

# Deep Dive into the NIST Cybersecurity Framework 2.0

Kelly Hood & Tom Conkle



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



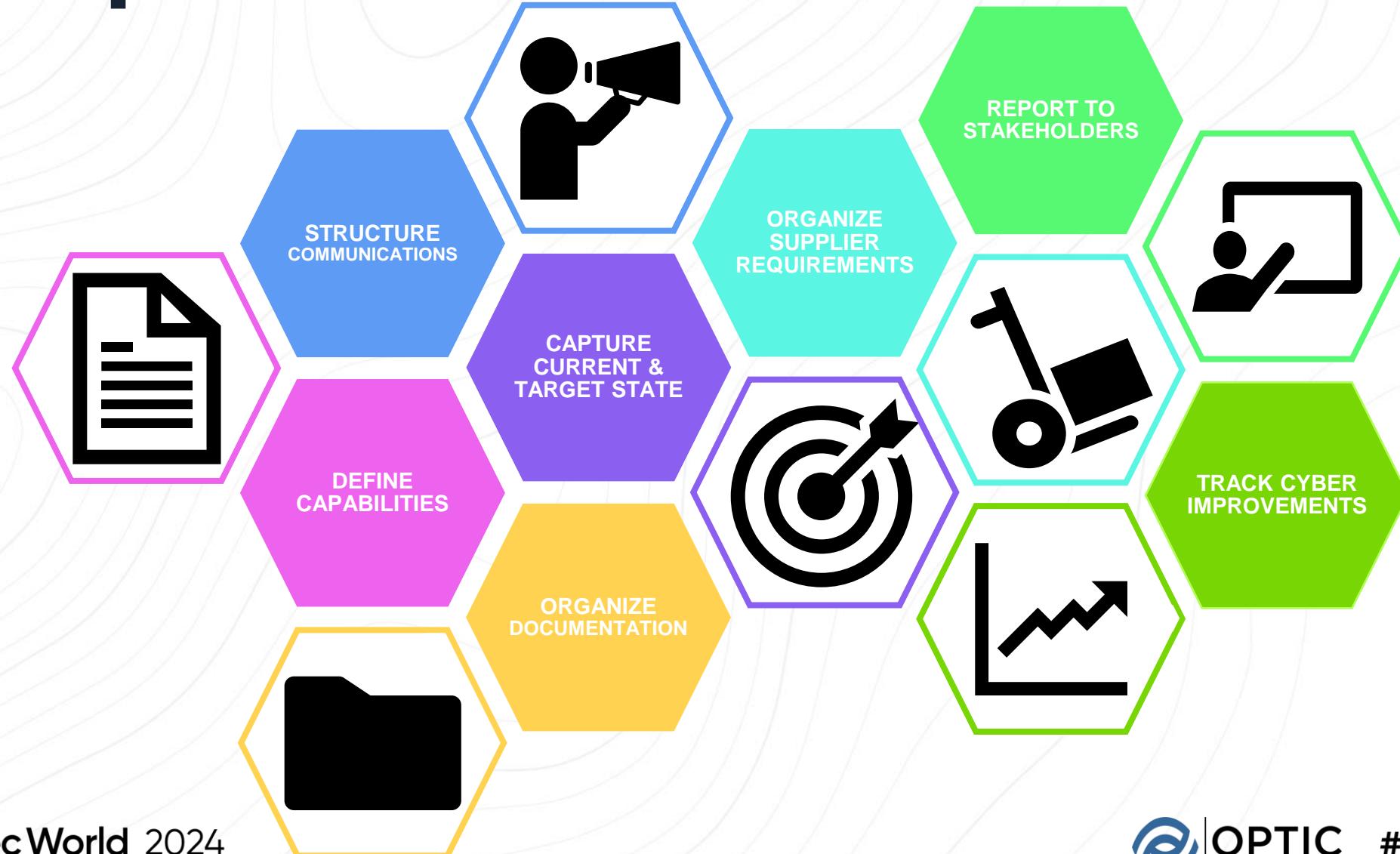
**Tom Conkle**  
Cybersecurity Engineer  
Optic Cyber Solutions

# Introductions

- Name
  - Role
  - Company / Industry
- 
- Why are you here?
  - What are you looking to get out of this session?

