + \frac{g_y t^2}{2}$
$\frac{t_0}{\sqrt{1-\beta}}$
$W = \frac{kq_1q_2}{\varepsilon r}$
$E = E_k + E_p = const$
$A = mgh$
$A = \frac{kx^2}{2}$
$A = -F_{mp}S$
$P_1 = P - F_A$
$F_2 = F_1\frac{S_2}{S_1}$
$A = FS\cos\alpha$
$= \frac{m\upsilon_2^2}{2} - \frac{m\upsilon_1^2}{2}$
$V - V_0 = \beta V_0(t - t_0)$
$\vec{a} = \frac{\vec{\upsilon} - \vec{\upsilon}_0}{t}$
$V_x = V_0 - at$
$\upsilon_\varphi = \frac{S}{t}$
$X_C = \frac{1}{\omega C}$
$\frac{kq}{\varepsilon r}$
$E_к = \frac{m\upsilon_e^2}{2} = eU_з$
$S_1 = \frac{\upsilon_x^2 - \upsilon_{0x}^2}{2a_x}$
$\varphi =$
$\frac{1}{\sqrt{LC}}$
$T = 2\pi\sqrt{LC}$
$V = \frac{\lambda}{T}$
$R = \frac{m\upsilon}{qB}$
$T = \frac{2\pi m}{qB}$
$\upsilon = \frac{m}{M} = \frac{N}{N_A}$
$\upsilon_p = \frac{\upsilon_0 + \upsilon}{2}$
$\omega_0 =$
$\frac{V_{0x}^2}{2a_x}$
$\frac{h_1}{h_2} = \frac{\rho_2}{\rho_1}$
$\beta = \frac{\upsilon^2}{c^2}$
$\eta = \frac{A_n}{A} = \frac{N_n}{N}$
$\vec{p} = \frac{m_0\upsilon}{\sqrt{1-\beta}}$
$S_x = \frac{a_x}{2}\left(t + \frac{V_{0x}}{a_x}\right)$
$X_L = \omega L$
$(t_2 - t_1) = U + A$
$pV = \nu RT$
$\vec{\upsilon} = \vec{\upsilon}_0 + \vec{a}t$
$Q = cm$
$S_x = \frac{a_x}{2}\left(t^2 + 2\frac{V_{0x}}{a_x}t\right)$

Key Framework Attributes

Principles of the Current and Future Versions of Framework

Common and accessible language

- Understandable by many professionals

It's adaptable to many **technologies**[1.1], **lifecycle phases**[1.1], sectors and uses

- Meant to be *customized*

It's risk-based

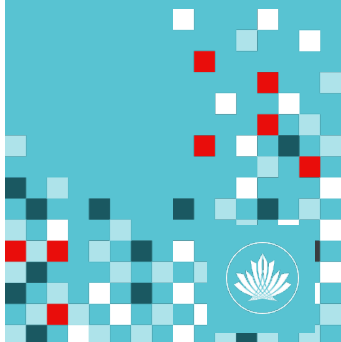
- A Catalog of cybersecurity outcomes
- Does not provide *how* or *how much* cybersecurity is appropriate

It's meant to be paired

- Take advantage of great pre-existing things

It's a living document

- Enable best practices to become *standard practices for everyone*
- Can be updated as *technology and threats* change
- Evolves *faster* than regulation and legislation
- Can be updated as stakeholders *learn from implementation*



