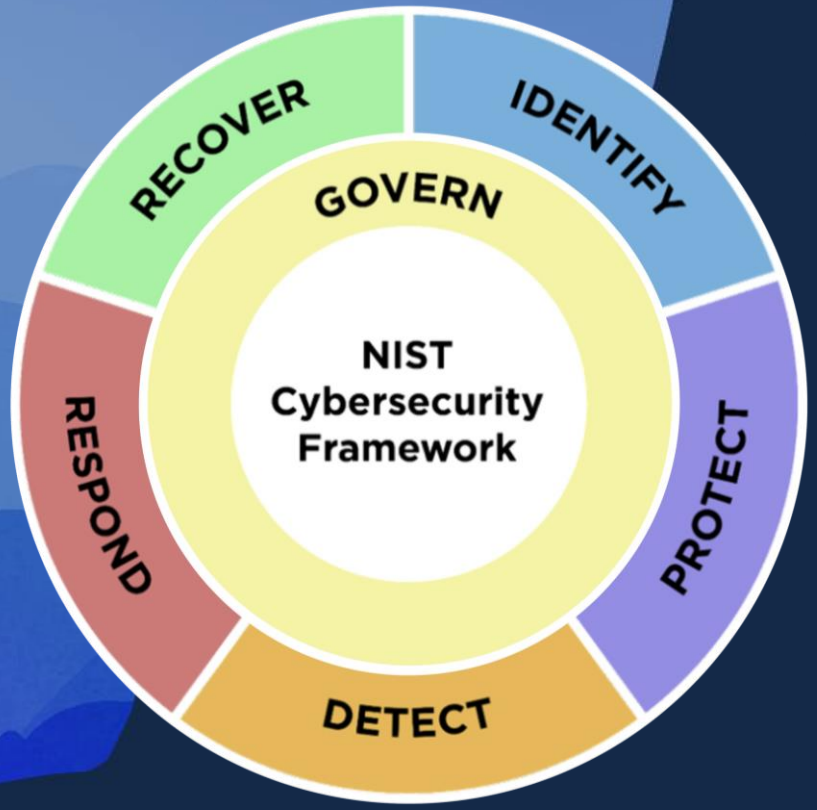
Deep Dive into the NIST Cybersecurity Framework 2.0

Kelly Hood & Tom Conkle

OPTIC CYBER SOLUTIONS



September 2024

Deep Dive into the NIST CSF 2.0

- Explore the latest updates
- Dive into practical application of the CSF
- Use interactive examples to showcase the CSF's flexibility
- Dig into each Function highlighting key Categories and their significance in managing cybersecurity risk
- Provide actionable insights on integrating the CSF into your operations
- Enhance your cybersecurity posture and resilience!

InfoSec World Workshop Handouts

https://www.opticcyber.com/resources/CSF2Handouts.html

Kelly Hood

Cybersecurity Engineer

Optic Cyber Solutions

Tom Conkle

Cybersecurity Engineer

Optic Cyber Solutions

Introductions

- Name
- Role
- Company / Industry

- Why are you here?
- What are you looking to get out of this session?

OUR AGENDA FOR THE DAY

Start	Topic
9:00 AM	Introductions
9:15 AM	CSF Overview
9:55 AM	CSF Profile Development Steps
10:15 AM	Govern Function
11:00 AM	**Break**
11:15 AM	Govern Function (cont.)
11:35 AM	Identify Function
12:05 PM	Protect Function
12:15 PM	**Lunch**
1:15 PM	Protect Function (cont.)
1:55 PM	Detect Function
2:15 PM	**Break**
2:00 PM	Detect Function (cont.)
2:30 PM	Respond Function
3:15 PM	Recover Function
3:35 PM	Apply the CSF using MaPT
4:35 PM	Resources
4:55 PM	Wrap Up & Adjourn

Why use it?

Examples of Use

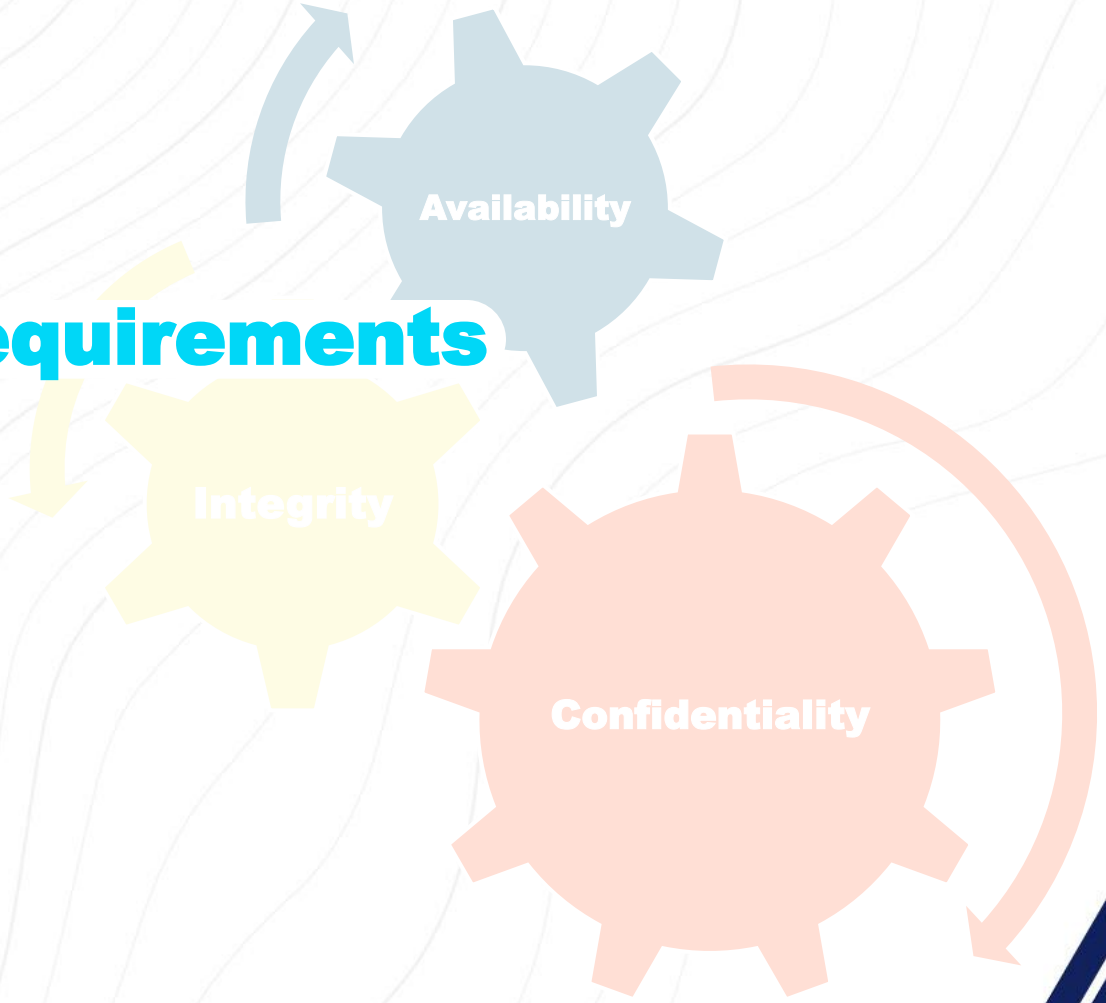
Use the Cybersecurity Framework to streamline requirements & capabilities

- Define capabilities for your cybersecurity program
- Align to standards & regulations
- Develop a common lexicon for you & your suppliers

Define capabilities for your cybersecurity program

Capture your priorities & requirements to drive cyber maturity

- Express your business goals & drivers
- Consider your cyber risks



Align to standards & regulations

Over 43 References are listed on NIST's website

- National Online Informative References Program (OLIR)
- Industry standards including:
  - ISO/IEC 27001
  - C2M2
  - NERC CIP
  - HITRUST CSF

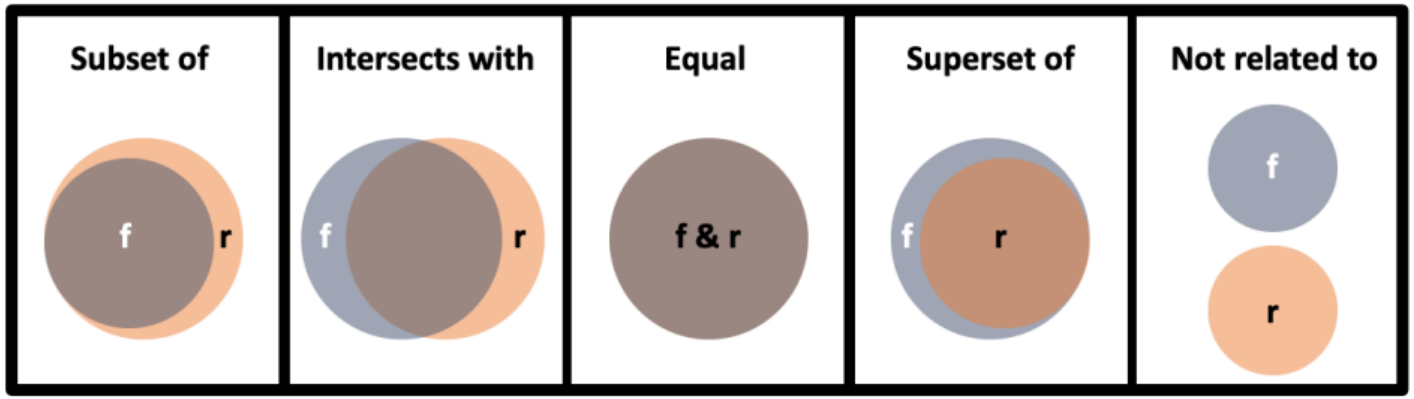


Figure 1: Relationship Types

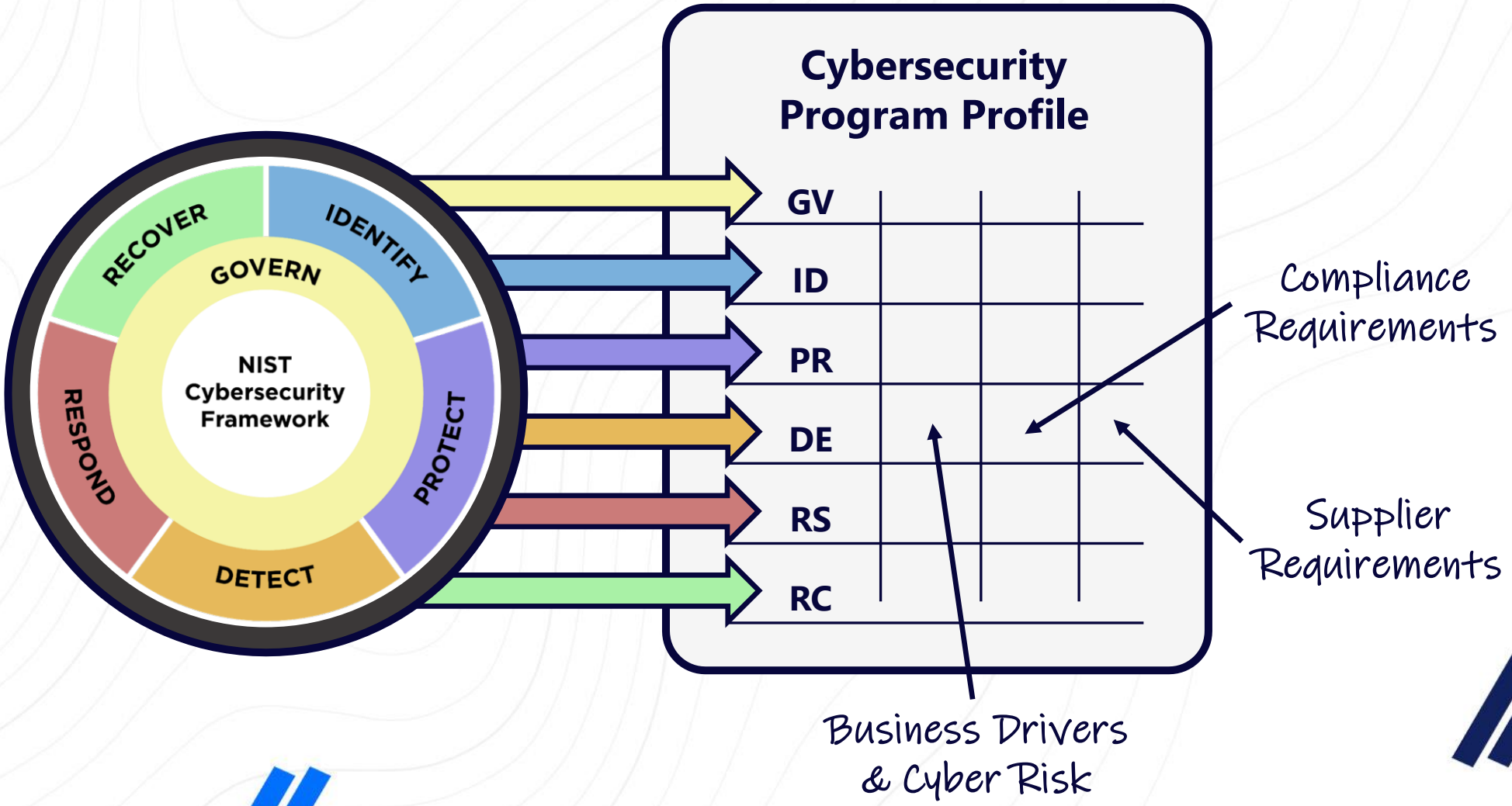
https://csrc.nist.gov/Projects/olir

Develop a common lexicon for you & your suppliers

Standardize on a common framework to ensure everyone is working towards the same goal

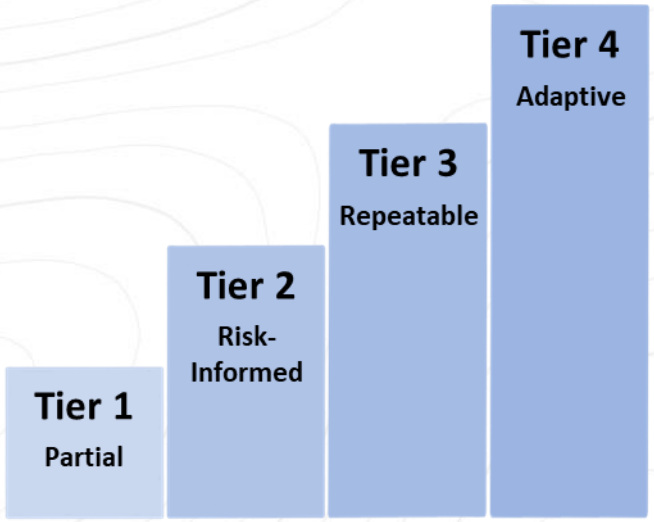
- Leverage the common language of the CSF
- Tailor for your industry
- Layer on the specific needs of your business

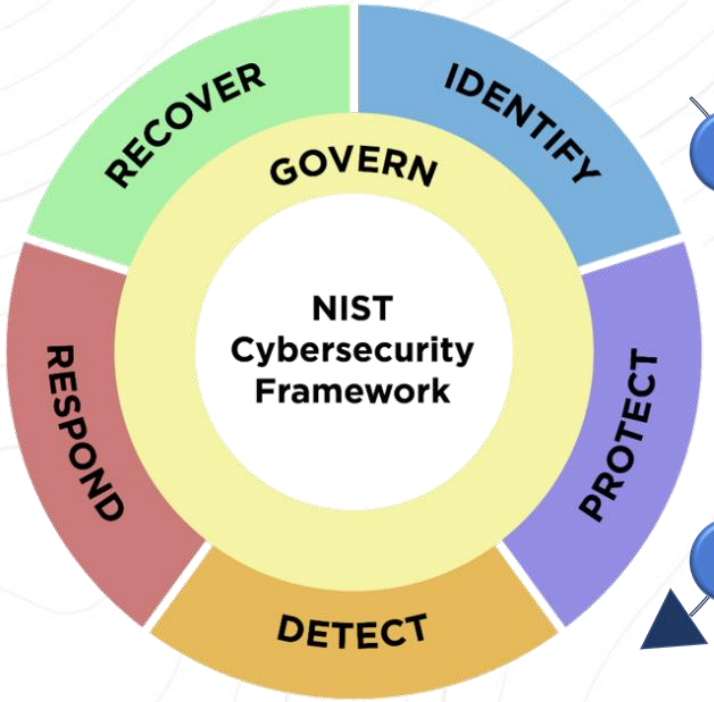
Develop a common lexicon for you & your suppliers

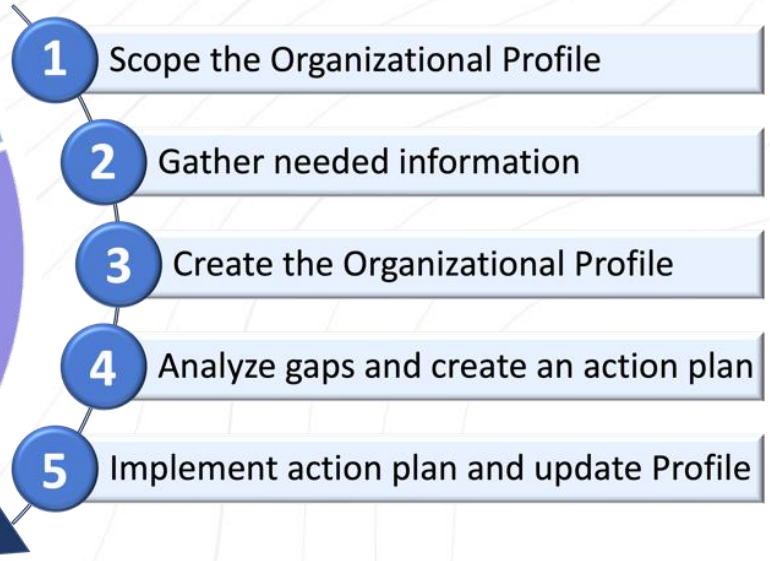


What is it?