# 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

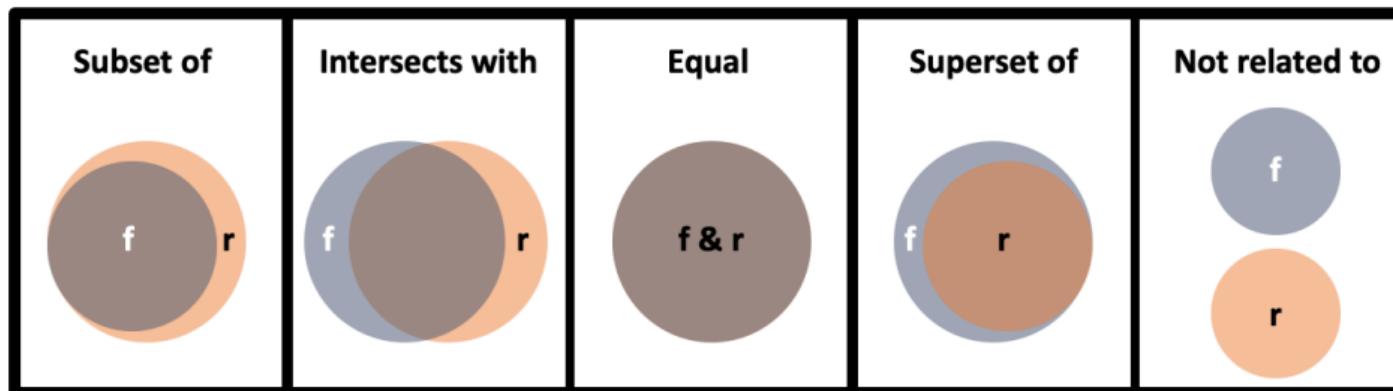


Figure 1: Relationship Types

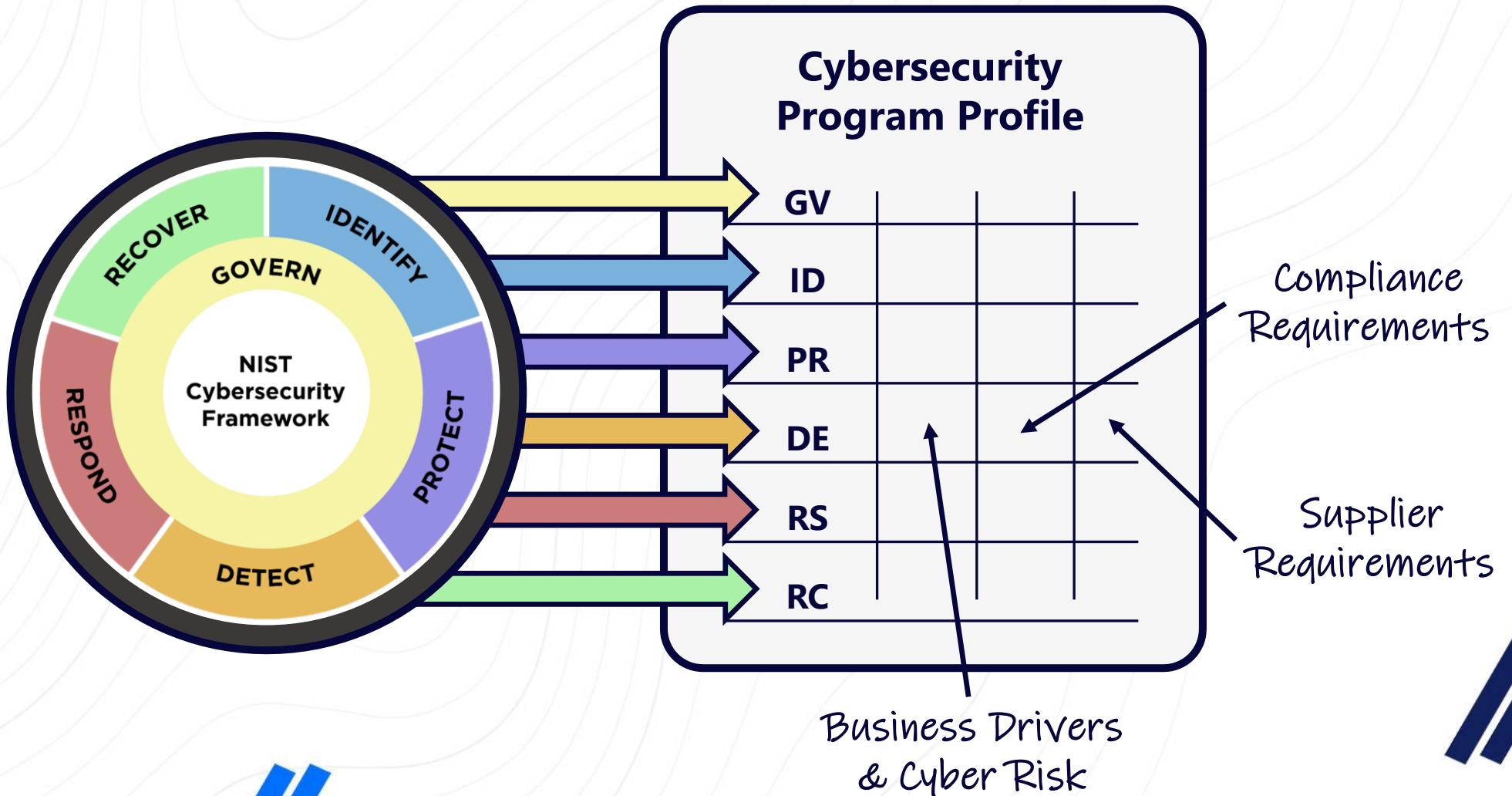
<https://csrc.nist.gov/Projects/olir>

**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

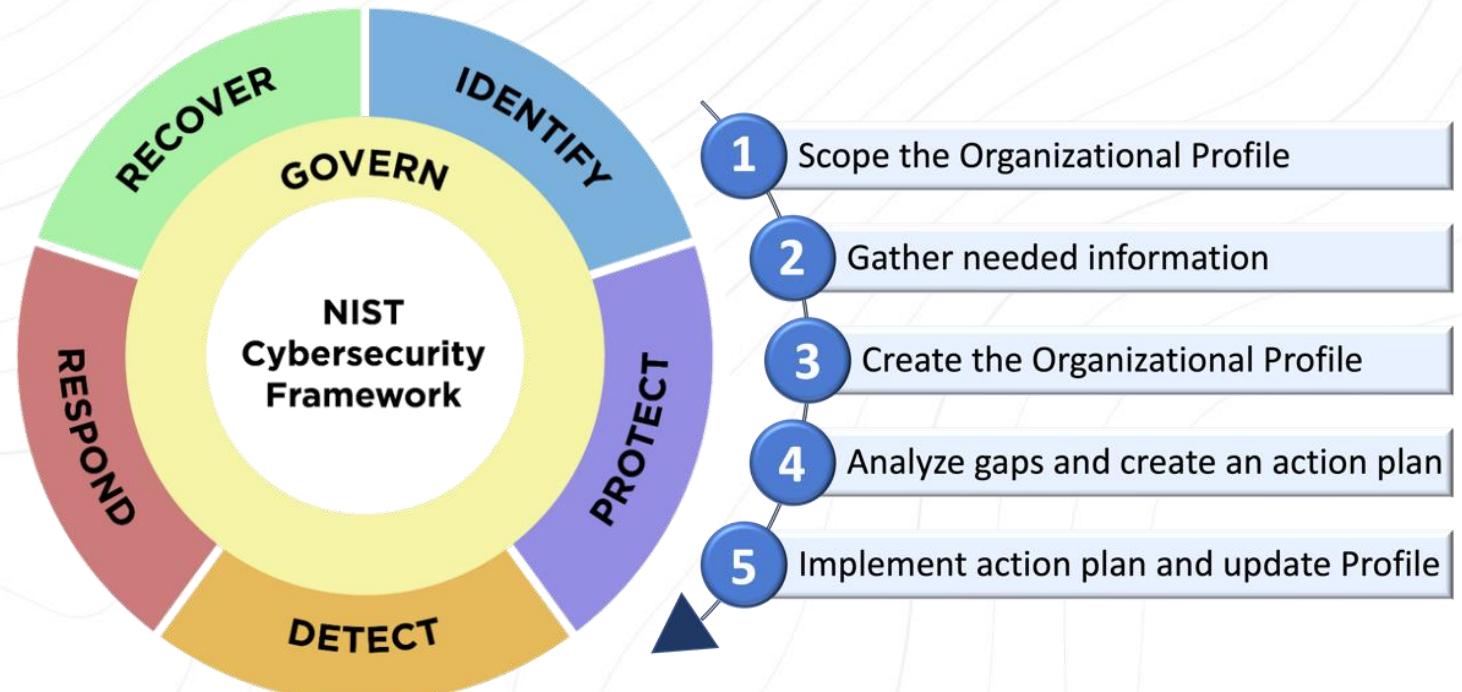
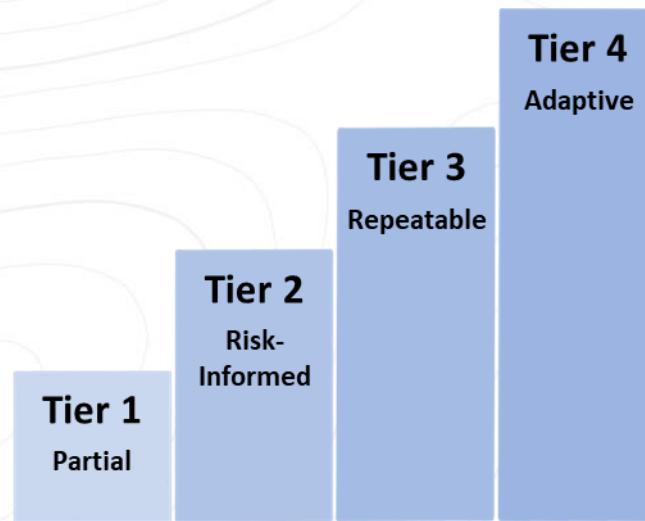
# Develop a common lexicon for you & your suppliers



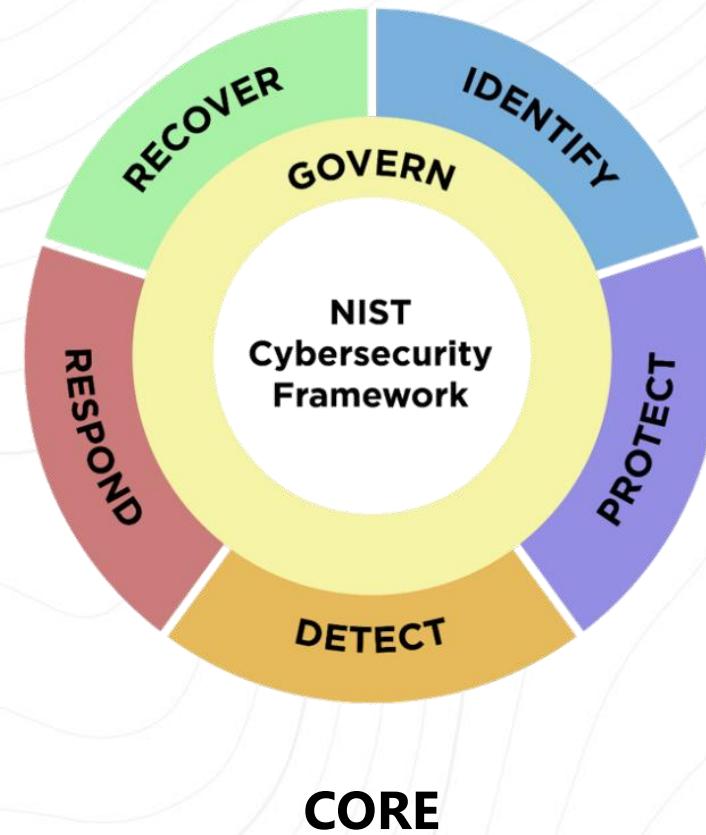


# What is it?

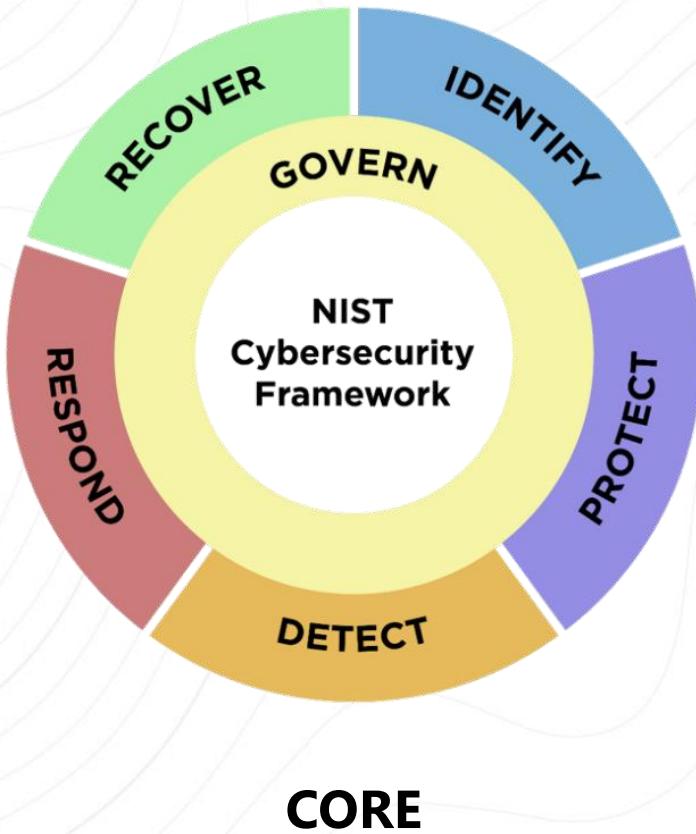
# NIST Cybersecurity Framework (CSF) 2.0