Cybersecurity Framework Components

Cybersecurity outcomes and informative references

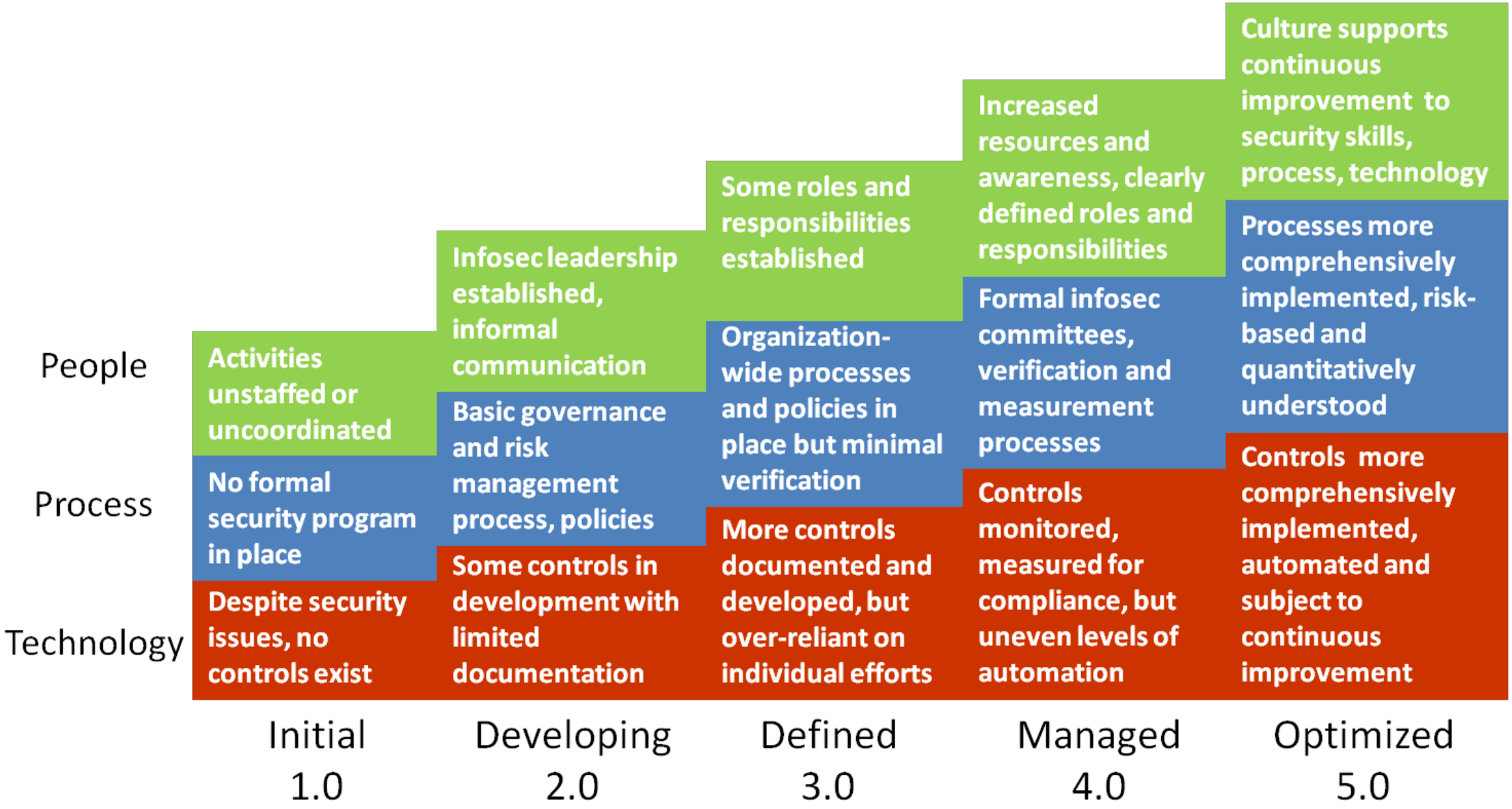
Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Aligns industry standards and best practices to the Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs

IMPLIMENTATION TIERS

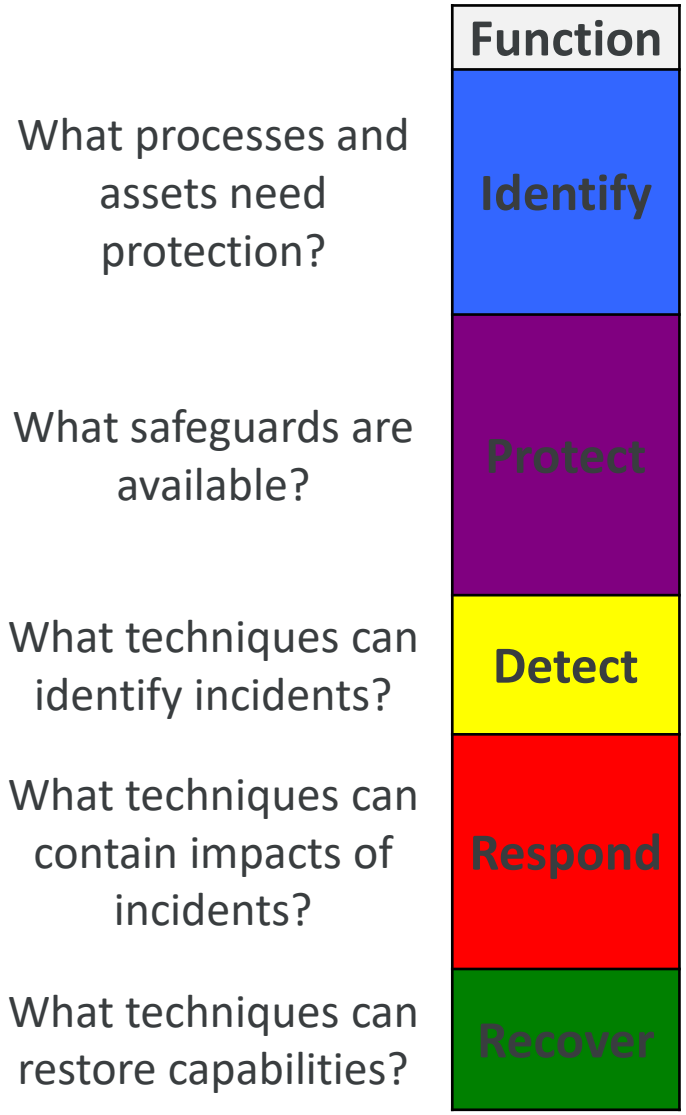
Cybersecurity Maturity Model



THE FIVE FUNCTIONS OF THE NIST CYBERSECURITY FRAMEWORK

Core

A Catalog of Cybersecurity Outcomes



- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Core

A Catalog of Cybersecurity Outcomes

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management[1.1]
Protect	**Identity Management, Authentication and Access Control**[1.1]
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Core – Example[1.1]

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Core – Example[1.1]

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Core – Example

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Component	Version 1.1	Comments
Functions	5	
Categories	23	• Added a new category in ID.SC – Supply Chain
Subcategories	108	• Added 5 subcategories in ID.SC • Added 2 subcategories in PR.AC • Added 1 subcategory each to PR.DS, PR.PT, RS.AN • Clarified language in 7 others
Informative References	5	