NIST Cybersecurity Framework (CSF) 2.0





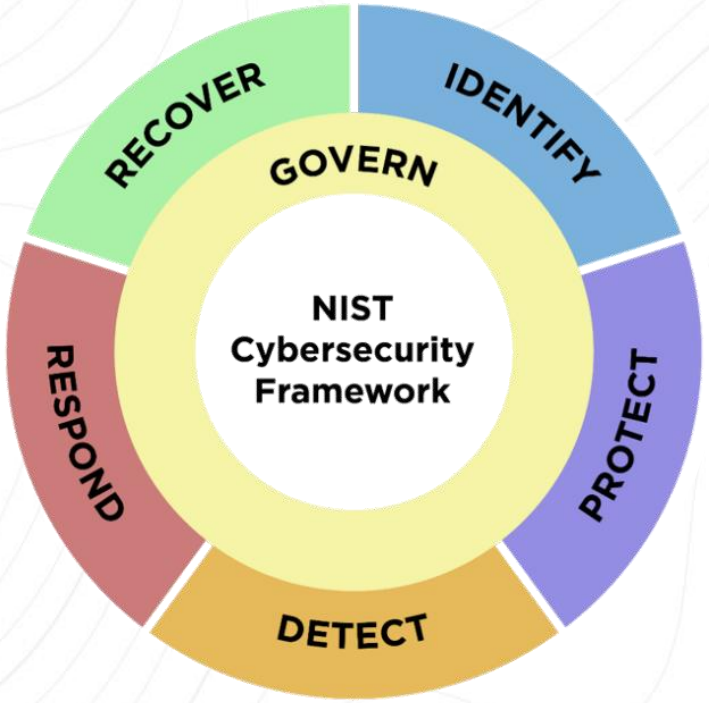


TIERS **CORE** **PROFILE**

Cybersecurity Framework 2.0 - Core

CORE

Cybersecurity Framework 2.0 - Core



CORE

FUNCTIONS

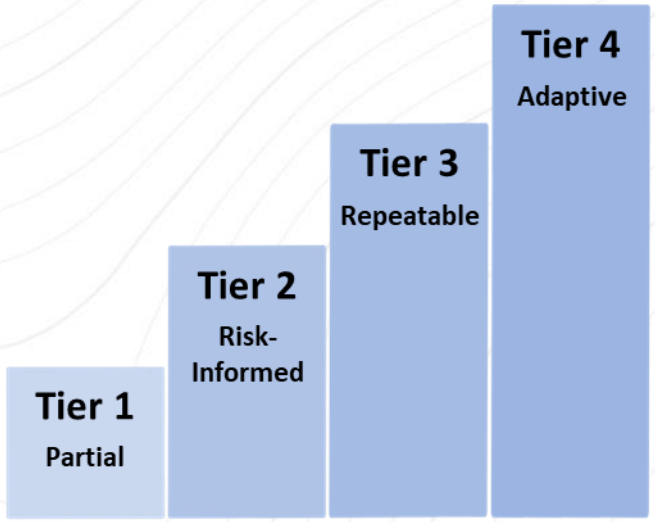
↓

CATEGORIES

↓

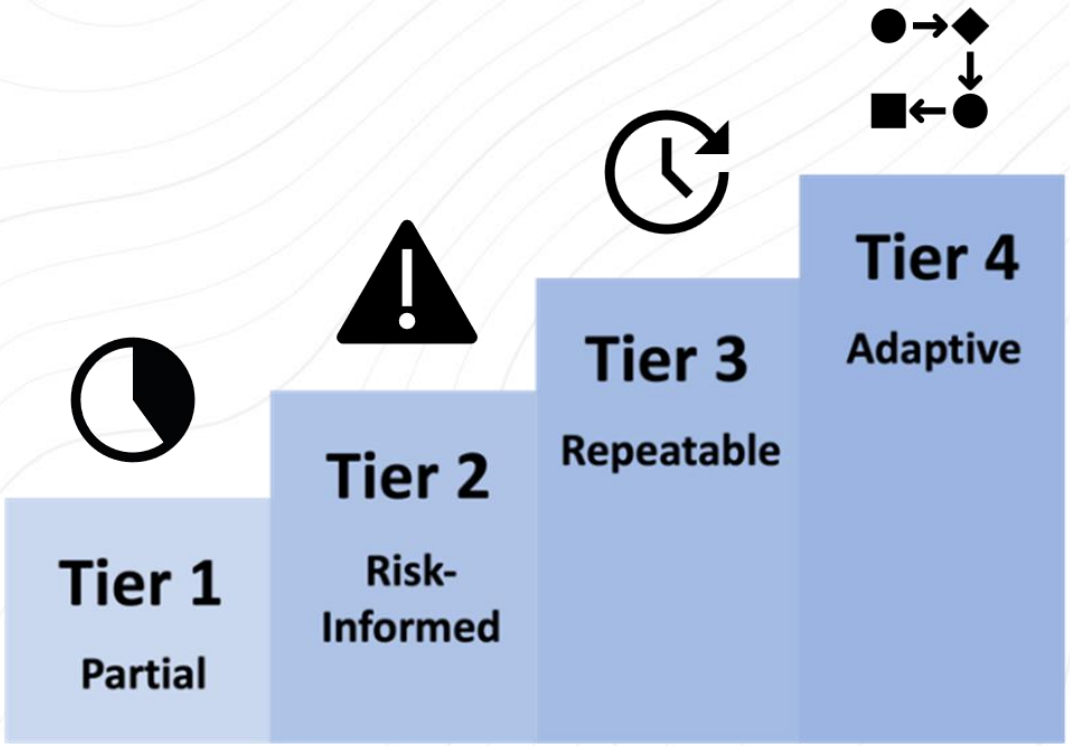
SUBCATEGORIES

Cybersecurity Framework 2.0 - Tiers



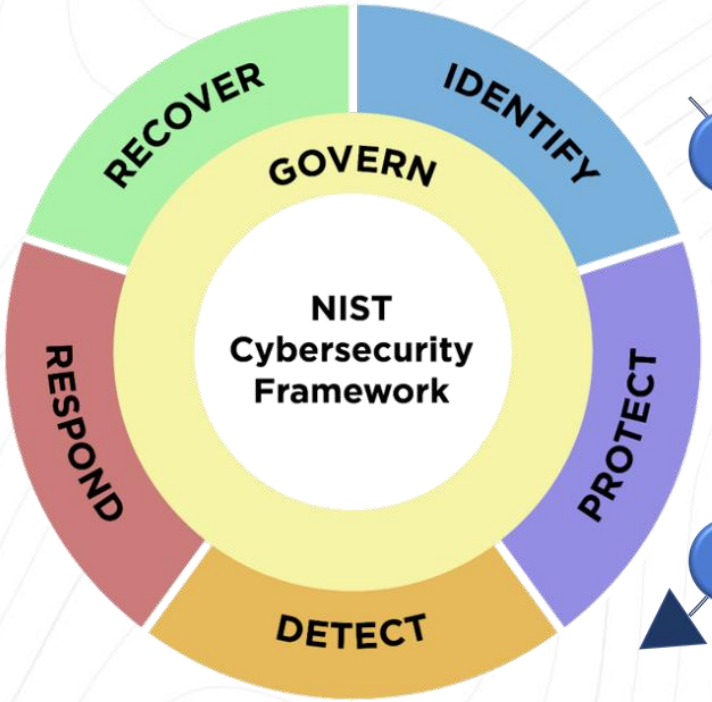
TIERS

Cybersecurity Framework 2.0 - Tiers



TIERS

Cybersecurity Framework 2.0 - Profiles

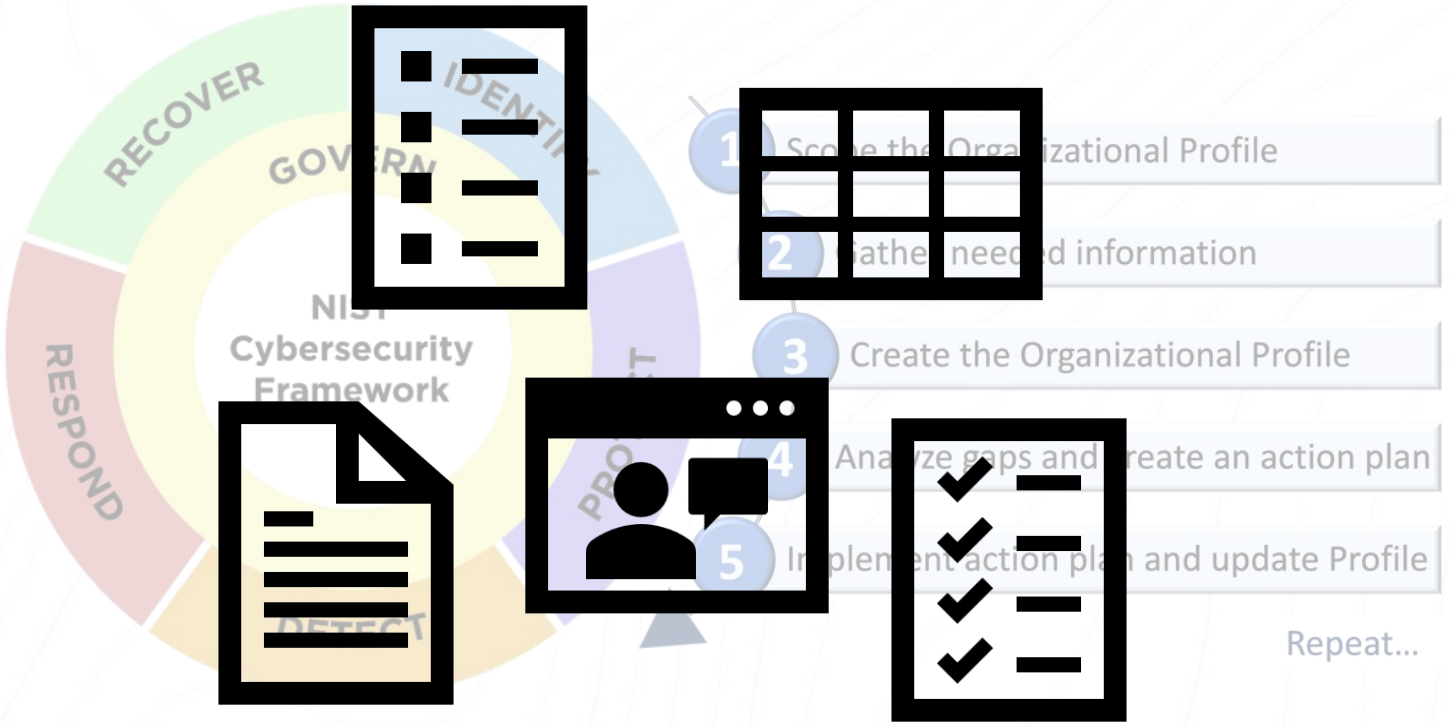


1. Scope the Organizational Profile
2. Gather needed information
3. Create the Organizational Profile
4. Analyze gaps and create an action plan
5. Implement action plan and update Profile

Repeat...

PROFILE

Cybersecurity Framework 2.0 - Profiles



PROFILE

What changed?

CSF v1.1

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

5 Functions

23 Categories

108 Subcategories

CSF v2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

↑ **6** Functions

↓ **22** Categories

↓ **106** Subcategories

Governance expanded from a Category to a Function

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

Framework Core

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

Framework Core

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Twelve Categories were removed *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

Framework Core

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Eleven new Categories were added *(or realigned)*

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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

Many areas stayed the same *(or very similar)*

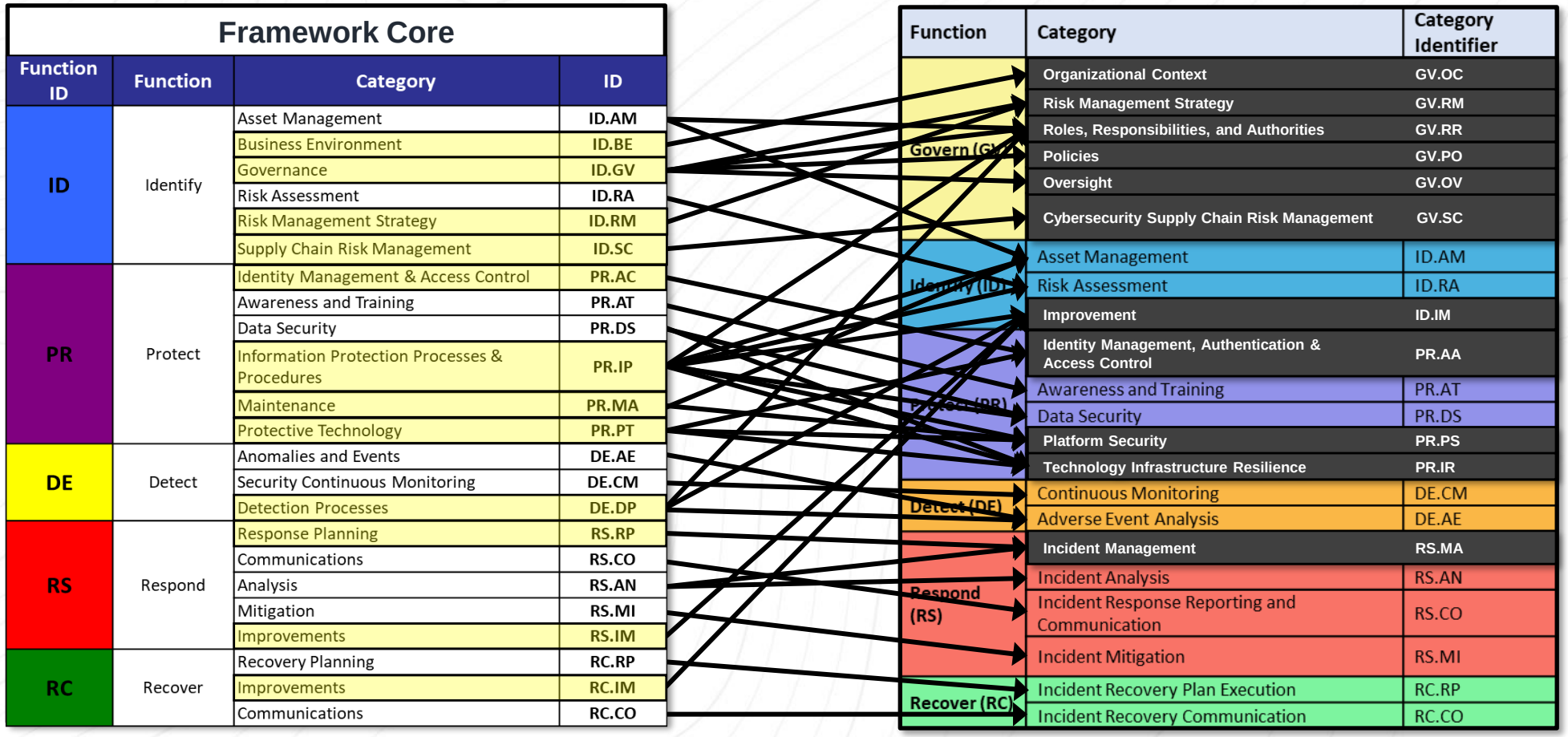
Framework Core			
Function ID	Function	Category	ID
ID	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PR	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training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