# Cybersecurity Framework 2.0 - Core



# Cybersecurity Framework 2.0 - Core



FUNCTIONS

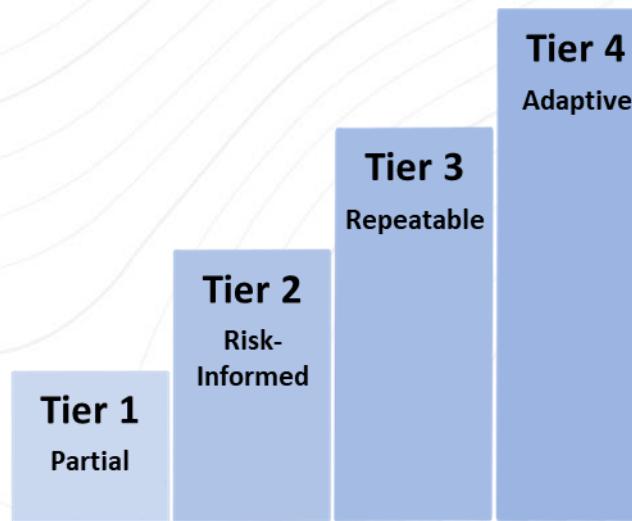


CATEGORIES



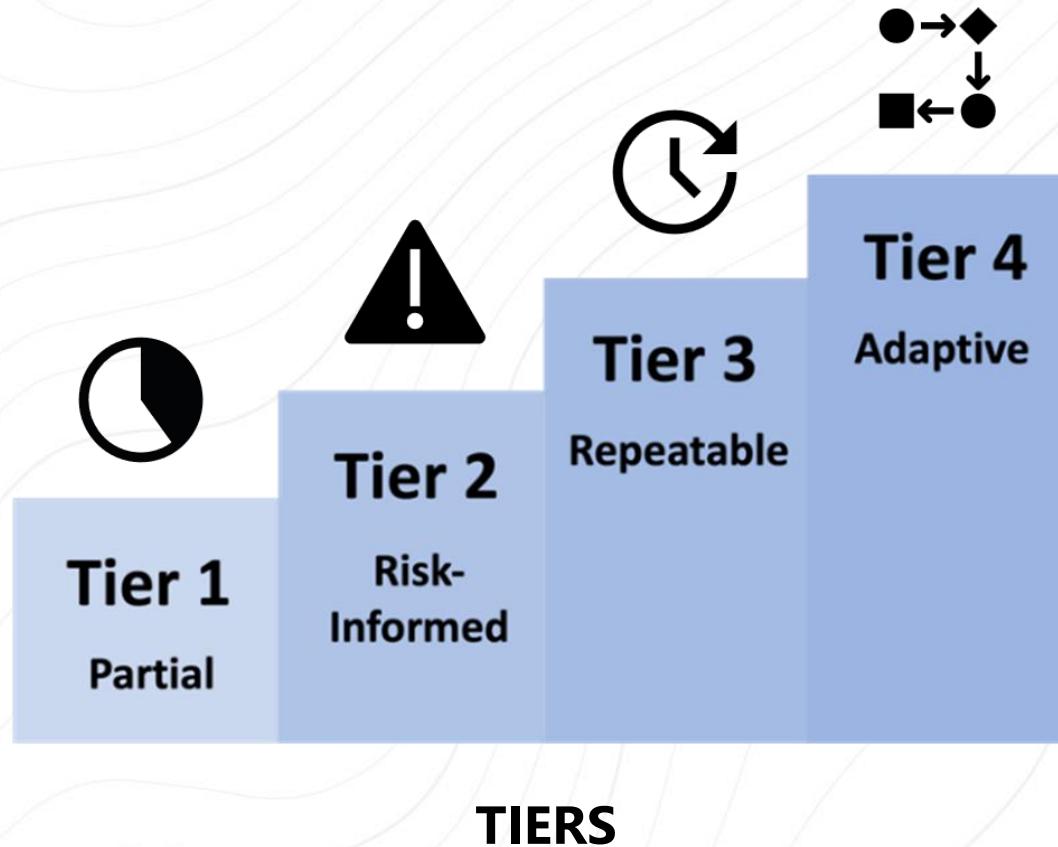
SUBCATEGORIES

# Cybersecurity Framework 2.0 - Tiers

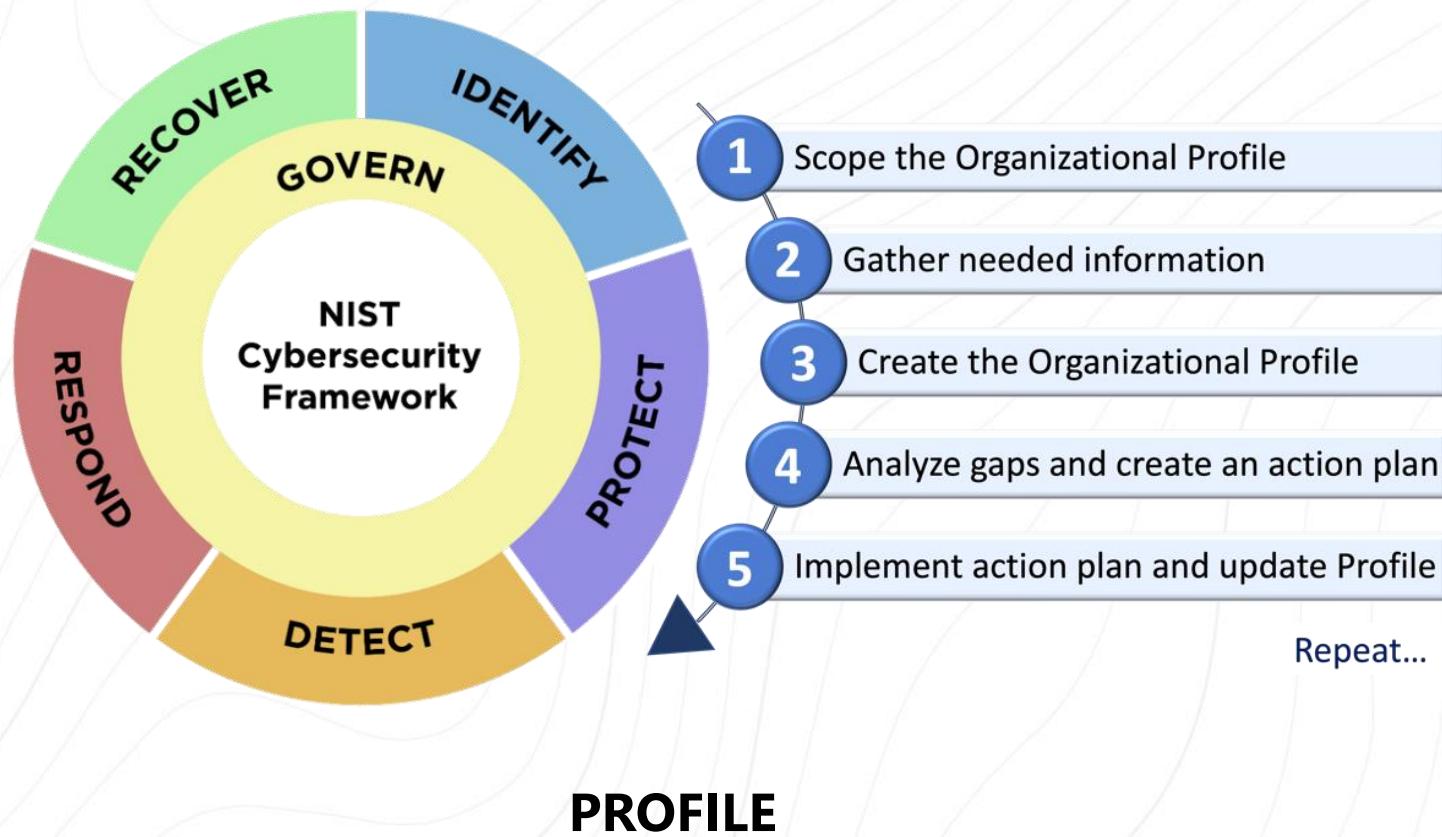


TIERS

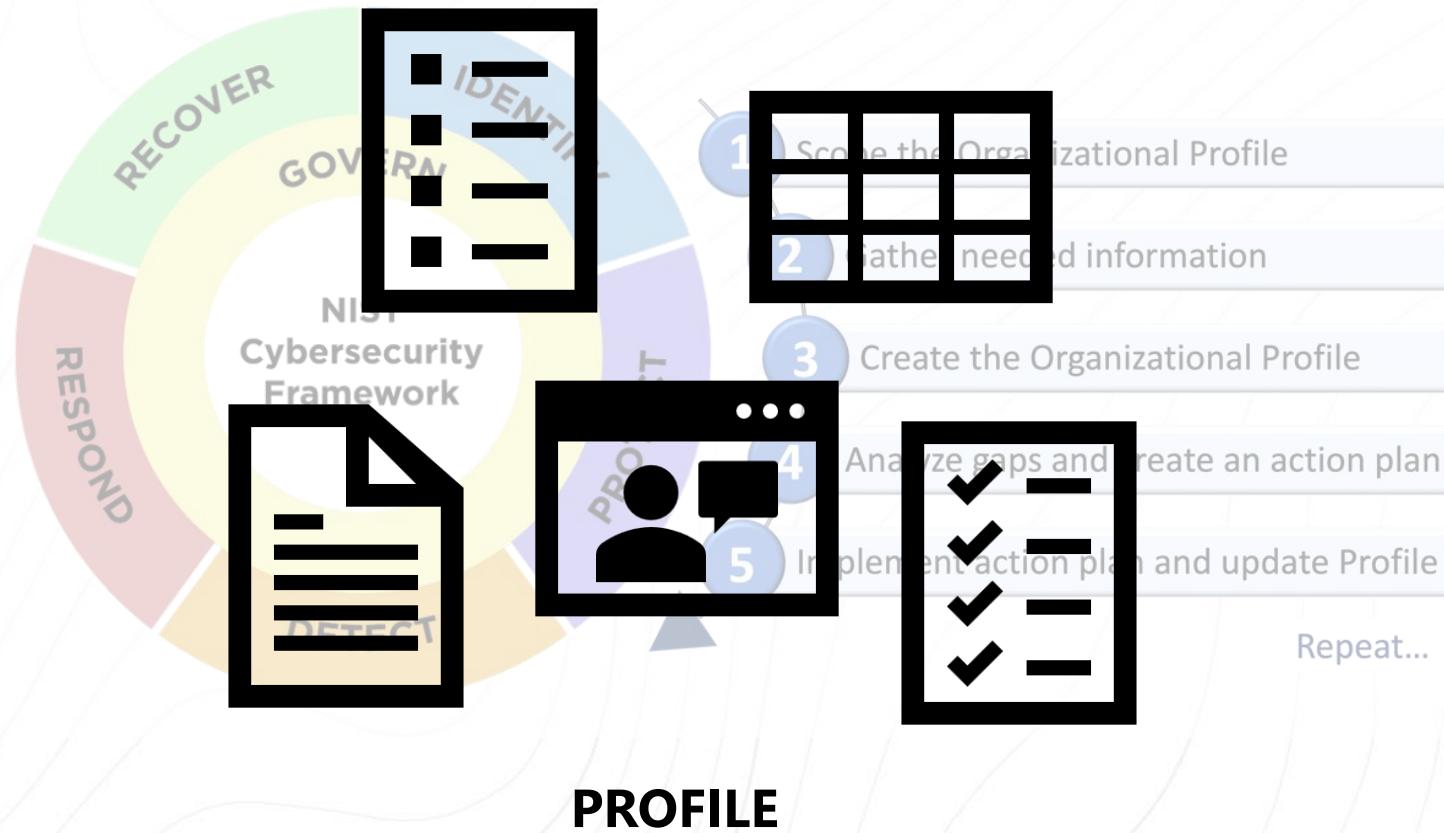
# Cybersecurity Framework 2.0 - Tiers



# Cybersecurity Framework 2.0 - Profiles



# Cybersecurity Framework 2.0 - Profiles





# 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
RC	Recover	Improvements	RS.IM
		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
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	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
	Identity Management, Authentication, and Access Control	PR-AA
	Awareness and Training	PR.AT
Protect (PR)	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	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
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
	Identity Management, Authentication, and Access Control	PR-AA
Protect (PR)	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
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	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
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
	Identity Management, Authentication, and Access Control	PR-AA
Protect (PR)	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
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	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
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	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
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	Incident Recovery Communication	RC.CO