Profile

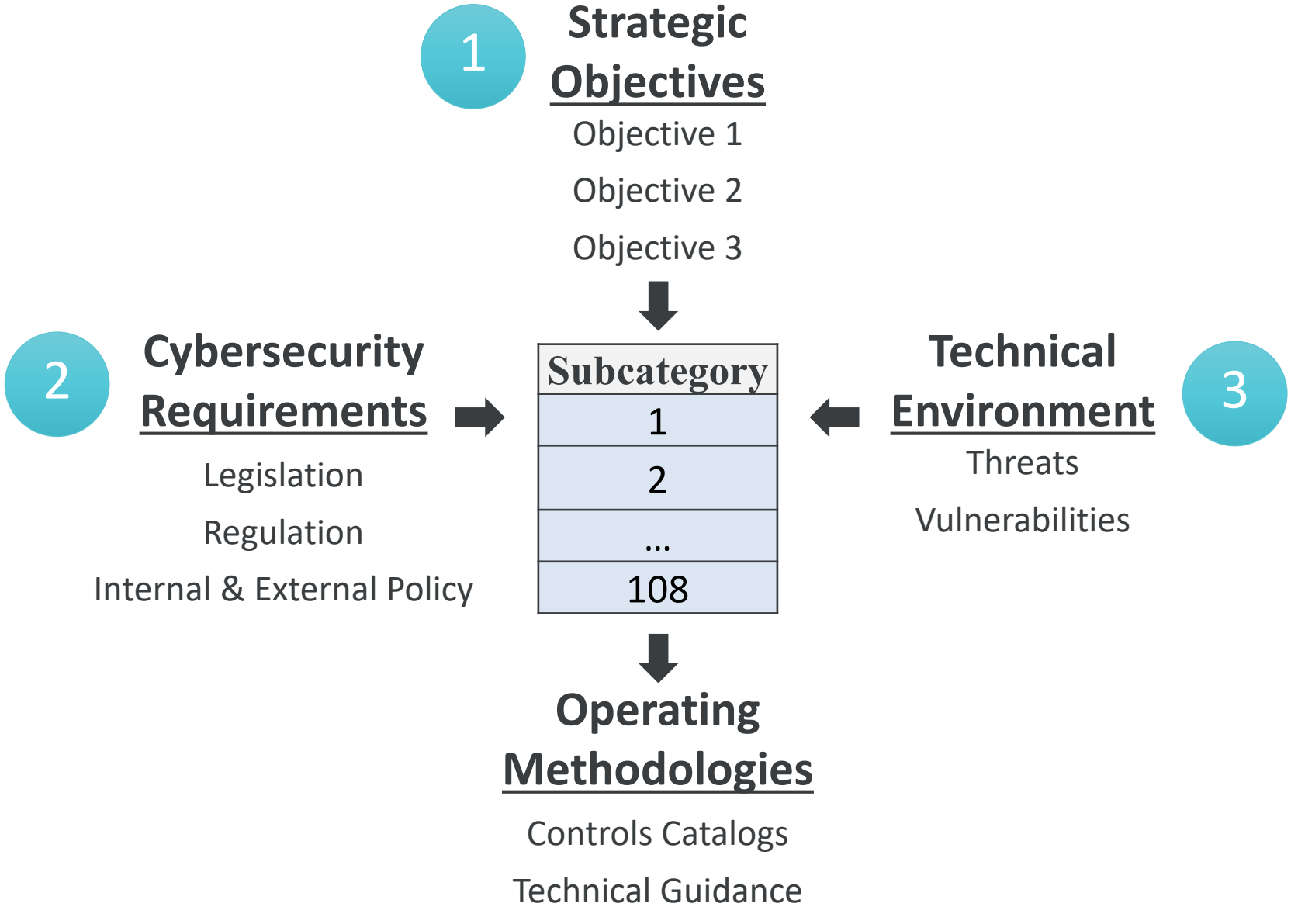
Customizing Cybersecurity Framework

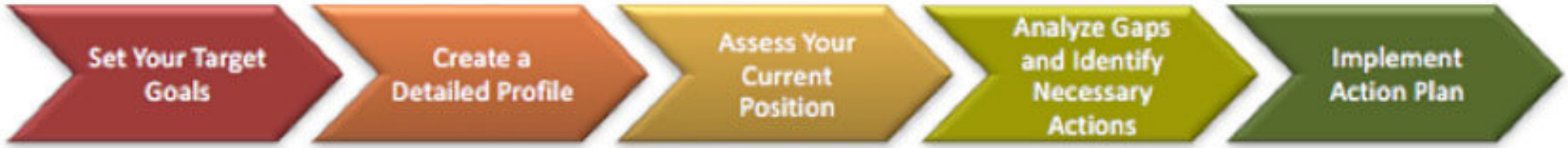
Ways to think about a Profile:

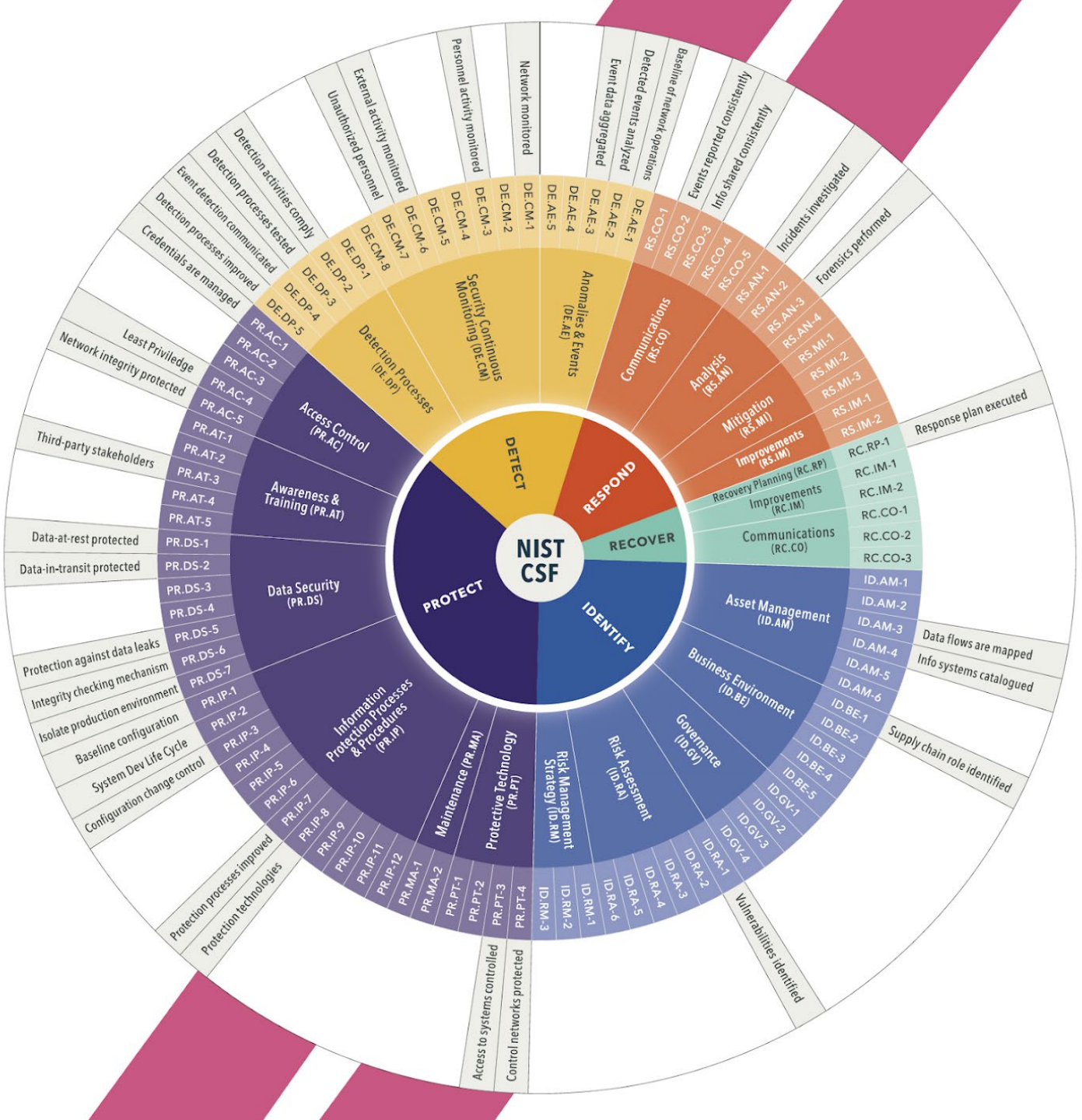
- A customization of the Core for a given sector, subsector, or organization
- A fusion of mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity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