CSF v1.1

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

NIST Cybersecurity Framework v2.0 Summary of Changes



Framework Core

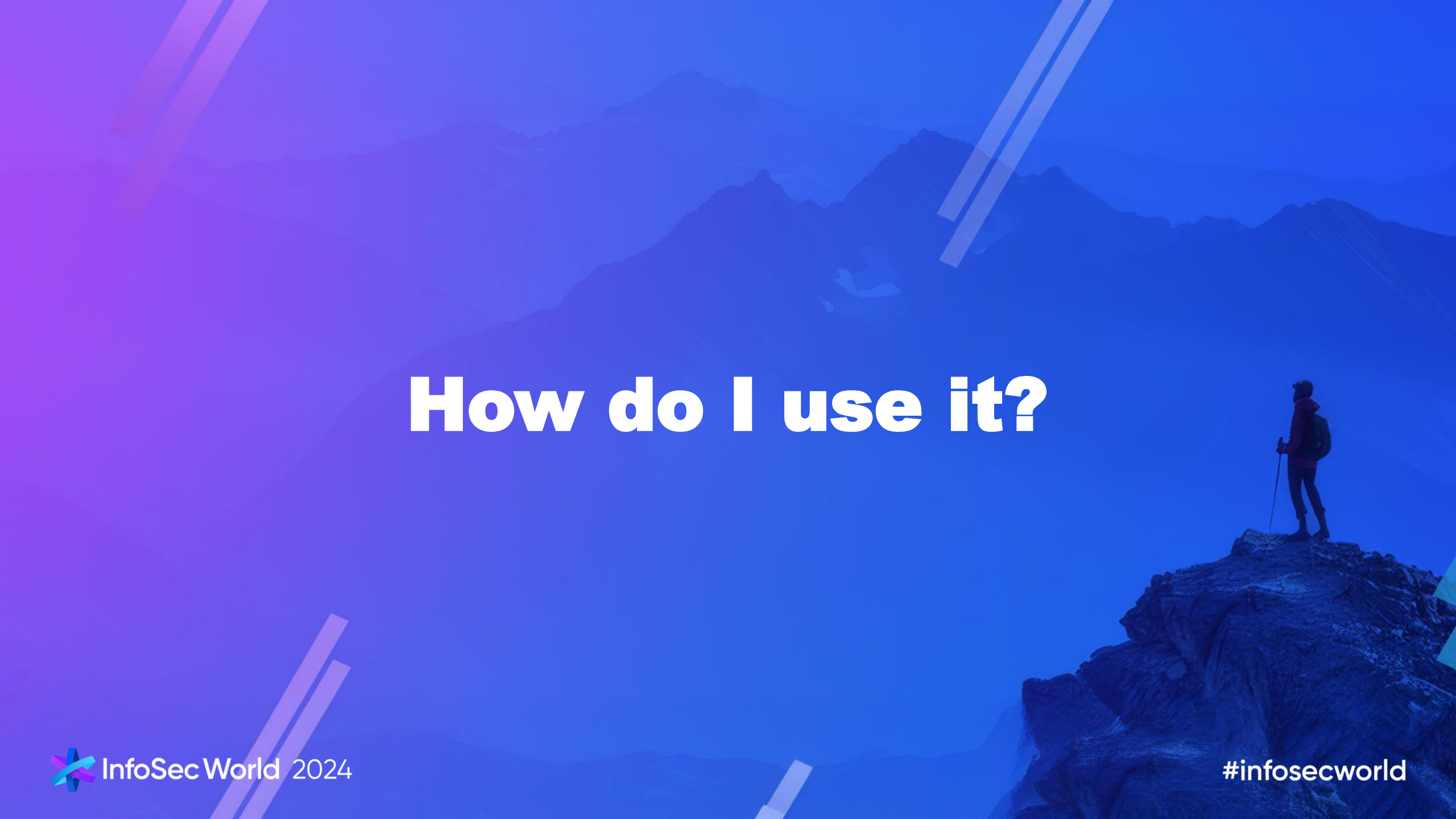
Function ID	Function	Category	ID
ID	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PR	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data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

CSF v1.1

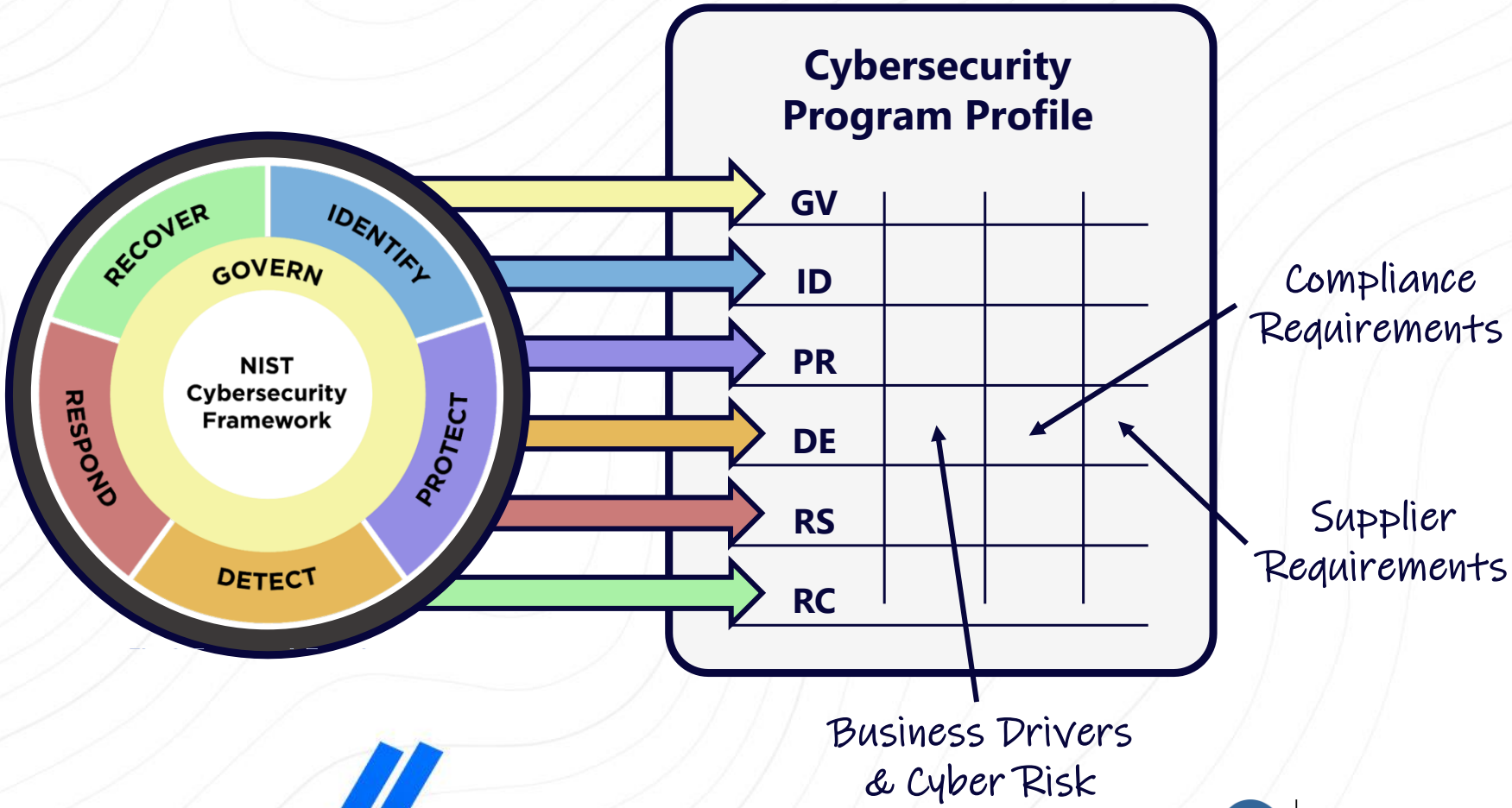
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policies	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication & Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF v2.0

How do I use it?



Using the Cybersecurity Framework enables you to streamline requirements & capabilities



Steps for Creating and Using Profiles

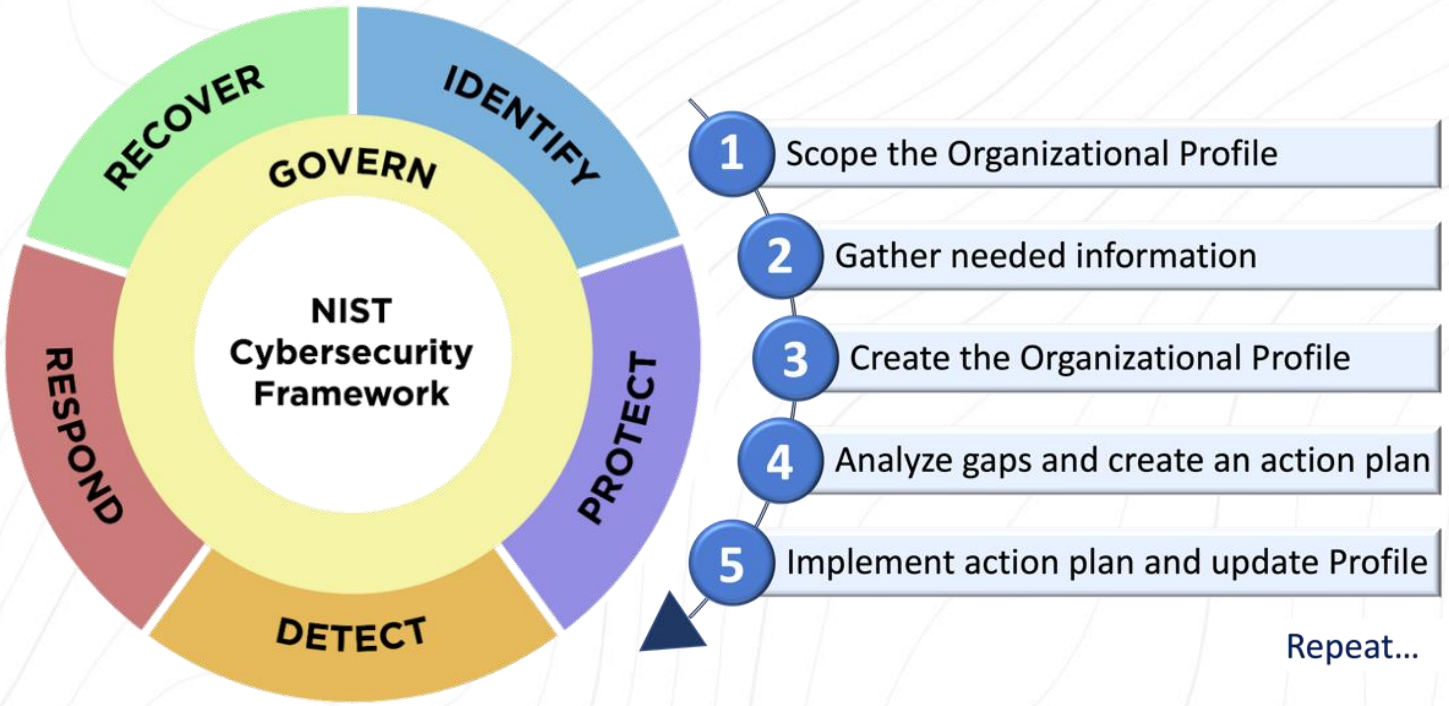
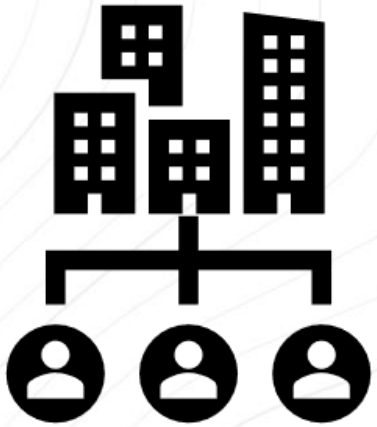


Figure 3: Steps for creating and using a CSF Organizational Profile

Step 1: Scope the Organizational Profile



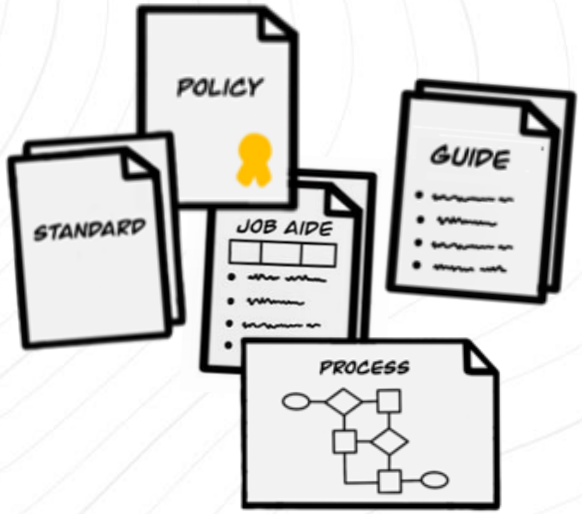
What are you evaluating?

- Your whole company?
- A line of business?
- A specific department?

Step 2: Gather Needed Information

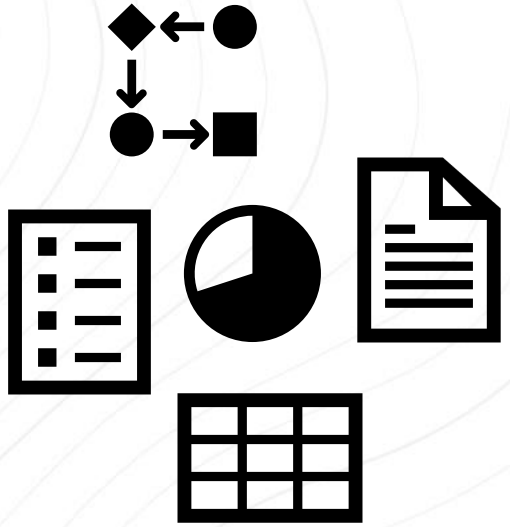
What do you already have?

- Policies
- Standards
- Procedures



HISTORY OF GREECE
J. B. BURY
ESSAYS AND STUDIES PRESENTED TO WILLIAM RIDGEWAY
EBLA
PAOLO MATTHIAE
PAX Britannica
THE FOUR SUNS
A World History
THE TRENCH
RICHARD VAN EMDEN
THE CELTIC HEROIC AGE
DUNGEON, FIRE AND SWORD
JOHN J. ROBINSON
THE VICTORIAN ECONOMY
François Crouzet
MACAULAY
FATAL COLOURS
Abraham Lincoln
The Chamberlain Letters
Basil Collier
RED GOLD
SEARLE
A NEW ENGLAND?
OXFORD
BRITANNIA
GRAHAM STEWART
THE CONQUEST OF PARADISE
Kirkpatrick Sale
THE STRIPPING OF THE ALTARS
DUFFY
YALE
THE PEOPLE'S WAR
Angus Calder
BATTLE FOR THE BUNDU

Step 3: Create the Organizational Profile



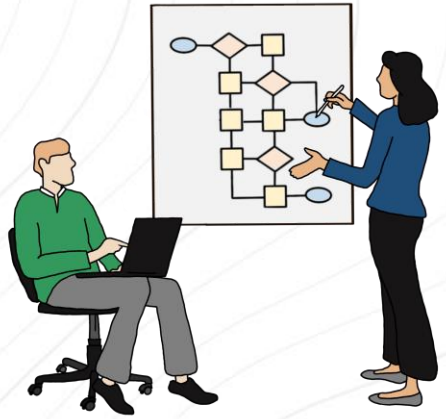
What is your Profile going to look like?