CSF v2.0

# Twelve Categories were removed (or realigned)

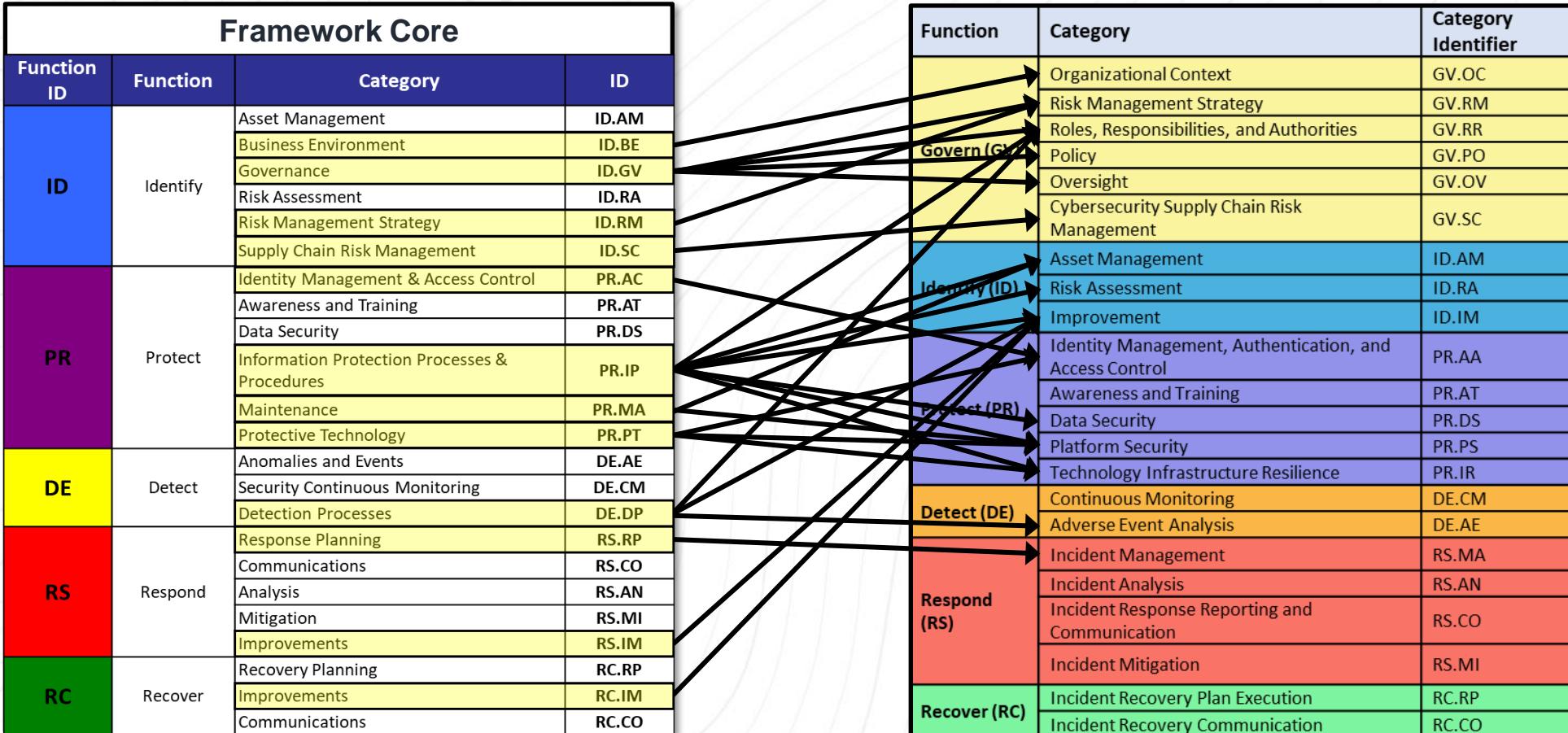
Framework Core			
Function ID	Function	Category	ID
ID	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PR	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	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
	Identity Management, Authentication, and Access Control	PR-AA
Protect (PR)	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Detect (DE)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Respond (RS)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO
Recover (RC)		

CSF v2.0

# Twelve Categories were removed (or realigned)



CSF v1.1

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
	Identity Management, Authentication & Access Control	PR-AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
Protect (PR)	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
	Incident Management	RS.MA
	Incident Analysis	RS.AN
Respond (RS)	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO
Recover (RC)		

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
	Identity Management, Authentication & Access Control	PR-AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
Protect (PR)	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
	Incident Management	RS.MA
	Incident Analysis	RS.AN
Respond (RS)	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO
Recover (RC)		

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
	Continuous Monitoring	DE.CM
Detect (DE)	Adverse Event Analysis	DE.AE
	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
Respond (RS)	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO
Recover (RC)		

CSF v2.0

# Eleven new Categories were added (or realigned)

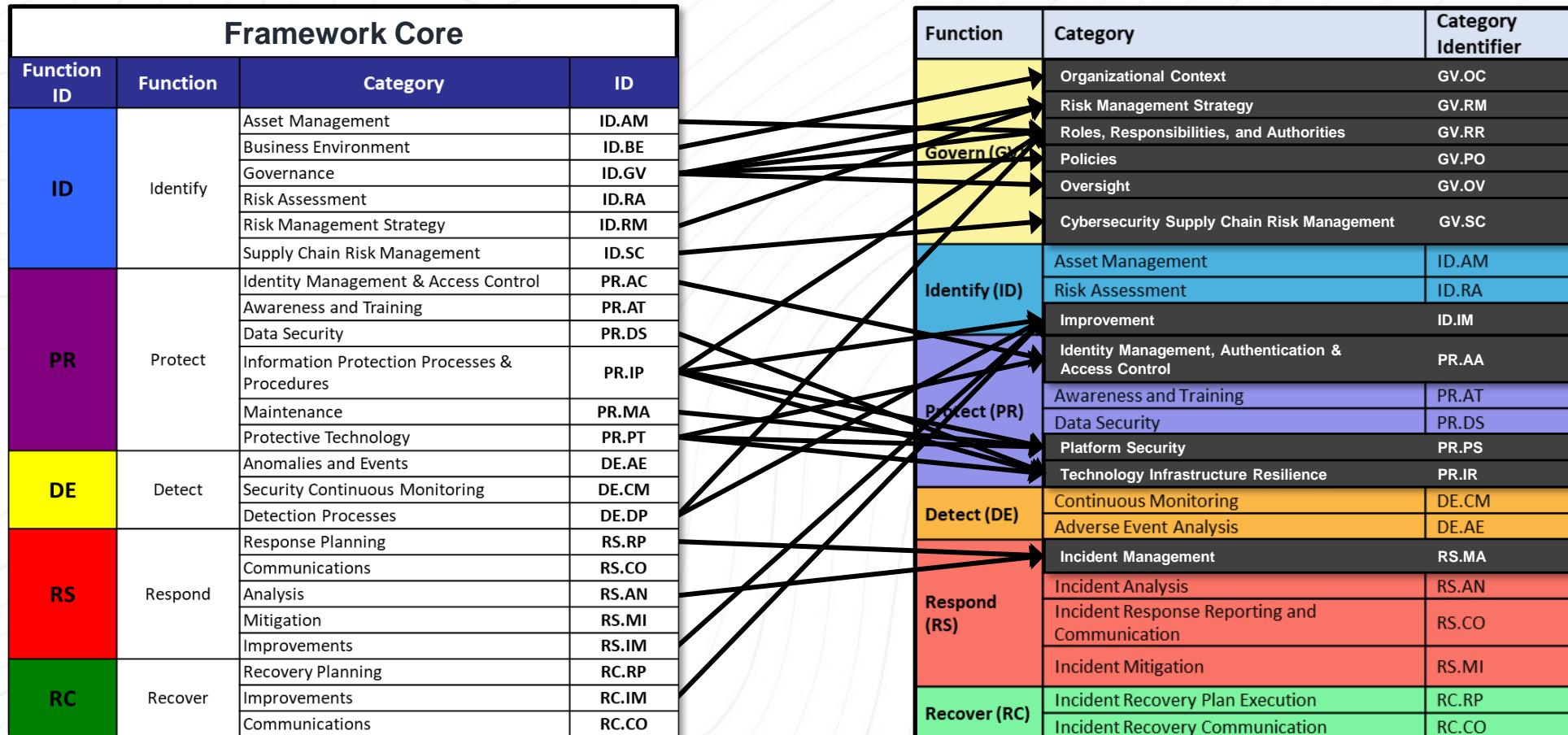
Framework Core			
Function ID	Function	Category	ID
ID	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PR	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	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