Profile Foundational Information

A Profile Can be Created from Three Types of Information



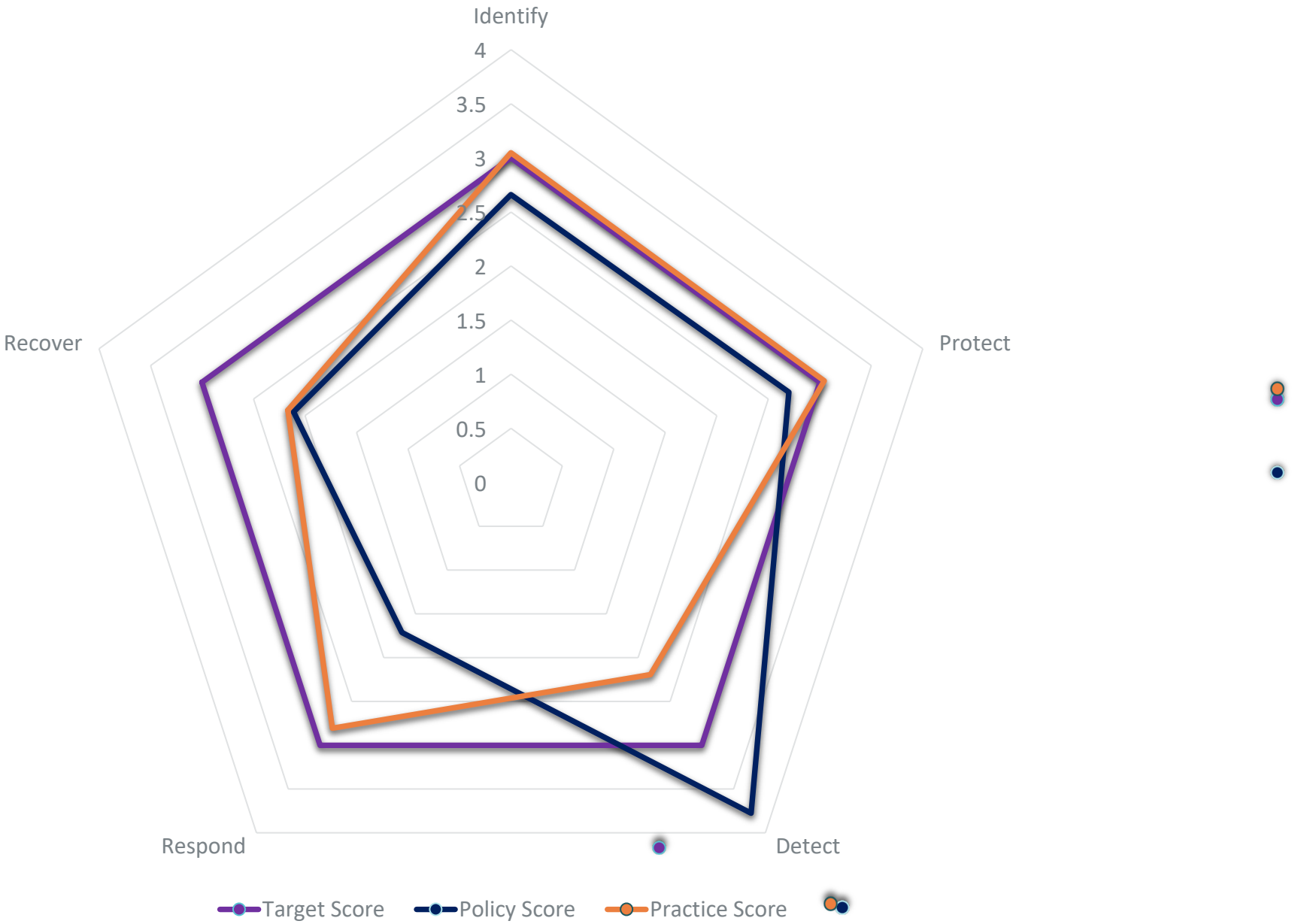

Set Your Target Goals
Create a Detailed Profile
Assess Your Current Position
Analyze Gaps and Identify Necessary Actions
Implement Action Plan


NIST CSF
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Asset Management (ID.AM)
Business Environment (ID.BE)
Governance (ID.GV)
Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM)
Access Control (PR.AC)
Awareness & Training (PR.AT)
Data Security (PR.DS)
Information Protection Processes & Procedures (PR.IP)
Maintenance (PR.MA)
Protective Technology (PR.PT)
Anomalies & Events (DE.AE)
Security Continuous Monitoring (DE.CM)
Detection Processes (DE.DP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
Recovery Planning (RC.RP)
Improvements (RC.IM)
Communications (RC.CO)
ID.AM-1
ID.AM-2
ID.AM-3
ID.AM-4
ID.AM-5
ID.AM-6
ID.BE-1
ID.BE-2
ID.BE-3
ID.BE-4
ID.BE-5
ID.GV-1
ID.GV-2
ID.GV-3
ID.GV-4
ID.RA-1
ID.RA-2
ID.RA-3
ID.RA-4
ID.RA-5
ID.RA-6
ID.RM-1
ID.RM-2
ID.RM-3
PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AT-1
PR.AT-2
PR.AT-3
PR.AT-4
PR.AT-5
PR.DS-1
PR.DS-2
PR.DS-3
PR.DS-4
PR.DS-5
PR.DS-6
PR.DS-7
PR.IP-1
PR.IP-2
PR.IP-3
PR.IP-4
PR.IP-5
PR.IP-6
PR.IP-7
PR.IP-8
PR.IP-9
PR.IP-10
PR.IP-11
PR.IP-12
PR.MA-1
PR.MA-2
PR.PT-1
PR.PT-2
PR.PT-3
PR.PT-4
DE.AE-1
DE.AE-2
DE.AE-3
DE.AE-4
DE.AE-5
DE.CM-1
DE.CM-2
DE.CM-3
DE.CM-4
DE.CM-5
DE.CM-6
DE.CM-7
DE.CM-8
DE.DP-1
DE.DP-2
DE.DP-3
DE.DP-4
DE.DP-5
RS.CO-1
RS.CO-2
RS.CO-3
RS.CO-4
RS.CO-5
RS.AN-1
RS.AN-2
RS.AN-3
RS.AN-4
RS.MI-1
RS.MI-2
RS.MI-3
RS.IM-1
RS.IM-2
RC.RP-1
RC.IM-1
RC.IM-2
RC.CO-1
RC.CO-2
RC.CO-3
Data flows are mapped
Info systems catalogued
Supply chain role identified
Vulnerabilities identified
Access to systems controlled
Control networks protected
Protection processes improved
Protection technologies
Configuration change control
System Dev Life Cycle
Baseline configuration
Isolate production environment
Integrity checking mechanism
Protection against data leaks
Data-in-transit protected
Data-at-rest protected
Third-party stakeholders
Network integrity protected
Least Priviledge
Credentials are managed
Detection processes improved
Event detection communicated
Detection processes tested
Detection activities comply
Unauthorized personnel
External activity monitored
Personnel activity monitored
Network monitored
Event data aggregated
Detected events analyzed
Baseline of network operations
Events reported consistently
Info shared consistently
Incidents investigated
Forensics performed
Response plan executed