- List of Capabilities
- Images / Graphical Representation of Capabilities
- Full Description of Capabilities

Profiles help to define & streamline cybersecurity objectives

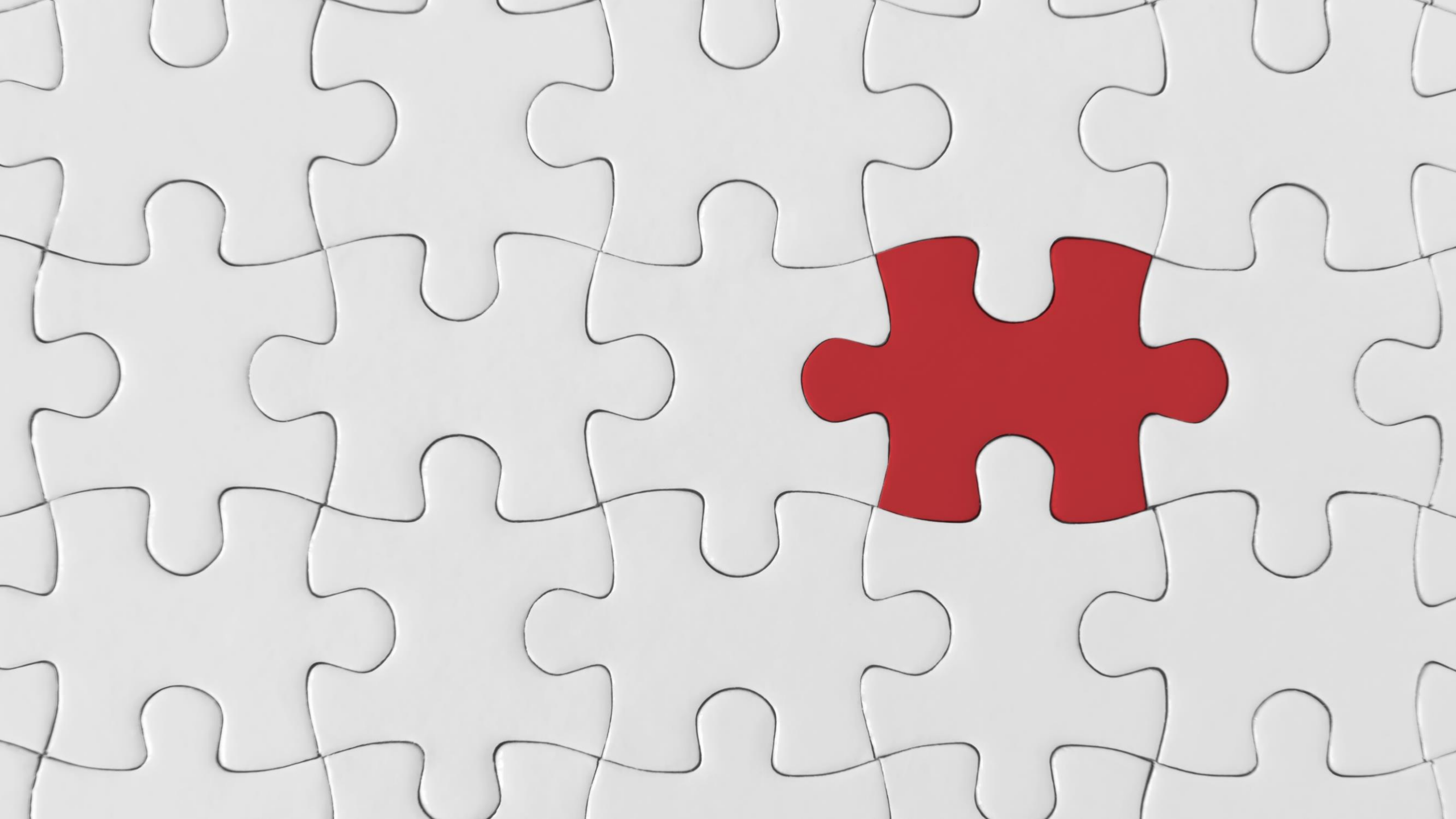
NIST Cybersecurity Framework 2.0	Business Drivers & Cyber Risk	Compliance Requirements		Supplier Requirements	Target Capability
		ISO 27001	CIRCIA		
RS.CO-02: Internal and external **stakeholders are notified** of incidents	**Internal** business leaders are notified of cyber incidents. Failure to notify appropriate stakeholders may compound the severity of cybersecurity incidents or lead to fines.	**A.6.8:** The organization should provide a mechanism for personnel to **report** observed or suspected **information security events** through **appropriate channels** in a **timely manner**.	Critical Infrastructure owners and operators are required to **report cybersecurity incidents within 72 hours** of discovery to CISA via **the CISA Incident Reporting portal**.	An **external** point of contact is maintained for all service providers with access to sensitive data or providing critical services	**Stakeholder reporting requirements** are defined in the Incident Response Plan (IRP). **Internal** and **external stakeholders'** contact information (e.g., phone number, email address) is maintained within the IRP. **Customer** account records include an email address for **notification** in the case of a **breach.**

Step 4: Analyze Gaps and Create an Action Plan



Compare your Current and Target Profiles

- Identify key gaps
- Prioritize resources
- Create a roadmap



Gaps in the current capabilities can be identified through by evaluating your Profile

NIST Cybersecurity Framework 2.0	Business Drivers & Cyber Risk	Compliance Requirements		Supplier Requirements	Target Capability	Gaps
		ISO 27001	CIRCIA			
RS.CO-02: Internal and external **stakeholders are notified** of incidents	**Internal** business leaders are notified of cyber incidents. Failure to notify appropriate stakeholders may compound the severity of cybersecurity incidents or lead to fines.	**A.6.8:** The organization should provide a mechanism for personnel to **report** observed or suspected **information security events** through **appropriate channels** in a **timely manner**.	Critical Infrastructure owners and operators are required to **report cybersecurity incidents within 72 hours** of discovery to CISA via **the CISA Incident Reporting portal**.	An **external** point of contact is maintained for all service providers with access to sensitive data or providing critical services	**Stakeholder reporting requirements** are defined in the Incident Response Plan (IRP). **Internal** and **external stakeholders'** contact information (e.g., phone number, email address) is maintained within the IRP. **Customer** account records include an email address for **notification** in the case of a **breach.**	**External stakeholders** have not been identified. A **process** for notifying **customers** has not been created.

Step 5: Implement Action Plan and Update Profile

Go forth and conquer!


HOLLYWOOD

Steps for Creating and Using Profiles

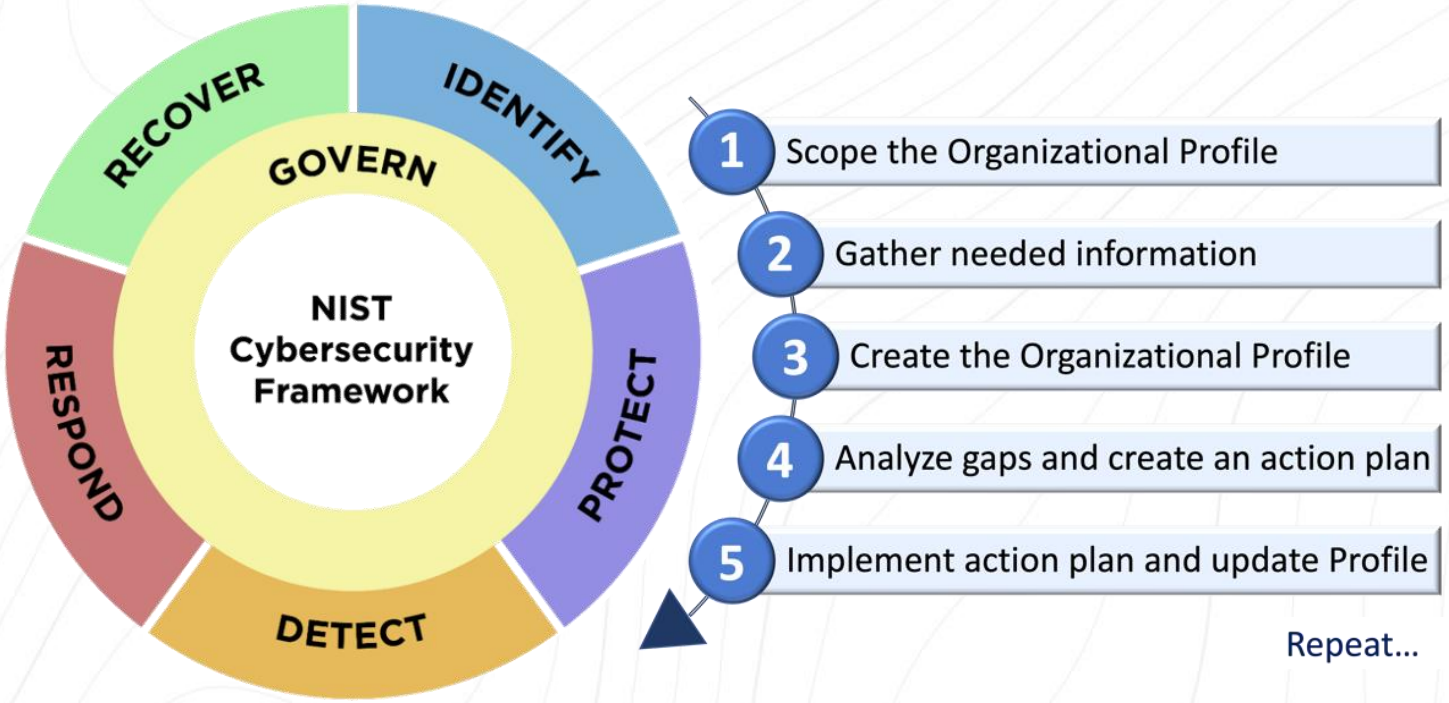
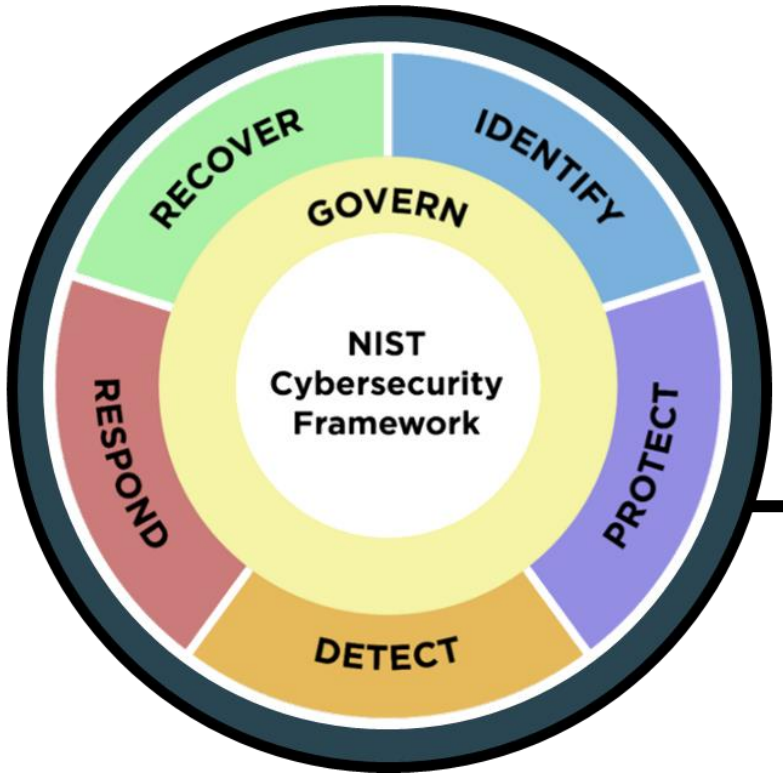


Figure 3: Steps for creating and using a CSF Organizational Profile

What should I know?



NIST Cybersecurity Framework v2.0

Workbook

InfoSec World Workshop Handouts

https://www.opticcyber.com/resources/CSF2Handouts.html

Prepared by:

OPTIC CYBER SOLUTIONS

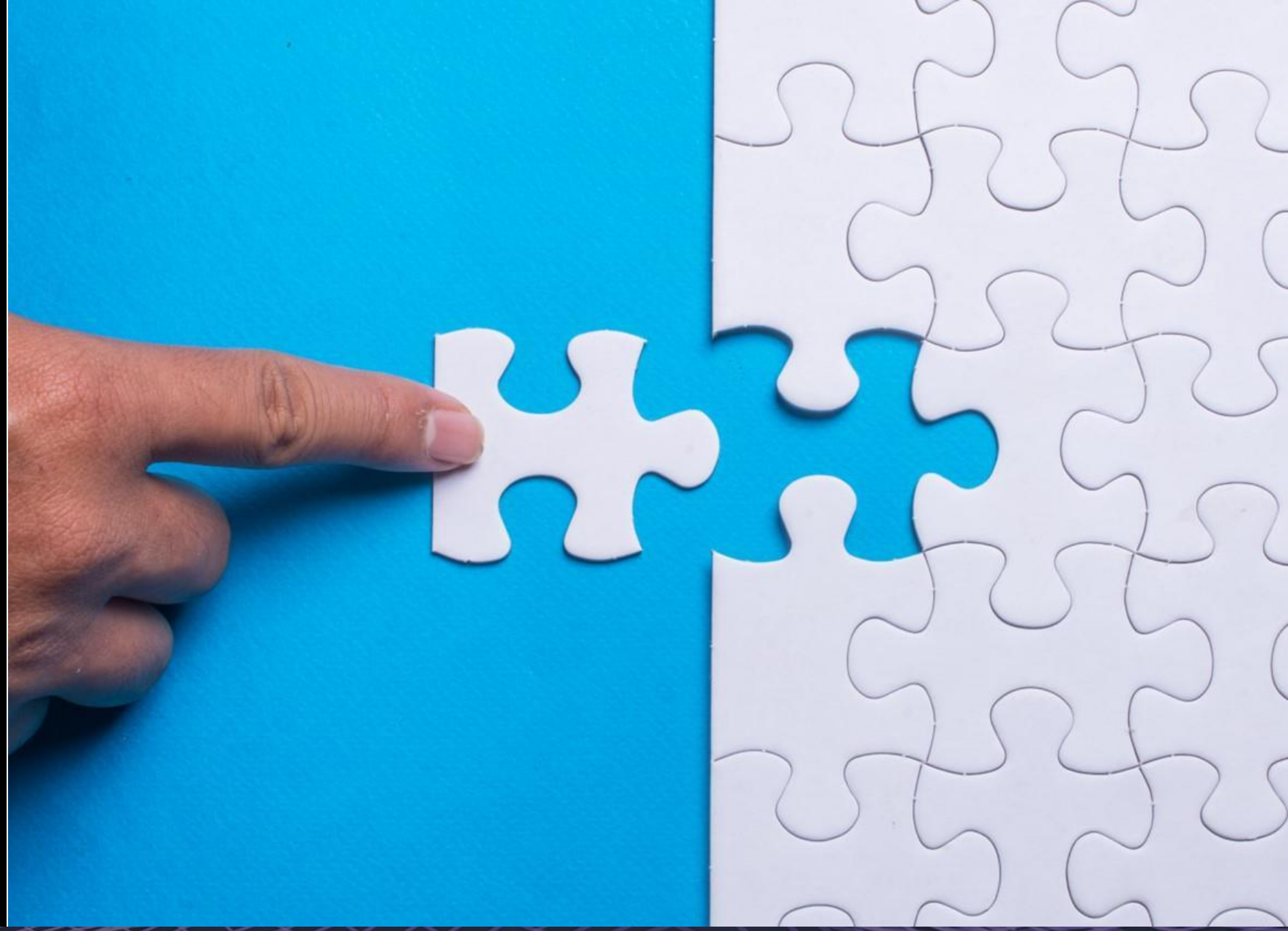
What are your business goals & objectives?

What's included in the new Govern Function?

GOVERN

- Organizational Context (GV.OC)
- Risk Management Strategy (GV.RM)
- Roles, Responsibilities, & Authorities (GV.RR)
- Policy (GV.PO)
- Oversight (GV.OV)
- Cybersecurity Supply Chain Risk Management (GV.SC)

ORGANIZATIONAL CONTEXT (GV.OC)



RISK MANAGEMENT STRATEGY (GV.RM)

How much risk is ok?

Risk Appetite

The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value.

Source: NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)

How much risk is ok?

Risk Appetite

The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value.

Risk Tolerance

The organization's or stakeholder's readiness to bear the remaining risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be influenced by legal or regulatory requirements.

Source: NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)

How much risk is ok?