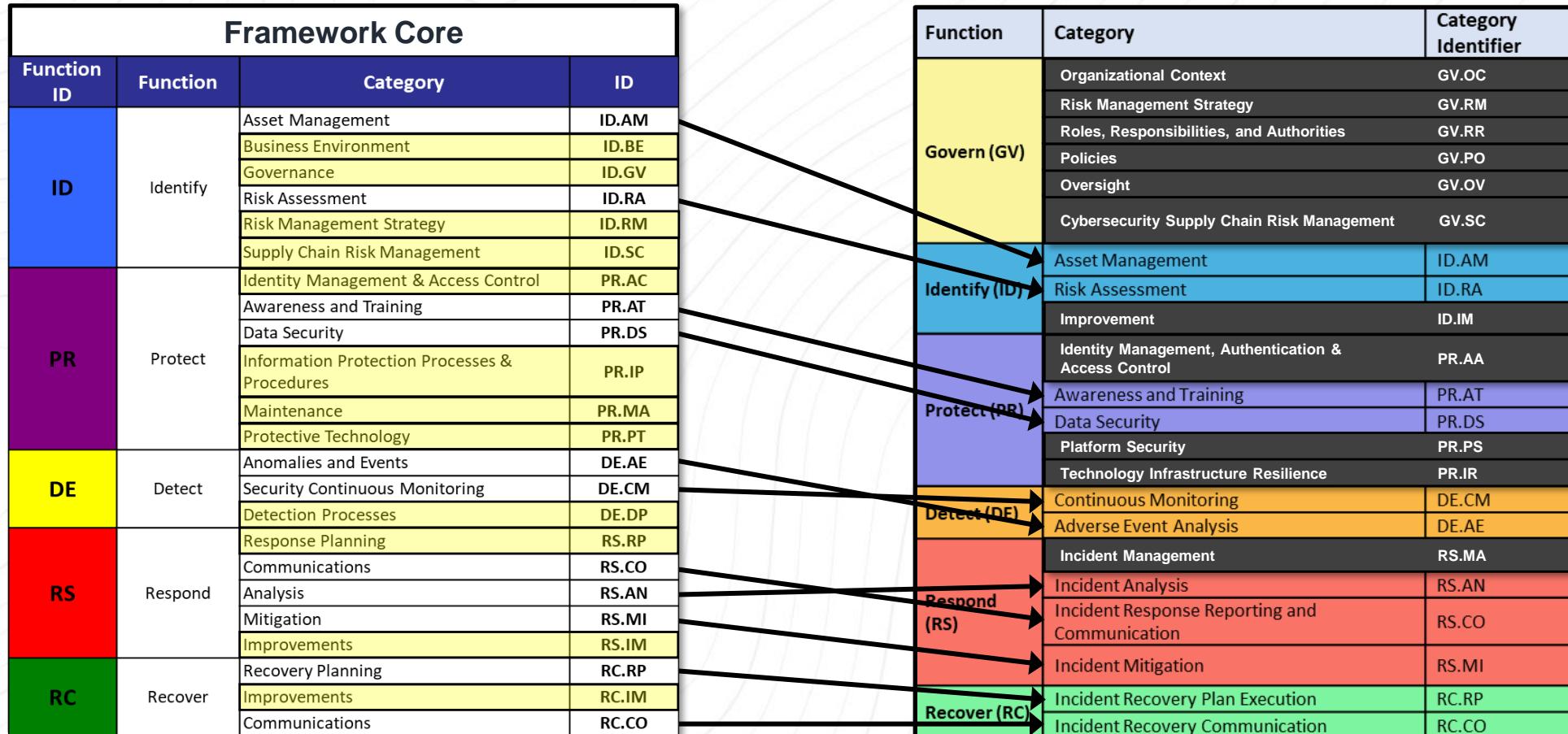
# Eleven new Categories were added (or realigned)



CSF v1.1

CSF v2.0

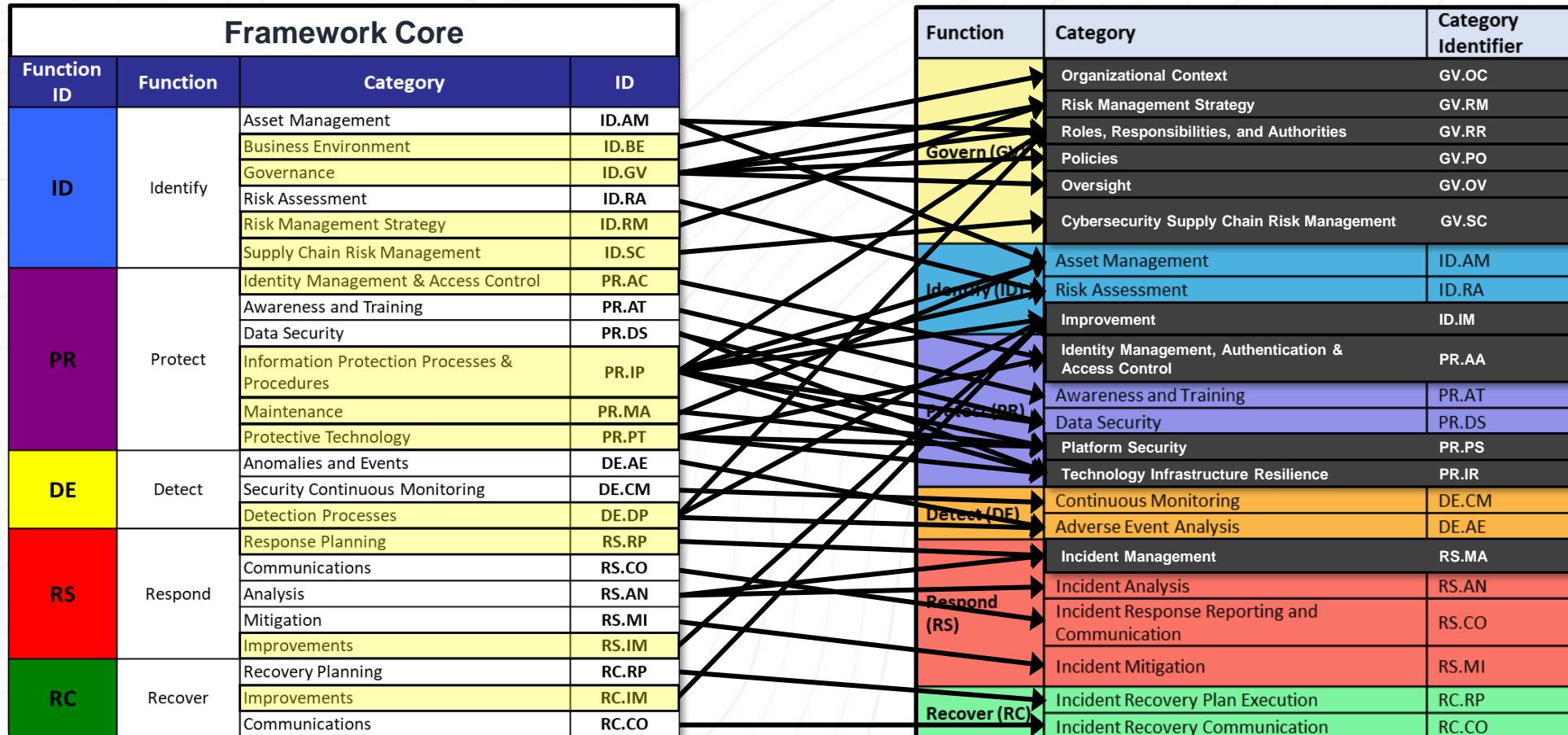
# Many areas stayed the same (or very similar)