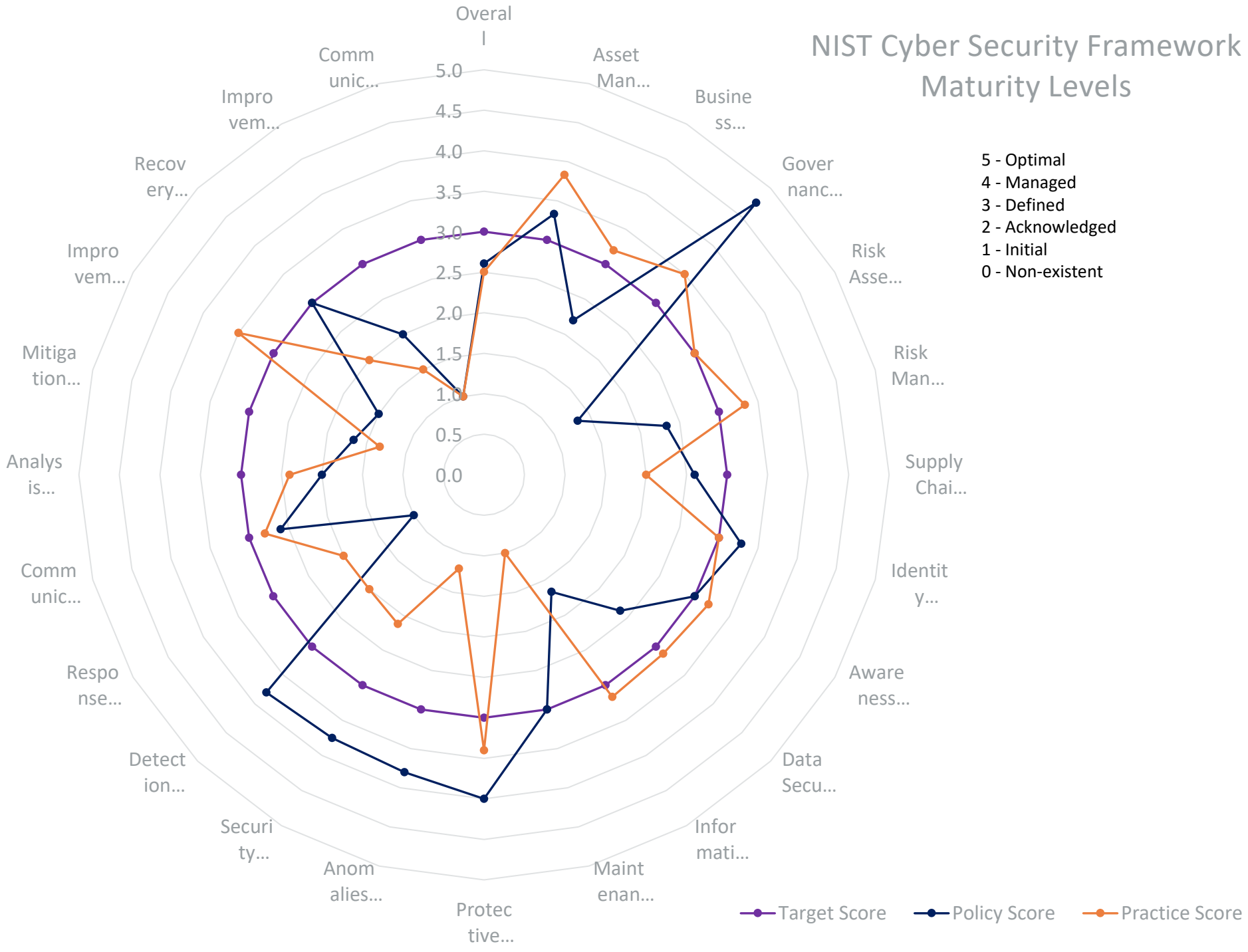
An Example: NIST in action

If you can't measure it – you can't manage it – Peter Drucker

NIST Cybersecurity Framework: Strategic or High Level Goals



NIST Cyber Security Framework Maturity Levels

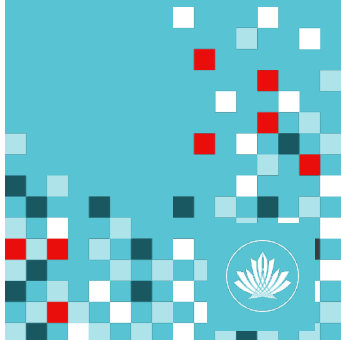


Standard? – Framework?