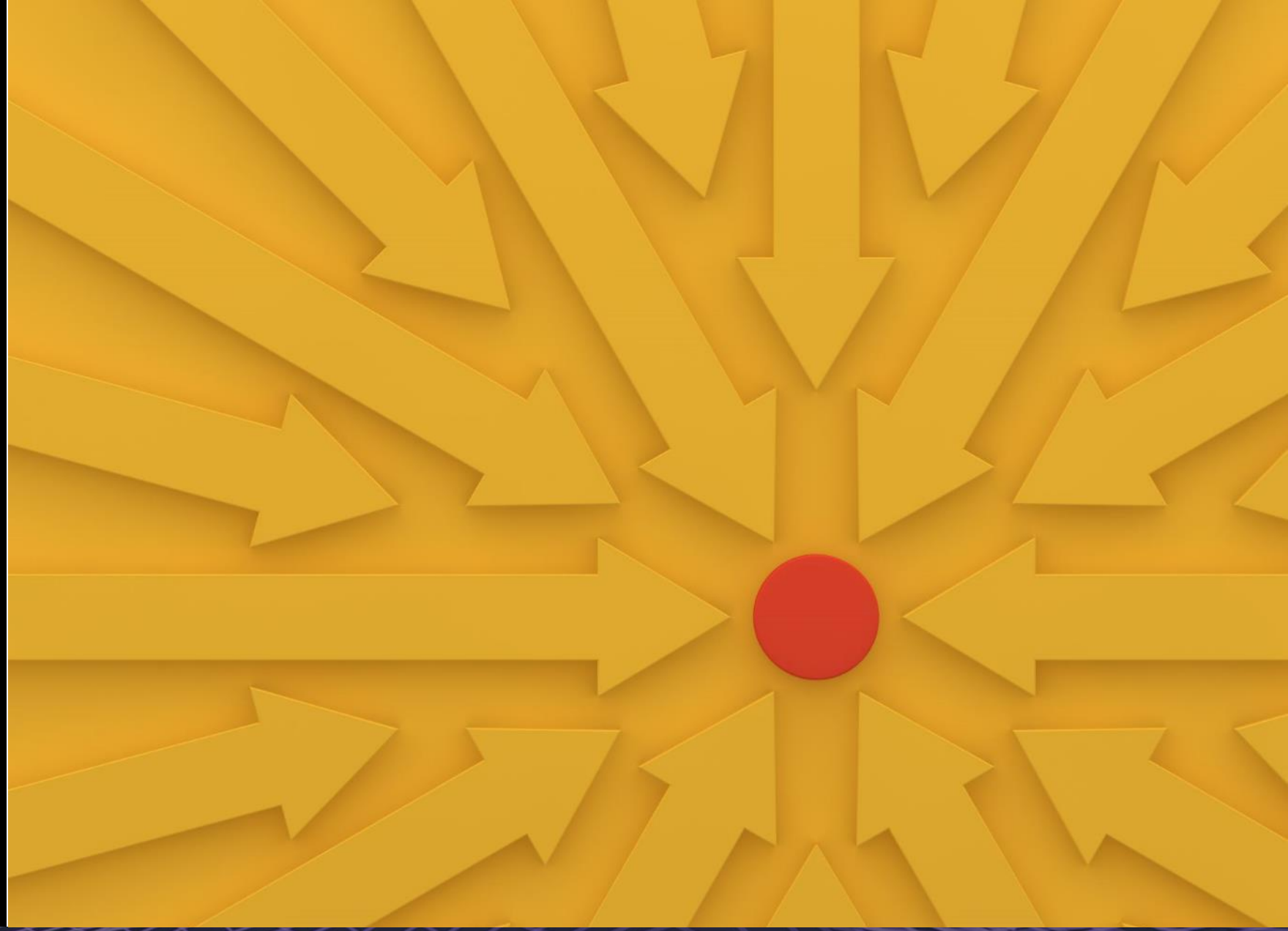
Table 1: Notional Examples of Risk Appetite and Risk Tolerance

Example Enterprise Type	Example Risk Appetite Statement	Example Risk Tolerance Statement
Global Retail Firm	Our customers associate reliability with our company's performance, so service disruptions must be minimized for any customer-facing websites.	Regional managers may permit website outages lasting up to 4 hours for no more than 5 % of its customers.
Government Agency	Mission-critical systems must be protected from known cybersecurity vulnerabilities.	Systems designated as mission-critical must be patched against critical software vulnerabilities (severity score of 10) within 14 days of discovery.
Internet Service Provider	The company has a low risk appetite with regard to failure to meet customer service level agreements, including network availability and communication speeds.	Patches must be applied within deadlines to avoid attack-related outages but also must be well-tested and deployed in a manner that does not reduce availability below agreed-upon service levels.

Source: NISTIR 8286a, Table 1

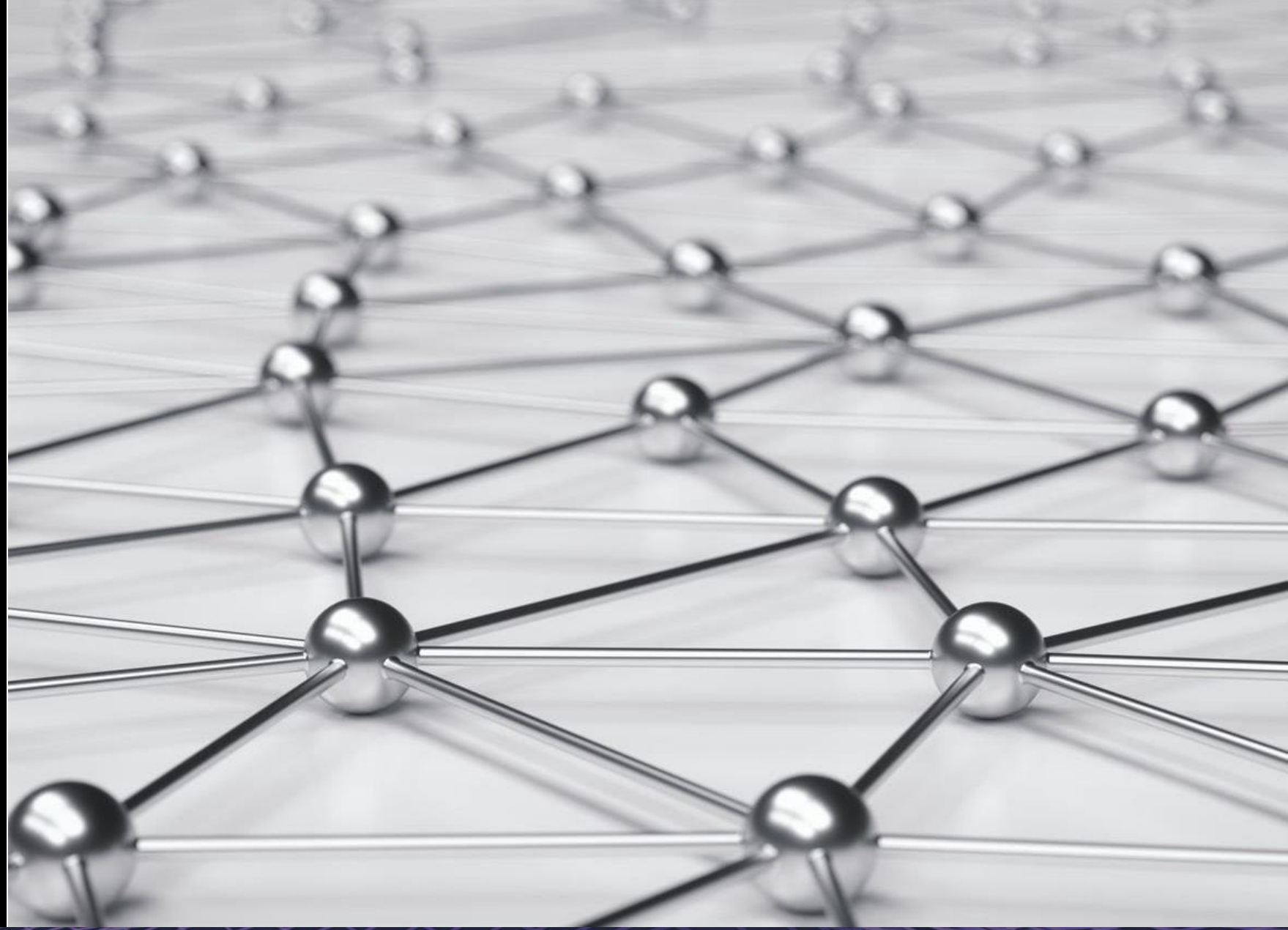
ROLES, RESPONSIBILITIES, & AUTHORITIES (GV.RR)

POLICY (GV.PO)

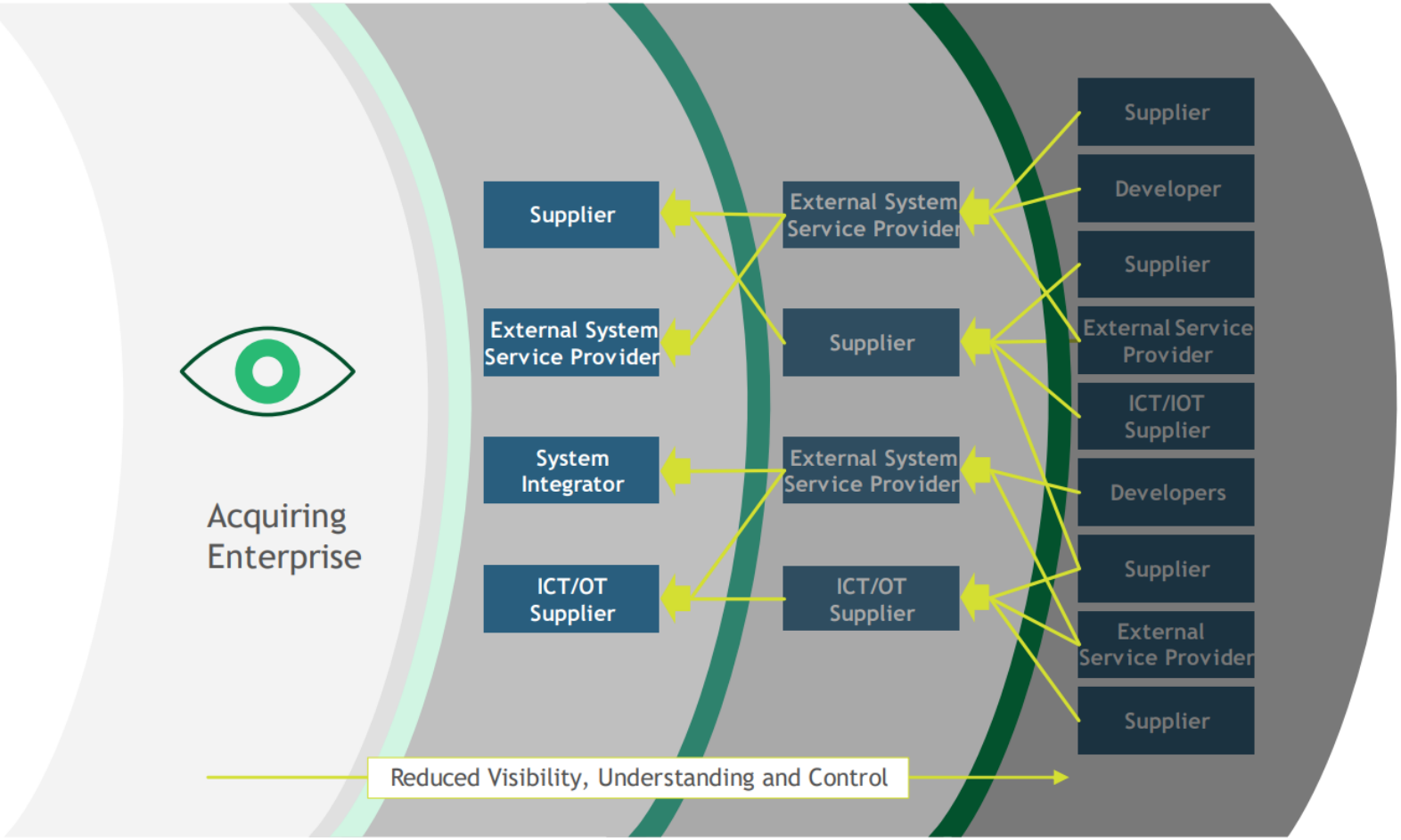


OVERSIGHT (GV.OV)

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (GV.SC)



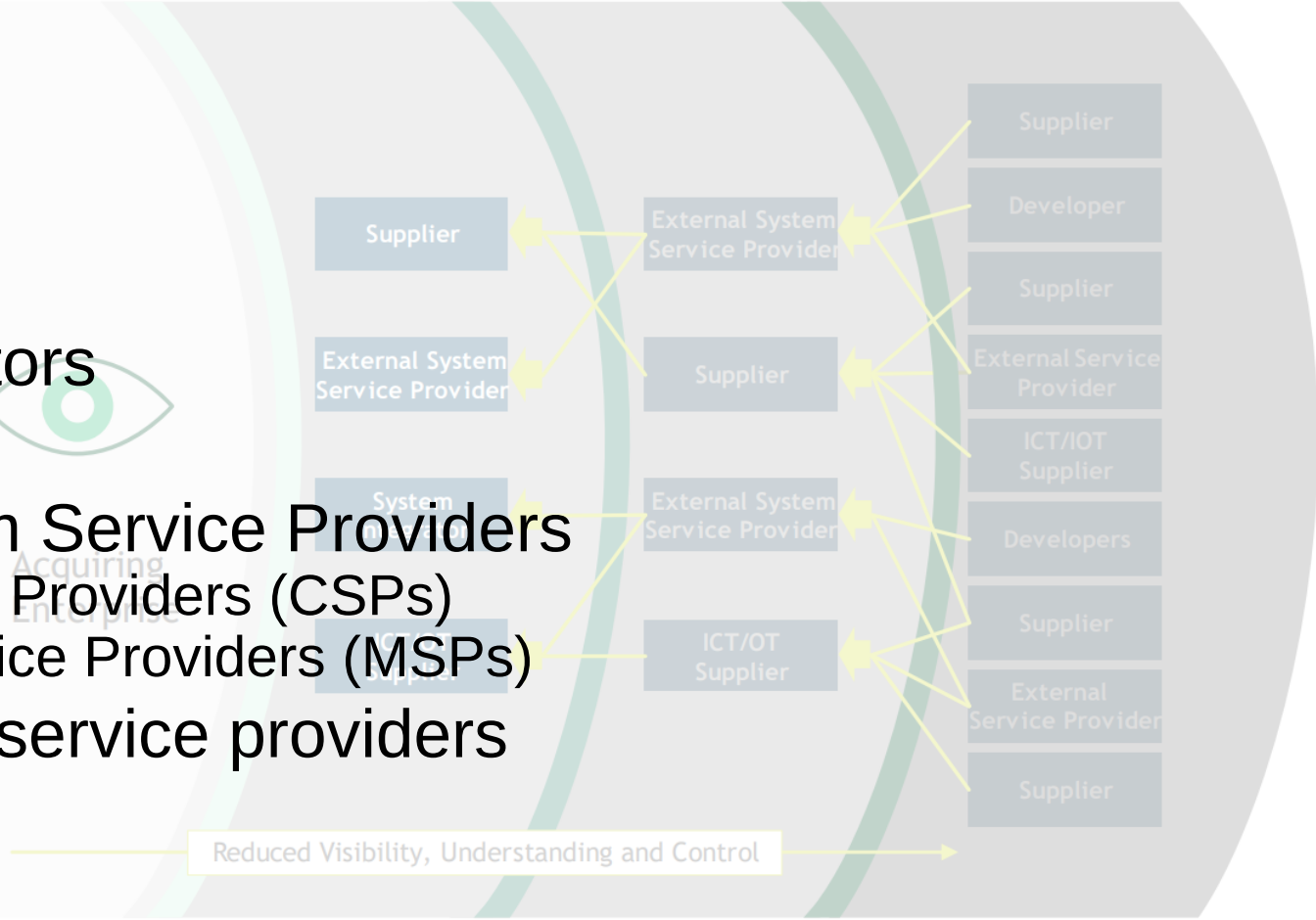
Cybersecurity Supply Chain Risk Management (C-SCRM)



NIST SP 800-161 r1: Fig. 1-2: An Enterprise's Visibility, Understanding, and Control of its Supply Chain

Who are you working with?

- Partners
- Suppliers
- Developers
- System Integrators
- Vendors
- External System Service Providers
  - Cloud Security Providers (CSPs)
  - Managed Service Providers (MSPs)
- ICT/OT-related service providers



Who are you working with?

- Partners
- Suppliers
- Developers
- System Integrators
- Vendors
- External System Service Providers
  - Cloud Security Providers (CSPs)
  - Managed Service Providers (MSPs)
- ICT/OT-related service providers

Google Cloud

Who are you working with?

- Partners
- Suppliers
- Developers
- System Integrators
- Vendors
- External System Service Providers
  - Cloud Security Providers (CSPs)
  - Managed Service Providers (MSPs)
- ICT/OT-related service providers

Who are you working with?