CSF v1.1

CSF v2.0

# NIST Cybersecurity Framework v2.0 Summary of Changes



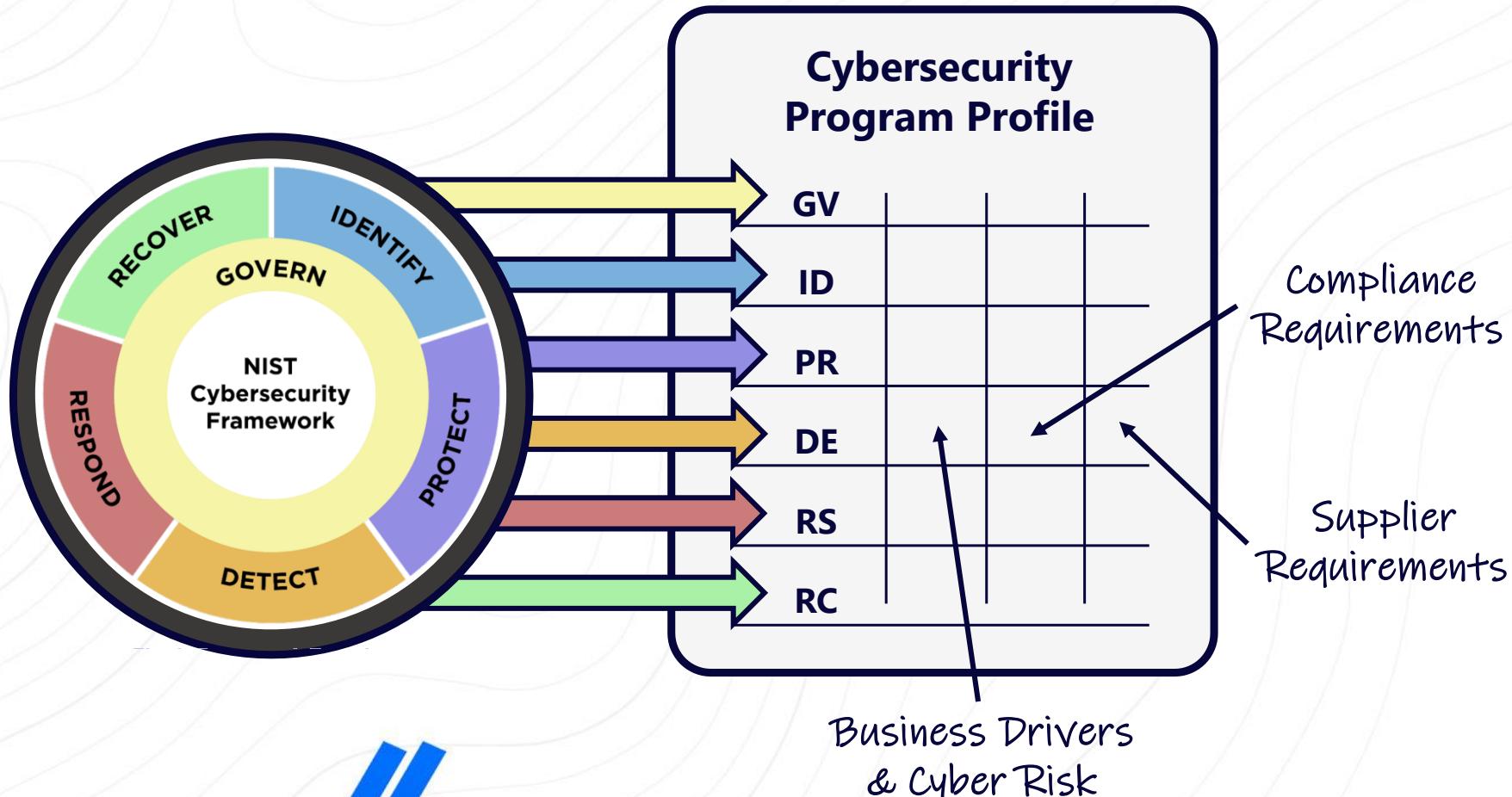
CSF v1.1

CSF v2.0



# How do I use it?

# Using the Cybersecurity Framework enables you to streamline requirements & capabilities



# Steps for Creating and Using Profiles

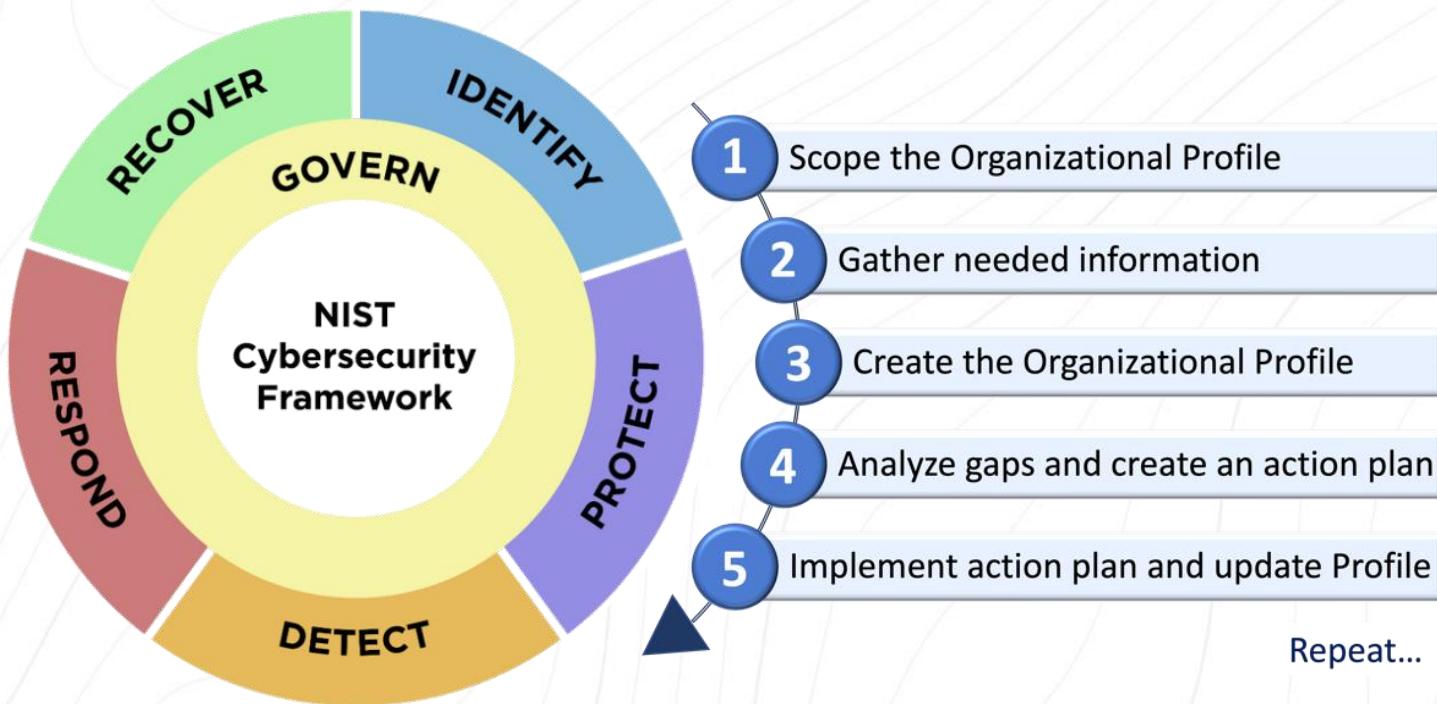


Figure 3: Steps for creating and using a CSF Organizational Profile

# Step 1: Scope the Organizational Profile

What are you evaluating?

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

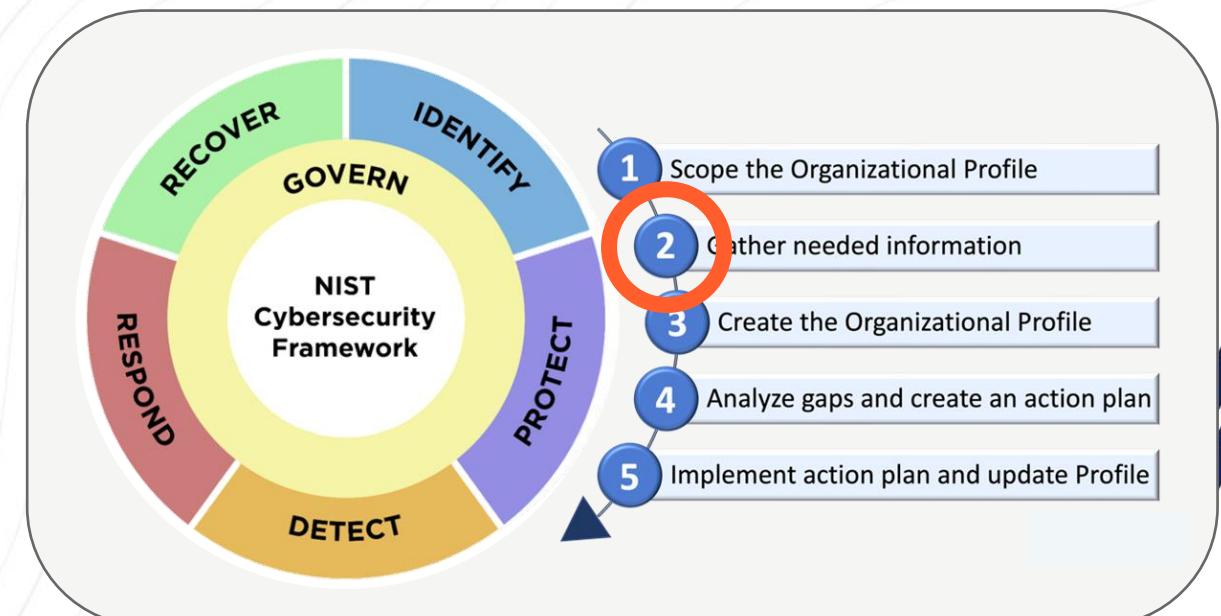




## Step 2: Gather Needed Information

What do you already have?

- Policies
- Standards
- Procedures

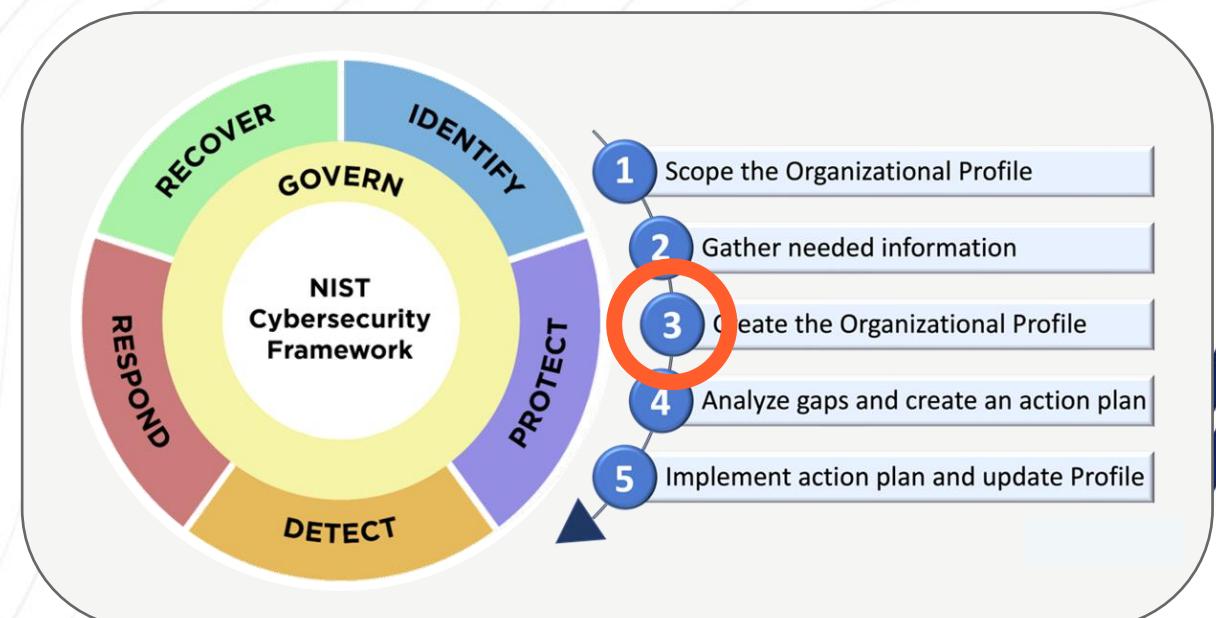




## Step 3: Create the Organizational Profile

What is your Profile going to look like?