If you can’t measure it – you can’t manage it – Peter Drucker

Standards

CIS CSC – **Control Standard (Sans Top 20)**
COBIT 5 - **Control Objectives for Information and Related Technology (ISACA)**
ISA 62443-2-1:2009 - **Security for Industrial Automation and Control Systems**
ISO/IEC 27001:2013 – **Information Security Management Standard from ISO**
NIST 800-53 Rev 4 – **Security & Privacy Controls**

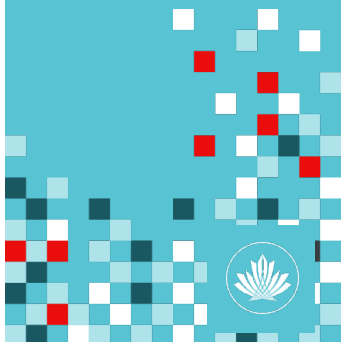


Standards

Compliance to a standard is a tool used to assess/validate an organizations cybersecurity regimen

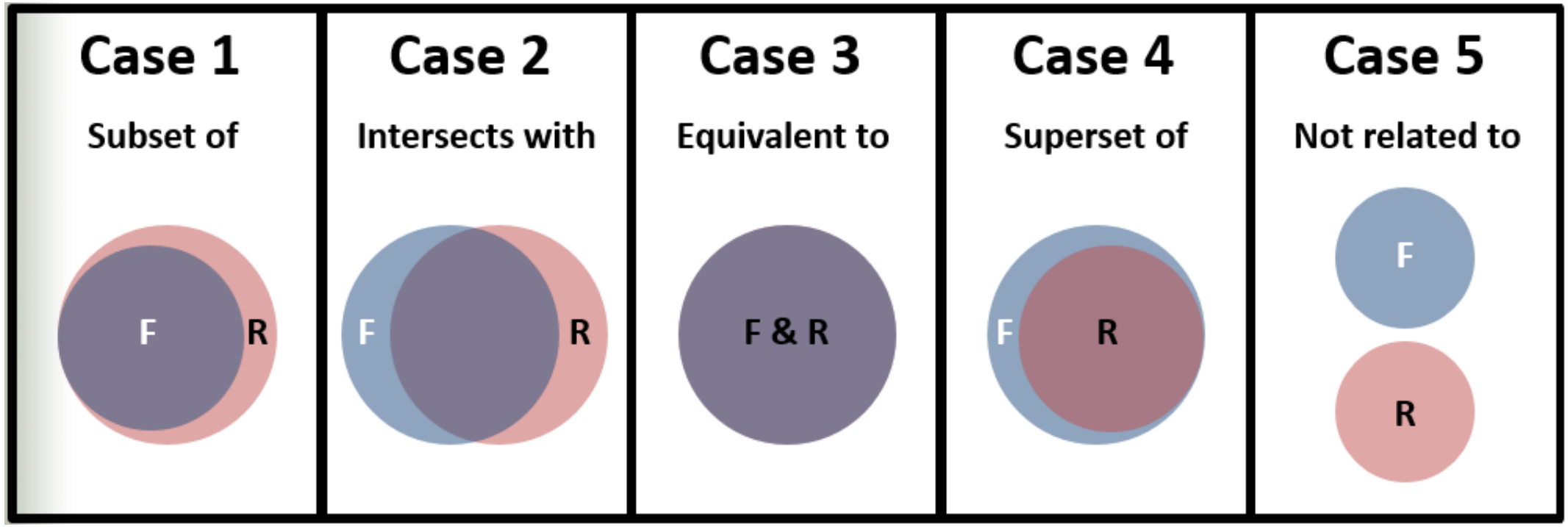
Frameworks

Framework is a tool that allows an organization to focus on outcomes



Relationship Types

Online Informative References



Key

Framework – blue

Reference Document - red

*The **NIST Cybersecurity Framework** is a voluntary framework issued by the US Department of Commerce which represents a collaborative effort between the public and private sectors and academia to improve management of cybersecurity risk.*


A
Q

canarie

canarie.ca | @canarie_inc

jeff.gardiner@computecanada.ca

Webinar Recording Policy

This webinar will be recorded and archived, including all audio. The video will be archived on the CANARIE YouTube channel and may be promoted through CANARIE communication channels.

Any text questions or comments, if responded to, will remain anonymous and not be part of the recording.

The recorded video will include your voice, if audio participation is enabled.

Politique concernant l'enregistrement des webinaires

Ce webinaire sera enregistré et archivé, y compris tout le matériel audio. La vidéo sera conservée sur le canal YouTube de CANARIE et pourra être promue au moyen des filières de communication de CANARIE.

Si on y répond, les questions écrites et orales demeureront anonymes et ne feront pas partie de l'enregistrement.

Toutefois, si la fonction « participation audio » a été activée, le fichier vidéo inclura votre voix.