- Partners
- Suppliers
- Developers
- System Integrators
- Vendors
- External System Service Providers
  - Cloud Security Providers (CSPs)
  - Managed Service Providers (MSPs)
- ICT/OT-related service providers

What's included in the Identify Function?

IDENTIFY

- Asset Management (ID.AM)
- Risk Assessment (ID.RA)
- Improvement (ID.IM)

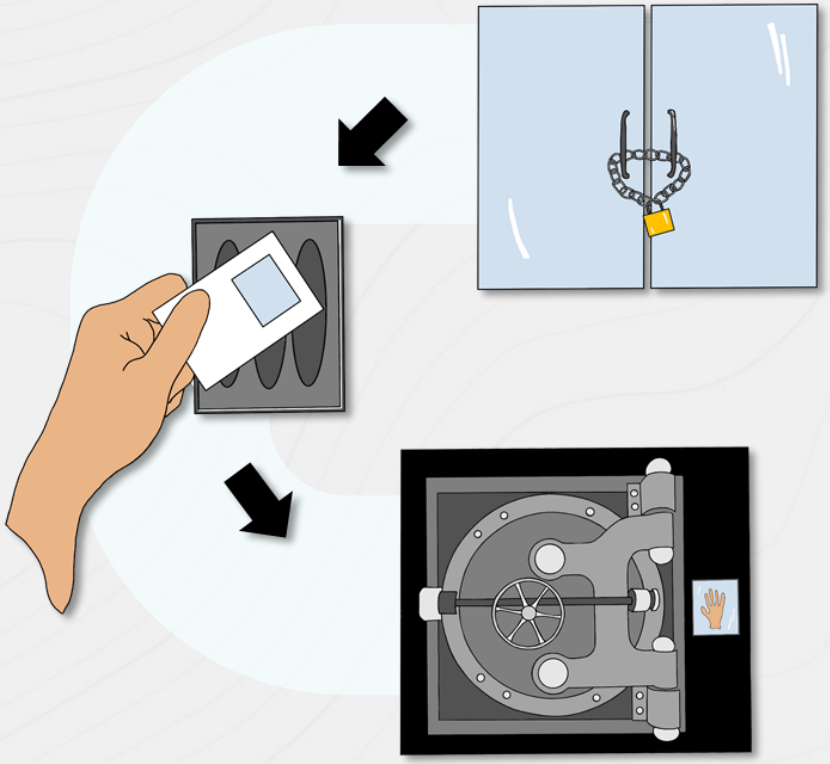
ASSET MANAGEMENT (ID.AM)

RISK ASSESSMENT (ID.RA)

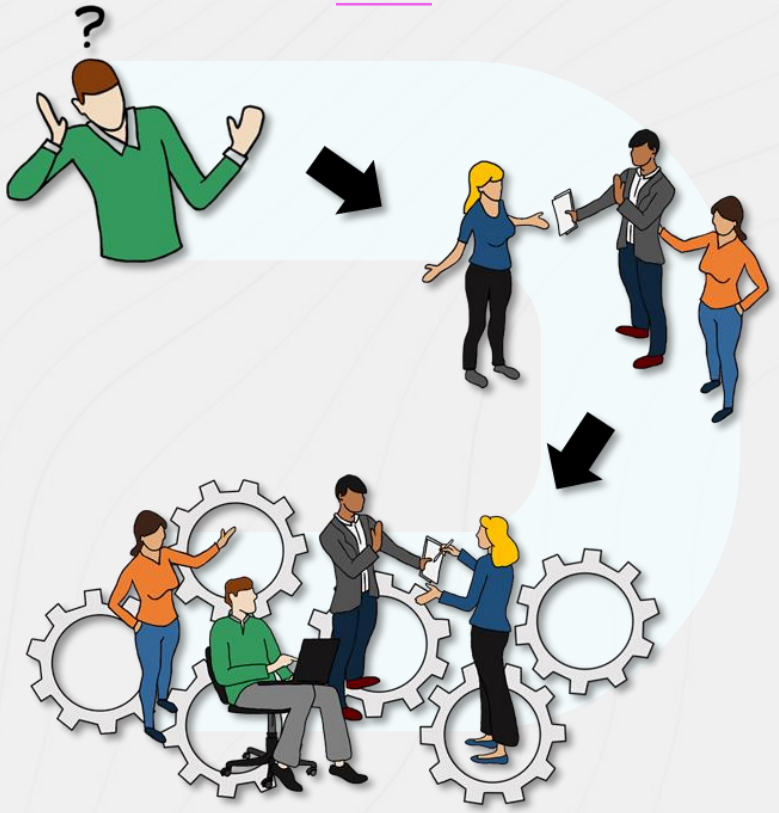
IMPROVEMENT (ID.IM)

There are multiple ways to evaluate performance

FUNCTIONALITY

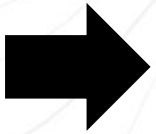


ASSURANCE



Looking at the tactical metrics in context helps to understand performance

Metric	Tactical
Count	Resolved Vulnerabilities
Count	False positives on SIEM
Time	System Outage
Count	Unknown Assets Discovered
Date	Capability Deployment
Time	Unresolved Vulnerabilities
Count	Open POA&M Items
Count	Phishing Links Clicked



Performance Indicator	Strategic
Trend up over & increase in speed	Vulnerability Management Program Effectiveness
Trend down over time	SOC Performance Effectiveness
RTO met	Incident Response Effectiveness
Trend down over time	Asset Management Program Effectiveness
Milestones met	SDLC Effectiveness
Speed increase over time	Vulnerability Management Program Effectiveness
Trend down over time	Program / Risk Management Effectiveness
Trend down over time	User Awareness Training Effectiveness

What's included in the Protect Function?

PROTECT

- Identity Management, Authentication, and Access Control (PR.AA)
- Awareness & Training (PR.AT)
- Data Security (PR.DS)
- Platform Security (PR.PS)
- Technology Infrastructure Resilience (PR.IR)

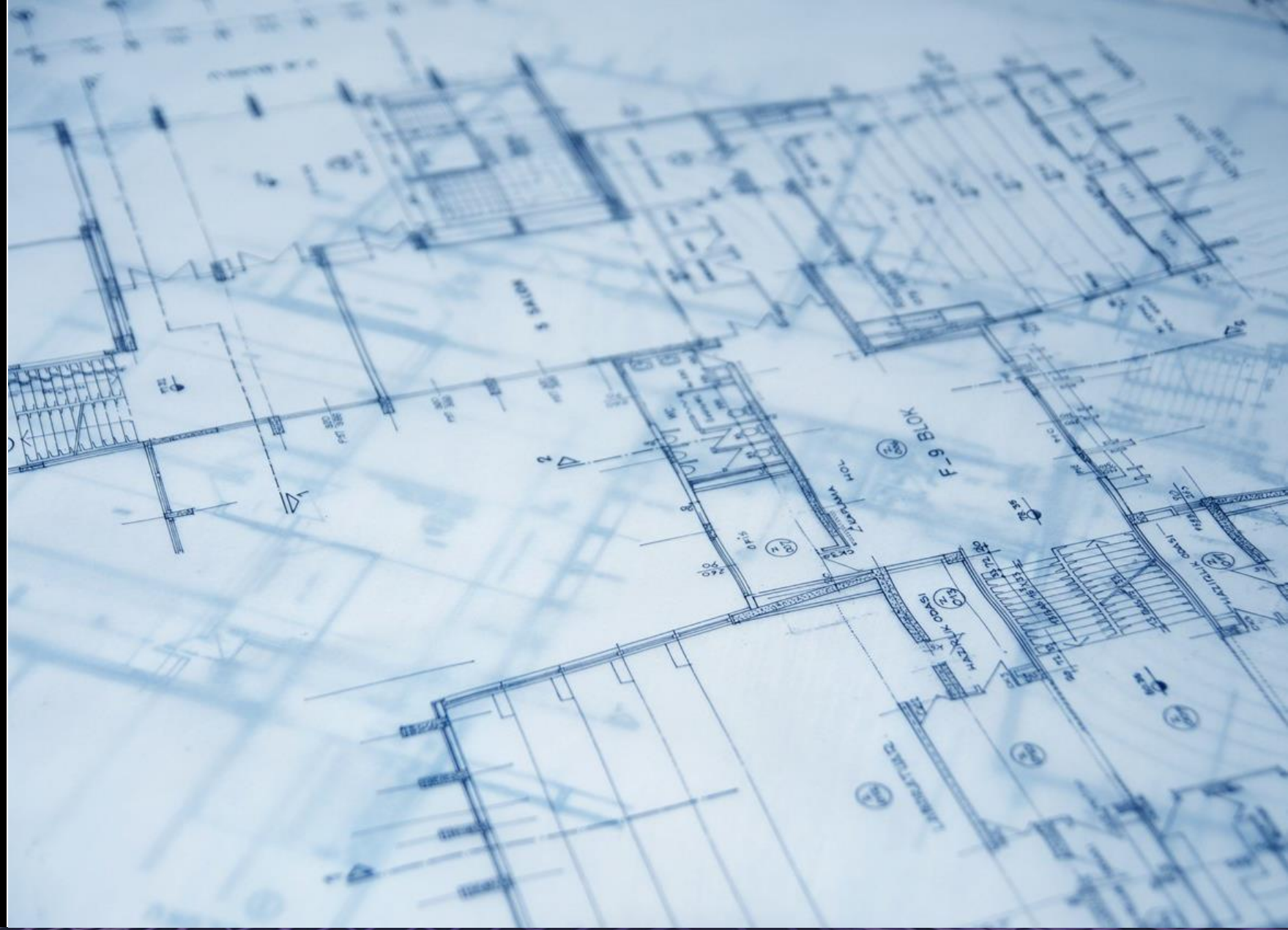
IDENTITY MANAGEMENT, AUTHENTICATION, & ACCESS CONTROL (PR.AA)

AWARENESS & TRAINING (PR.AT)

DATA SECURITY (PR.DS)

PLATFORM SECURITY (PR.PS)

TECHNOLOGY INFRASTRUCTURE RESILIENCE (PR.IR)



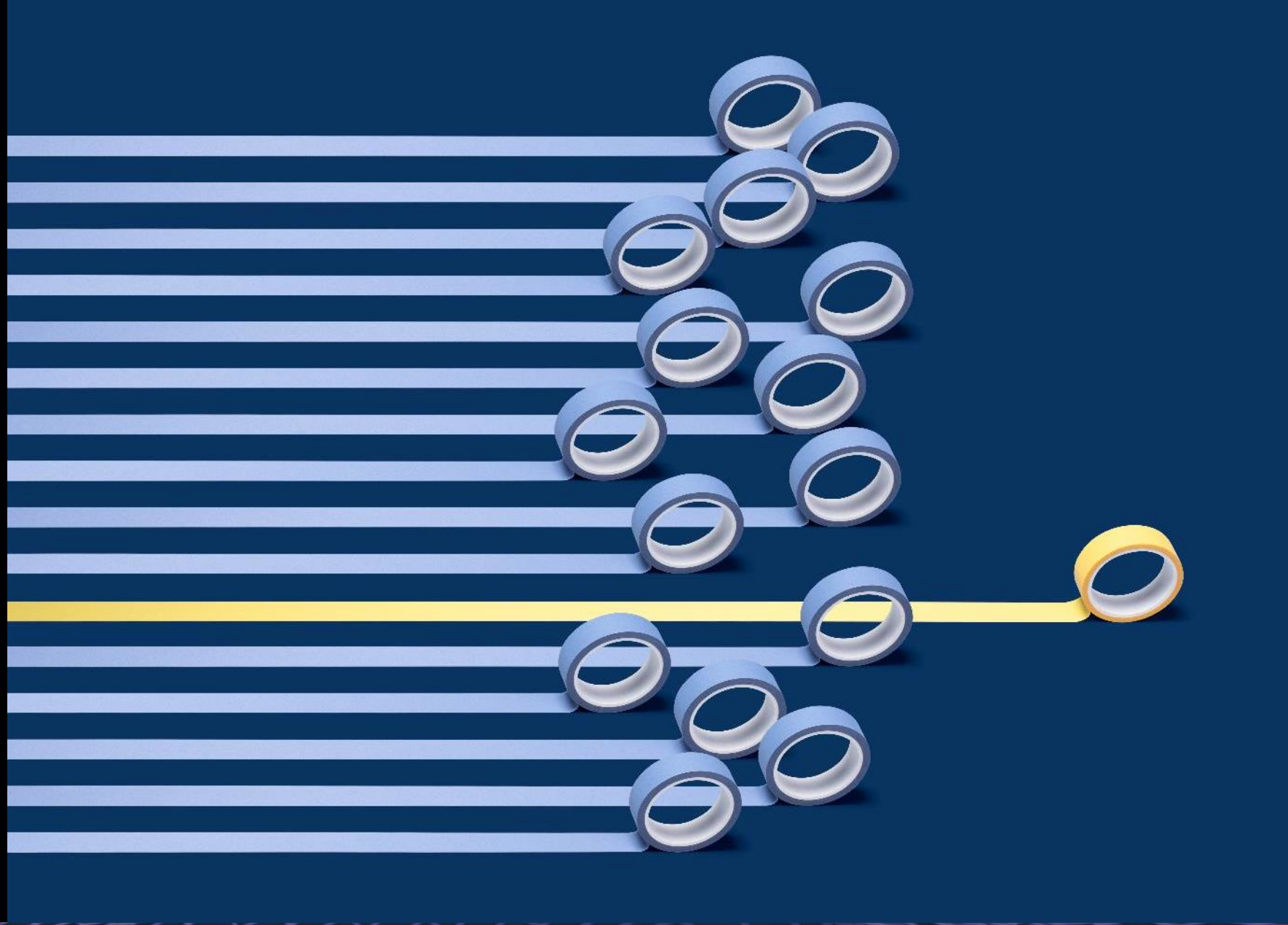
What's included in the Detect Function?

DETECT

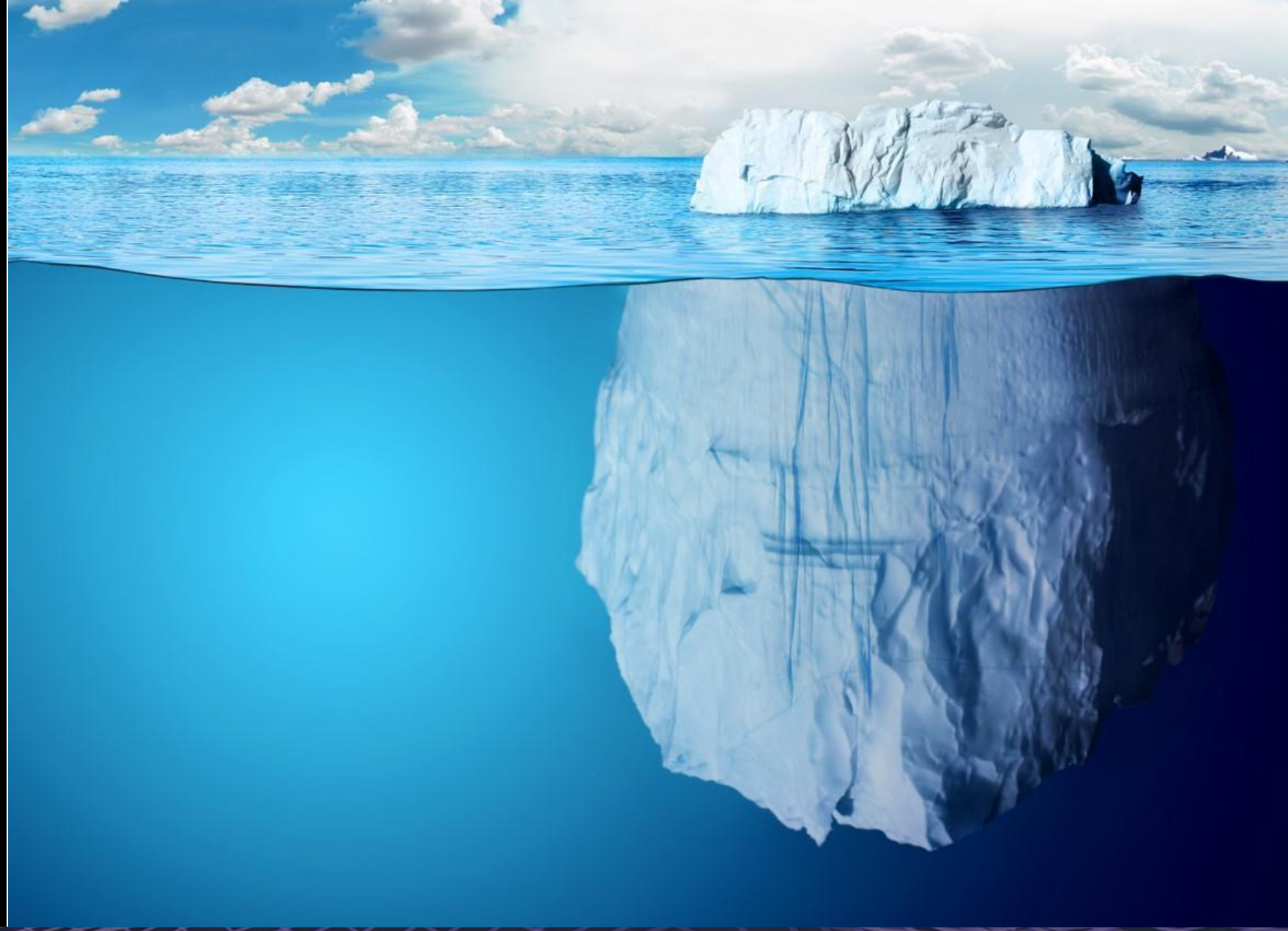
Continuous Monitoring
(DE.CM)

Adverse Event Analysis
(DE.AE)

CONTINUOUS MONITORING (DE.CM)



ADVERSE EVENT ANALYSIS (DE.AE)



What's included in the Respond Function?