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





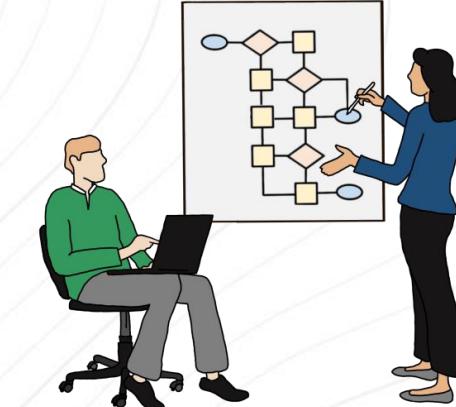
# Profiles help to define & streamline cybersecurity objectives

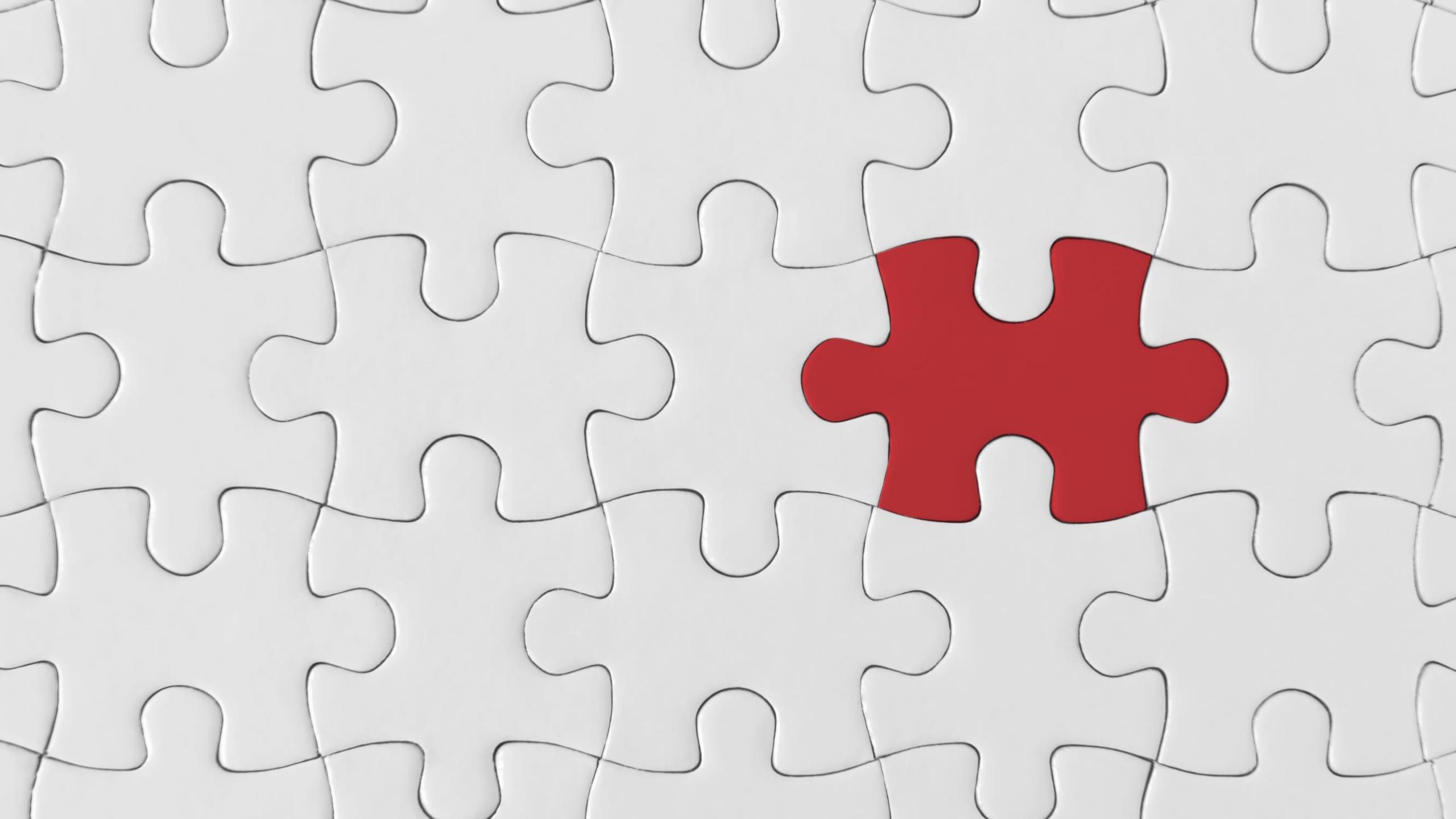
NIST Cybersecurity Framework 2.0	Business Drivers & Cyber Risk	Compliance Requirements		Supplier Requirements	Target Capability
		ISO 27001	CIRCIA		
RS.CO-02: Internal and external <b>stakeholders are notified of incidents</b>	<b>Internal</b> business leaders are notified of cyber incidents.  Failure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

## Step 4: Analyze Gaps and Create an Action Plan

Compare your Current and Target Profiles

- Identify key gaps
- Prioritize resources
- Create a roadmap



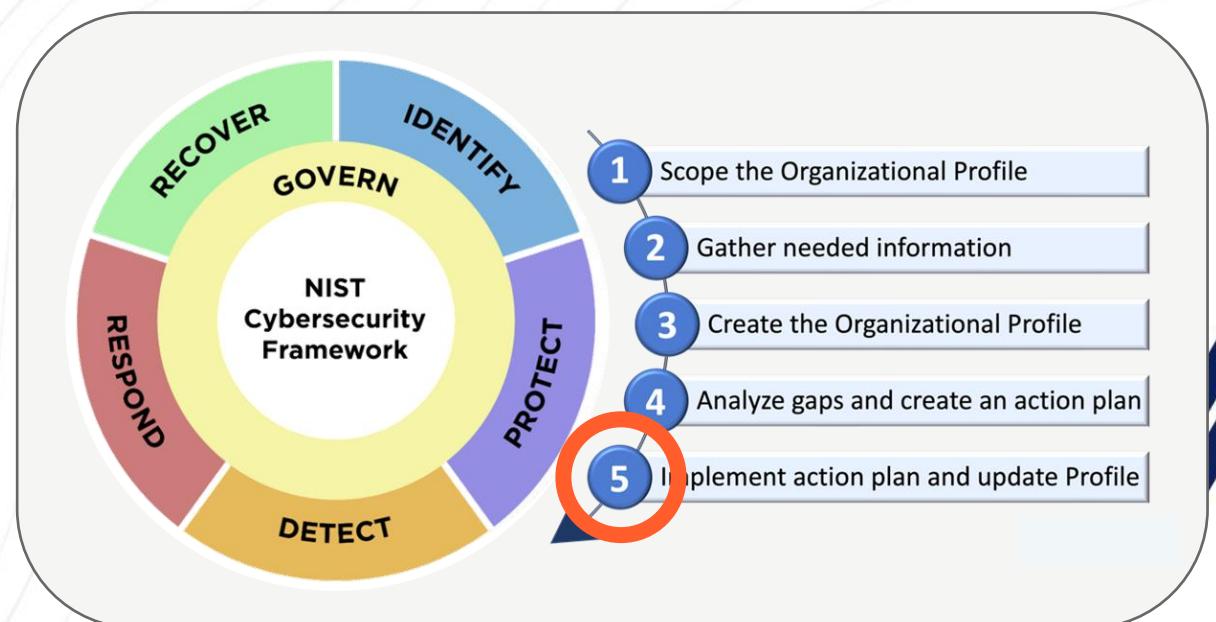


# Gaps in the current capabilities can be identified through by evaluating your Profile

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

# Step 5: Implement Action Plan and Update Profile

Go forth and conquer!