RESPOND

- Incident Management (RS.MA)
- Incident Analysis (RS.AN)
- Incident Response Reporting & Communication (RS.CO)
- Incident Mitigation (RS.MI)

INCIDENT MANAGEMENT (RS.MA)

INCIDENT ANALYSIS (RS.AN)

INCIDENT RESPONSE REPORTING & COMMUNICATION (RS.CO)

INCIDENT MITIGATION (RS.MI)

What's included in the Recover Function?

RECOVER

Incident Recovery Plan Execution (RC.RP)

Incident Recovery Communication (RC.CO)

INCIDENT RECOVERY PLAN EXECUTION (RC.RP)

INCIDENT RECOVERY COMMUNICATION (RC.CO)

CSF v1.1

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

5 Functions

23 Categories

108 Subcategories

CSF v2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

↑ **6** Functions

↓ **22** Categories

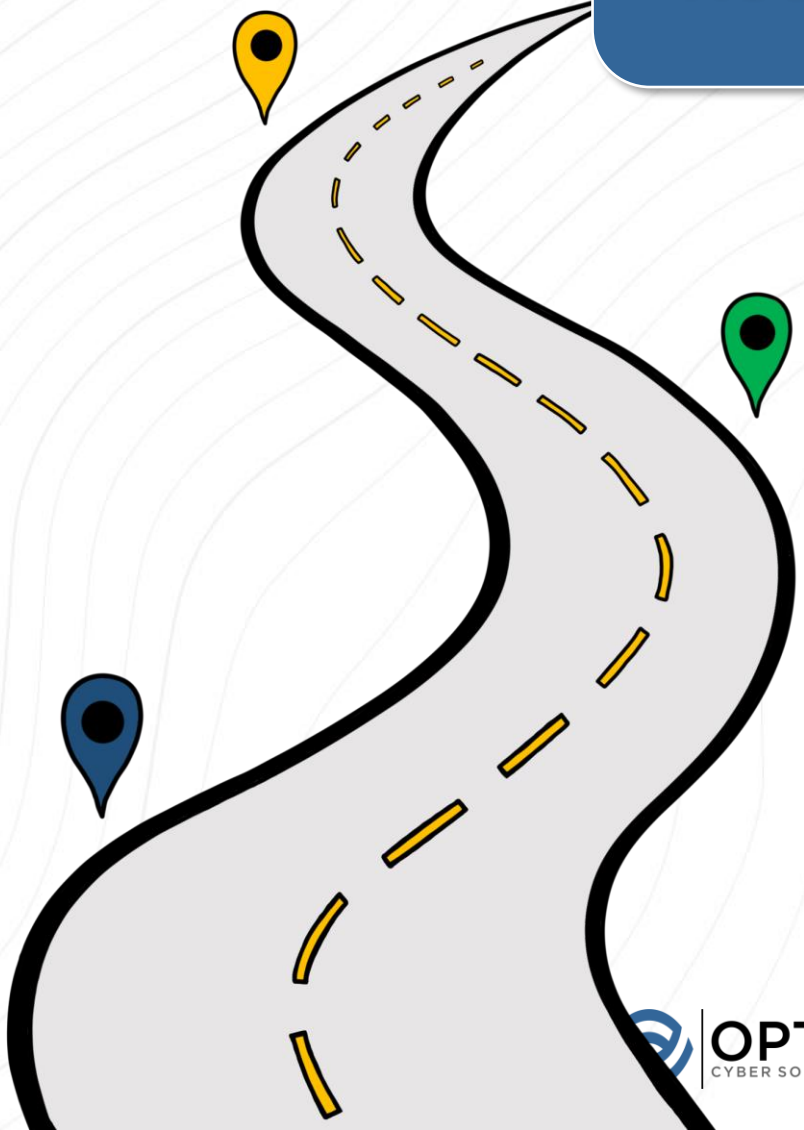
↓ **106** Subcategories

Do I measure up?

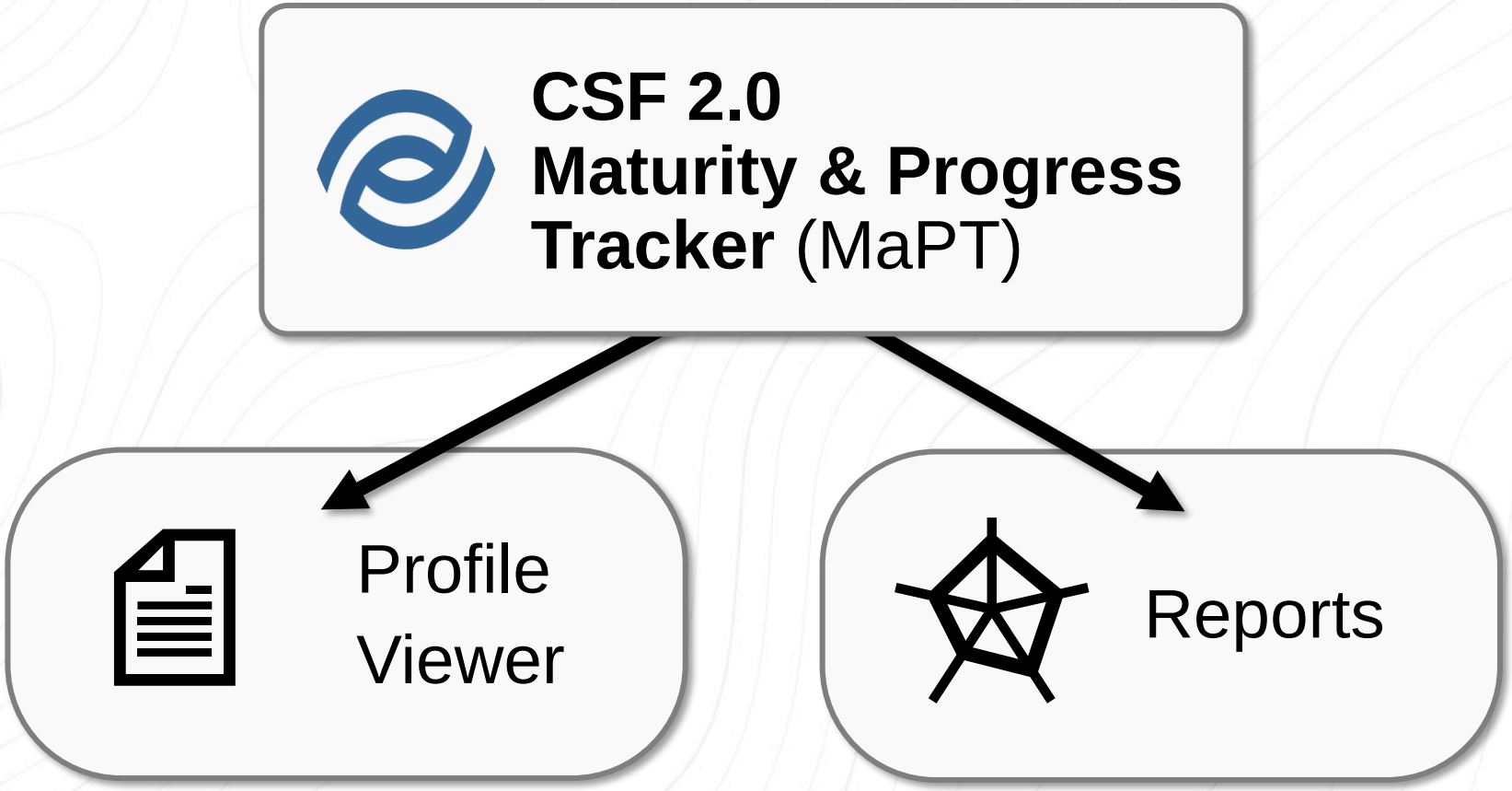
Where should you start?

- Evaluate our gaps
- Prioritize based on risk
- Create a Plan

CSF 2.0 Maturity & Progress Tracker (MaPT)



Build a Roadmap



Where should you start?

Profile Viewer

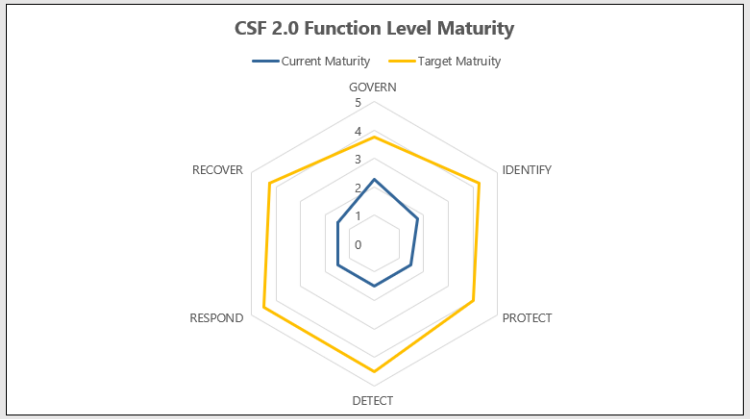
CSF 2.0 Maturity & Progress Tracker (MaPT)					
	Current State		Target State		Progress
Cybersecurity Framework v2.0 Core	Maturity	Description	Maturity	Description	Status
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored					
Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood					
GV.OC-01: **The organizational mission is understood and informs cybersecurity risk management**	4 - Quantitatively Managed	Training programs are developed to educate employees about the significance of the organizational mission and how their roles in cybersecurity contribute to achieving it, thereby embedding the mission into the fabric of the company's security culture.	5 - Optimized	The company regularly conducts cross-departmental meetings to ensure that all team leaders understand the organizational mission and how it impacts their cybersecurity practices, fostering a unified approach to risk management.	Started
GV.OC-02: **Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered**	5 - Optimized	The company establishes a comprehensive communication plan that includes regular engagement sessions with internal and external stakeholders, such as surveys and meetings, to gather insights on their cybersecurity expectations and concerns.	4 - Quantitatively Managed	A dedicated team is tasked with analyzing feedback from stakeholders to ensure that the company's cybersecurity strategies are responsive to their needs, leading to tailored risk management measures that address specific stakeholder concerns.	Started
GV.OC-03: **Legal, regulatory, and contractual requirements regarding**		Cybersecurity policies and procedures are directly aligned with the		Through transparent reporting and updates on cybersecurity initiatives, the company	

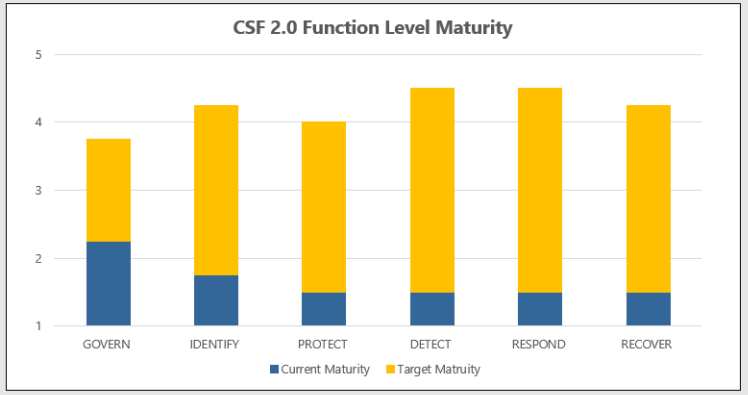
Where should you start?

Maturity Reports

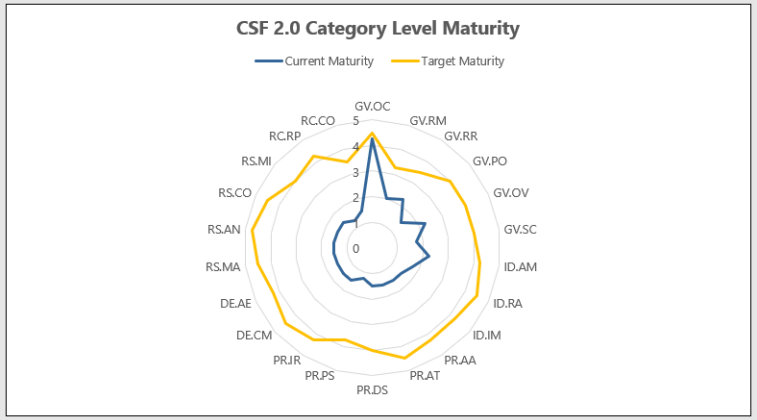
Cybersecurity Framework 2.0 Maturity Reports

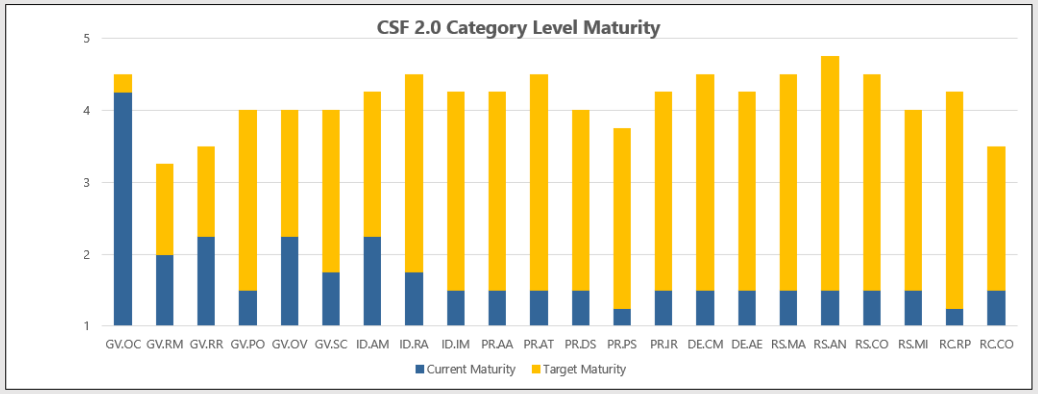
Function Reports





Category Reports



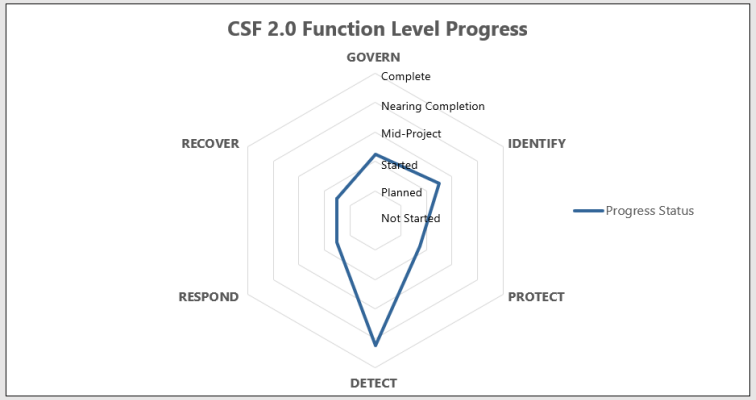


Where should you start?

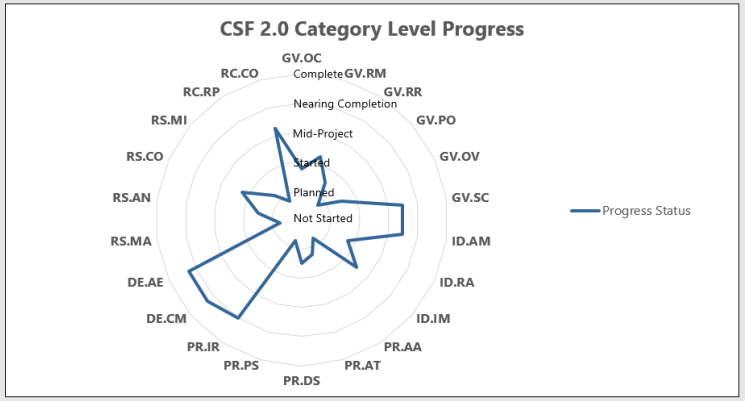
Progress Reports

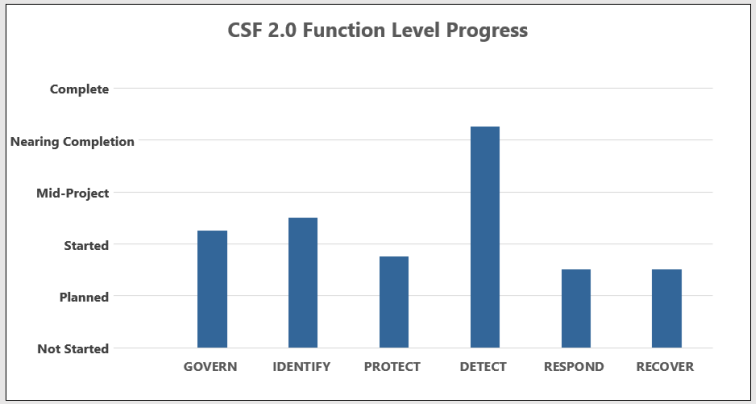
Cybersecurity Framework 2.0 Progress Reports

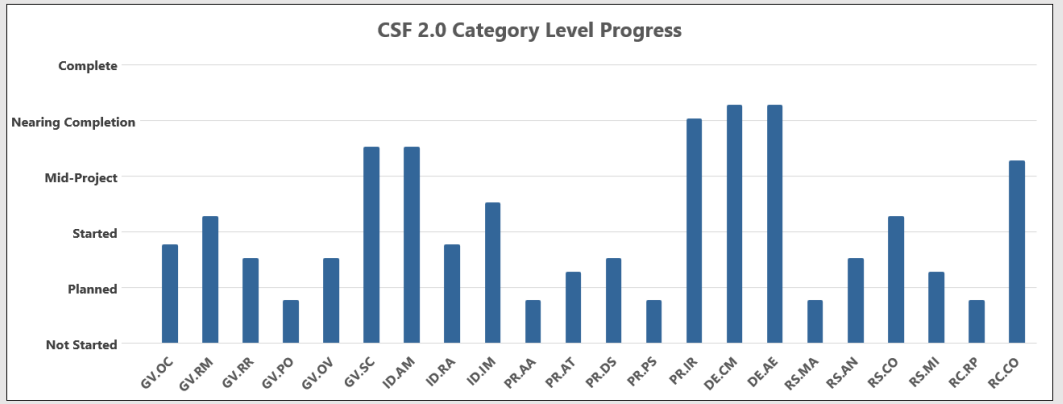
Function Reports



Category Repo







Do I measure up?

Resources Roundup

OPTIC CYBER SOLUTIONS

TRAVELING THROUGH NIST'S

CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES

CSF 2.0

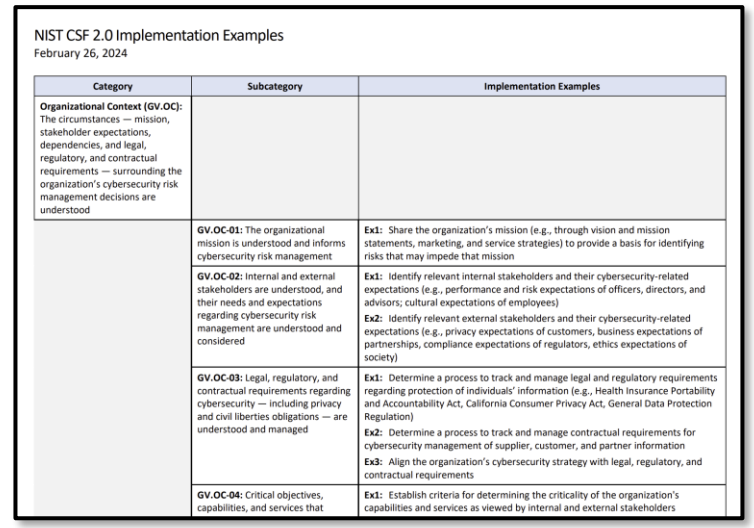
For industry, government, and organizations to reduce cybersecurity risks

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

OPTIC CYBER SOLUTIONS

IMPLEMENTATION EXAMPLES

Review action-oriented steps to help you achieve various outcomes of the subcategories



NIST CSF 2.0 Implementation Examples
February 26, 2024

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	**Ex1:** Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2:** Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3:** Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements
	GV.OC-04: Critical objectives, capabilities, and services that	**Ex1:** Establish criteria for determining the criticality of the organization's capabilities and services as viewed by internal and external stakeholders

QUICK START GUIDES

For organizations with specific common goals

MAPPINGS

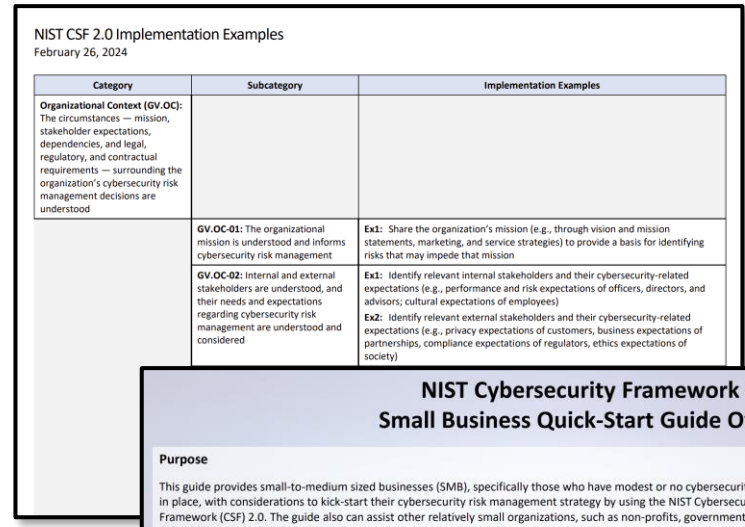
See how NIST's work interrelates and shares themes

OPTIC CYBER SOLUTIONS

OPTIC CYBER SOLUTIONS

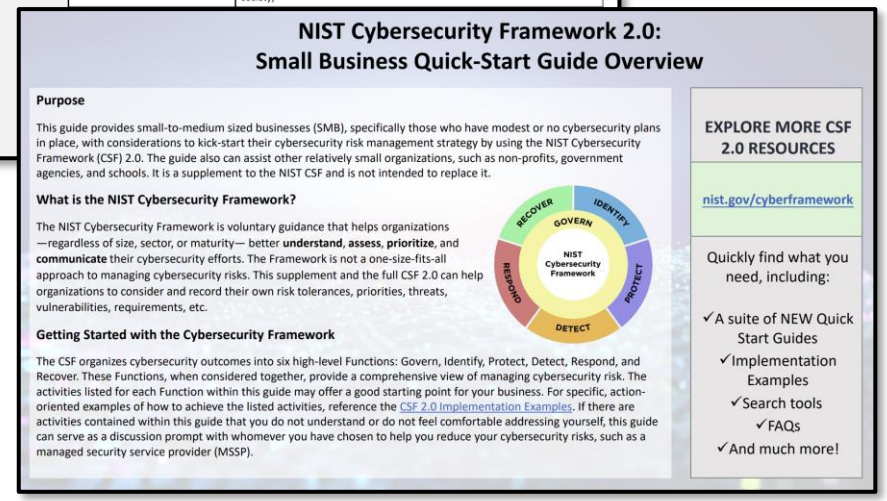
IMPLEMENTATION EXAMPLES

Review action-oriented steps to help you achieve various outcomes of the subcategories



NIST CSF 2.0 Implementation Examples
February 26, 2024

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)



NIST Cybersecurity Framework 2.0:
Small Business Quick-Start Guide Overview

Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance that helps organizations —regardless of size, sector, or maturity— better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

Getting Started with the Cybersecurity Framework

The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. These Functions, when considered together, provide a comprehensive view of managing cybersecurity risk. The activities listed for each Function within this guide may offer a good starting point for your business. For specific, action-oriented examples of how to achieve the listed activities, reference the CSF 2.0 Implementation Examples. If there are activities contained within this guide that you do not understand or do not feel comfortable addressing yourself, this guide can serve as a discussion prompt with whomever you have chosen to help you reduce your cybersecurity risks, such as a managed security service provider (MSSP).

EXPLORE MORE CSF 2.0 RESOURCES

nist.gov/cyberframework

Quickly find what you need, including:

- ✓A suite of NEW Quick Start Guides
- ✓Implementation Examples
- ✓Search tools
- ✓FAQs
- ✓And much more!

QUICK START GUIDES

For organizations with specific common goals

MAPPINGS

See how NIST's work interrelates and shares themes

OPTIC CYBER SOLUTIONS

OPTIC CYBER SOLUTIONS

IMPLEMENTATION EXAMPLES

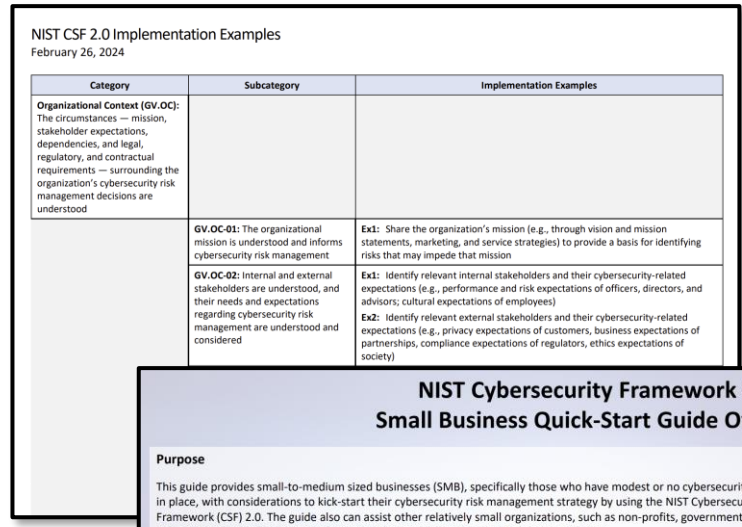
Review action-oriented steps to help you achieve various outcomes of the subcategories

QUICK START GUIDES

For organizations with specific common goals

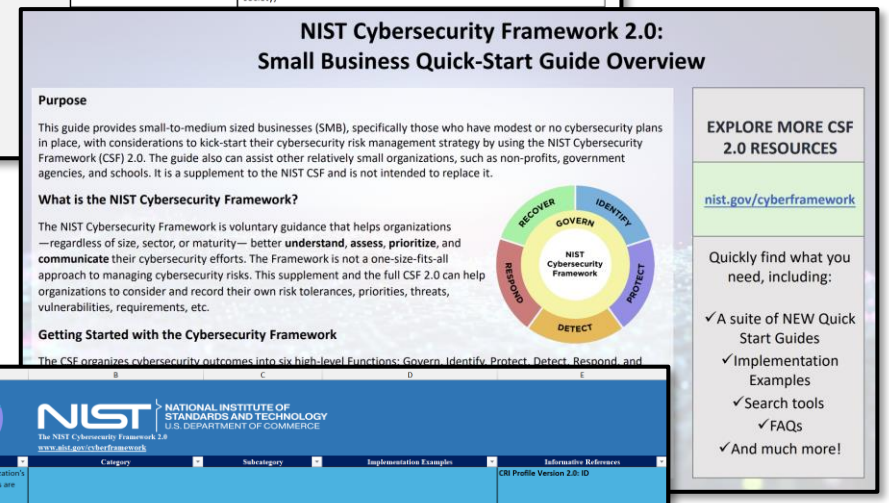
MAPPINGS

See how NIST's work interrelates and shares themes



NIST CSF 2.0 Implementation Examples
February 26, 2024

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)



NIST Cybersecurity Framework 2.0:
Small Business Quick-Start Guide Overview

Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance that helps organizations —regardless of size, sector, or maturity— better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

Getting Started with the Cybersecurity Framework

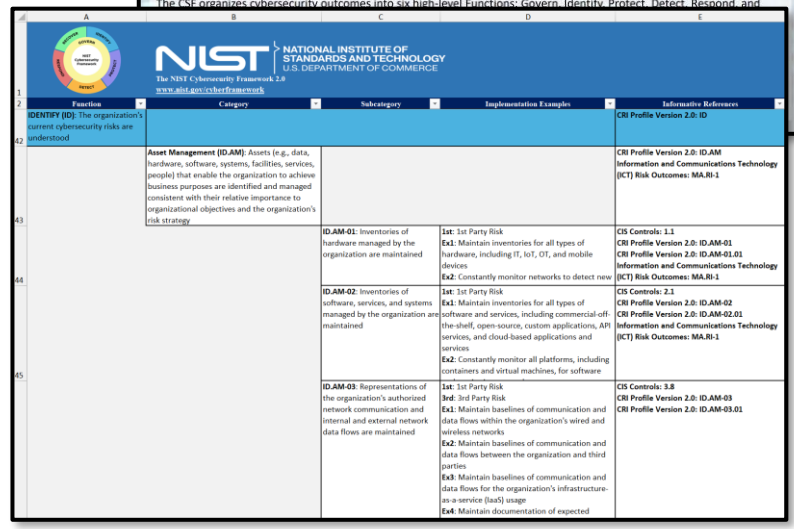
The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and

EXPLORE MORE CSF 2.0 RESOURCES

nist.gov/cyberframework

Quickly find what you need, including:

- ✓A suite of NEW Quick Start Guides
- ✓Implementation Examples
- ✓Search tools
- ✓FAQs
- ✓And much more!



NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE
The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples	Informative References
IDENTIFY (ID): The organization's current cybersecurity risks are understood				**CRI Profile Version 2.0: ID**
	Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy			**CRI Profile Version 2.0: ID.AM** **Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1**
		ID.AM-01: Inventories of hardware managed by the organization are maintained	**1st:** 1st Party Risk **Ex1:** Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2:** Constantly monitor networks to detect new	**CIS Controls: 1.1** **CRI Profile Version 2.0: ID.AM-01** **CRI Profile Version 2.0: ID.AM-01.01** **Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1**
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**1st:** 1st Party Risk **Ex1:** Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2:** Constantly monitor all platforms, including containers and virtual machines, for software	**CIS Controls: 2.1** **CRI Profile Version 2.0: ID.AM-02** **CRI Profile Version 2.0: ID.AM-02.01** **Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1**
		ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	**1st:** 1st Party Risk **3rd:** 3rd Party Risk **Ex1:** Maintain baselines of communication and data flows within the organization's wired and wireless networks **Ex2:** Maintain baselines of communication and data flows between the organization and third parties **Ex3:** Maintain baselines of communication and data flows for the organization's infrastructure-as-a-service (IaaS) usage **Ex4:** Maintain documentation of expected	**CIS Controls: 3.8** **CRI Profile Version 2.0: ID.AM-03** **CRI Profile Version 2.0: ID.AM-03.01**

What do I do now?

Next Steps

- **Map the Changes**
  - Use the Workbook to evaluate the changes & what they mean to you
- **Identify Any Gaps**
  - Fill out MaPT to record what you're doing today & where you need to be
- **Build a Roadmap**
  - Use the information captured in MaPT to build out a plan!

Resources

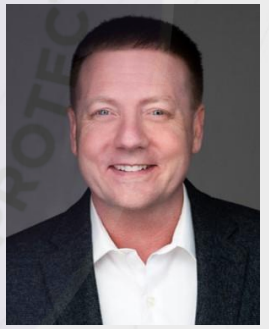
Optic

- InfoSec World Workshop Handouts
  - https://www.opticcyber.com/resources/CSF2Handouts.html
- Maturity and Progress Tracker (MaPT)
  - https://www.opticcyber.com/resources.html
- Cybersecurity Framework 2.0 Profile Template
  - https://www.opticcyber.com/resources.html

NIST

- The NIST Cybersecurity Framework (CSF) 2.0
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- CSF Website – Resources
  - https://www.nist.gov/cyberframework

Kelly Hood
Cybersecurity Engineer
Info@OpticCyber.com



Tom Conkle
Cybersecurity Engineer
Info@OpticCyber.com

THANK YOU!