# Steps for Creating and Using Profiles

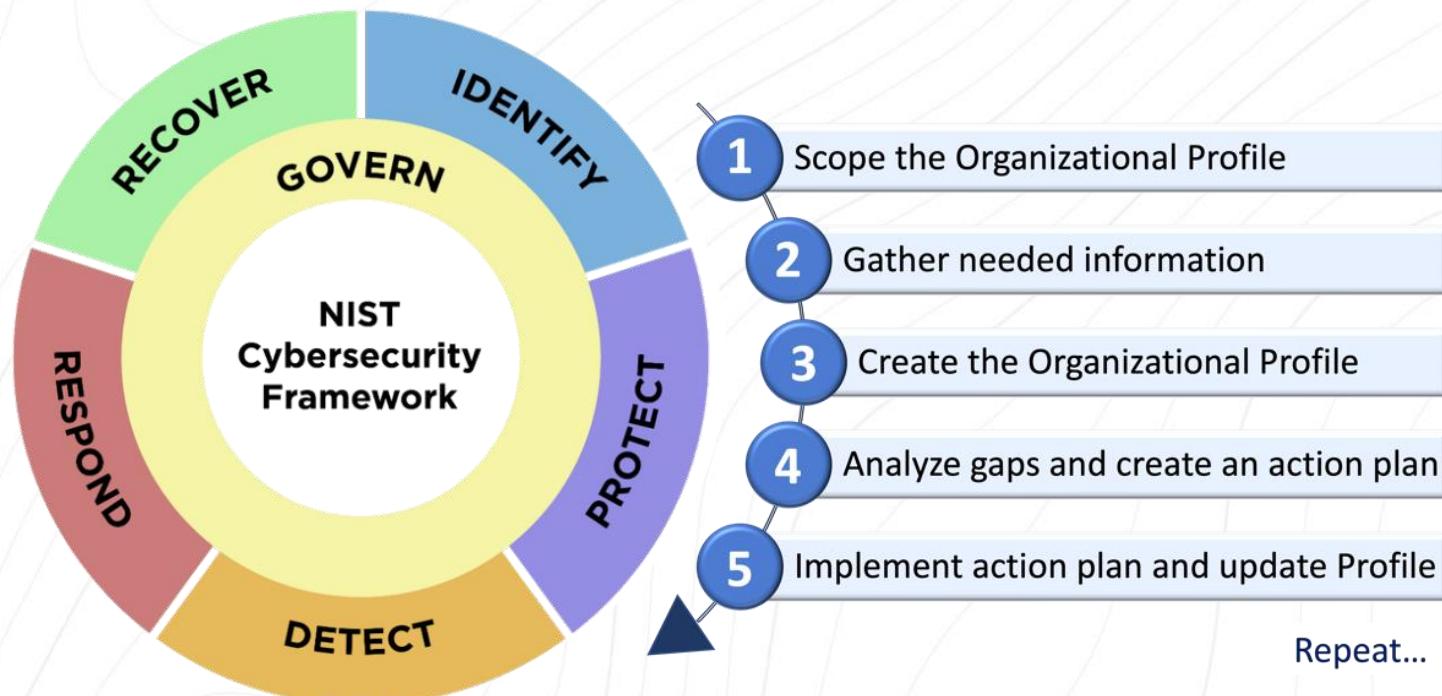
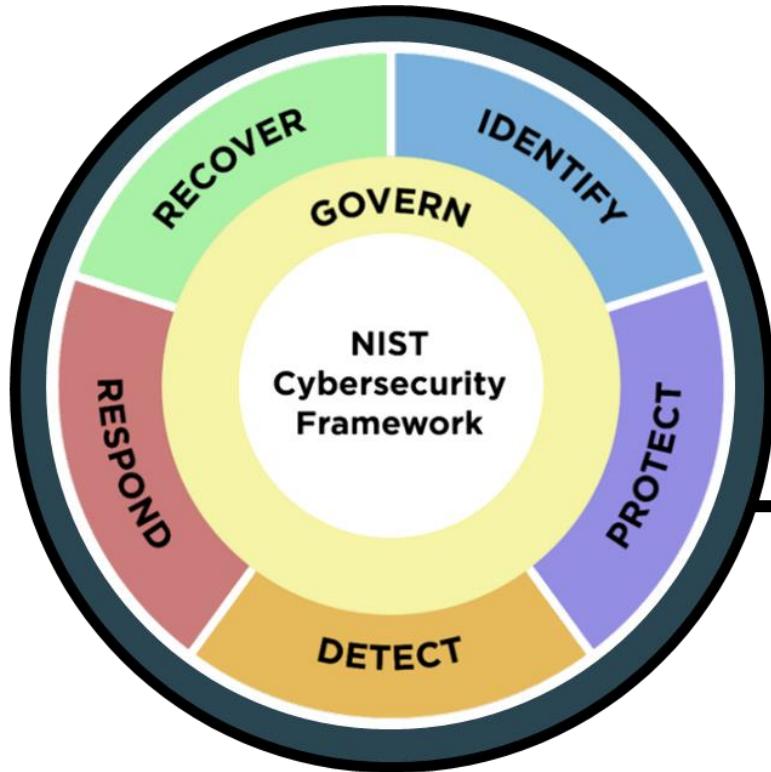


Figure 3: Steps for creating and using a CSF Organizational Profile

# What should I know?



# NIST Cybersecurity Framework v2.0

## Workbook

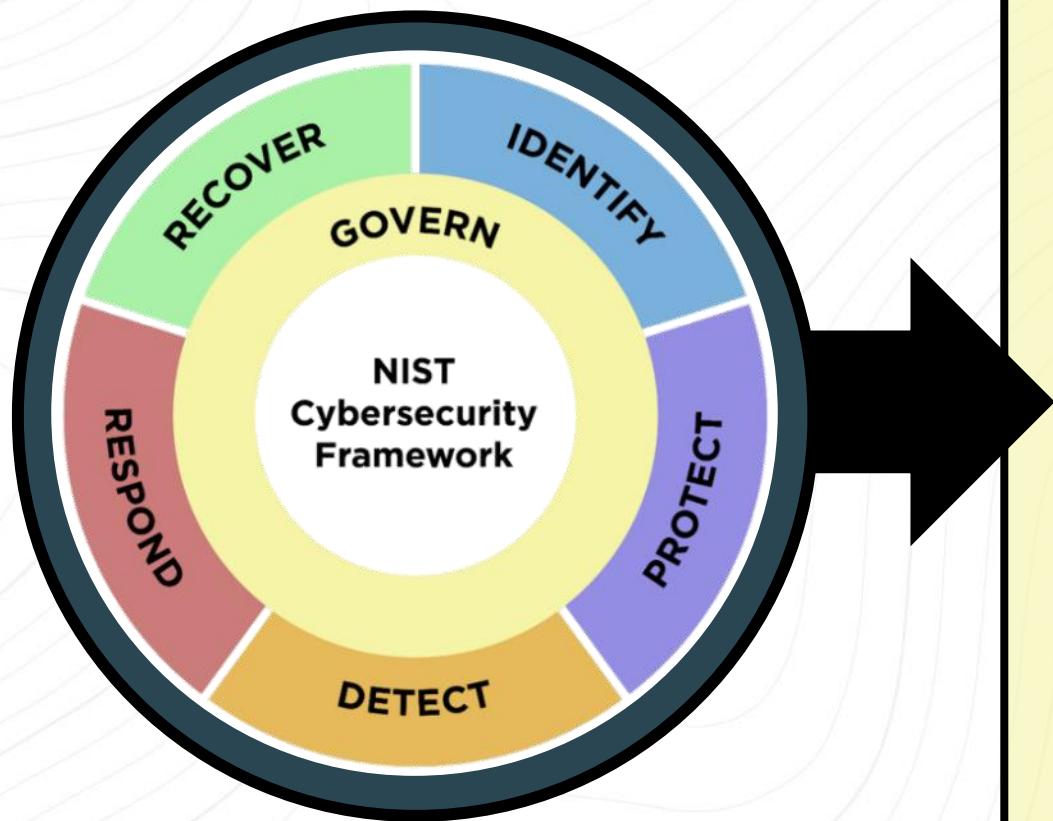
InfoSec World Workshop Handouts

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

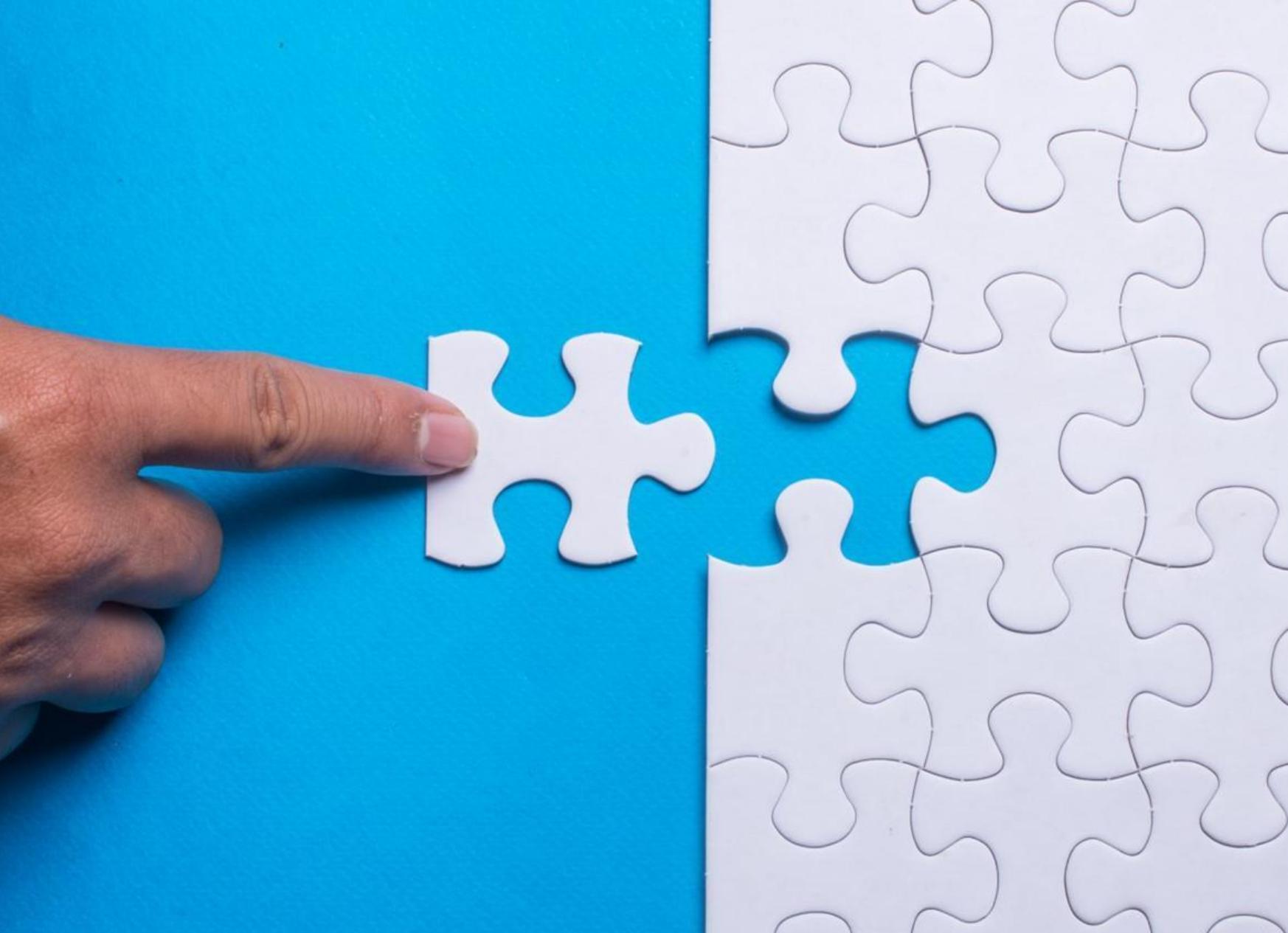
Prepared by:



# What's included in the new Govern Function?



# ORGANIZATIONAL CONTEXT (GV.OC)



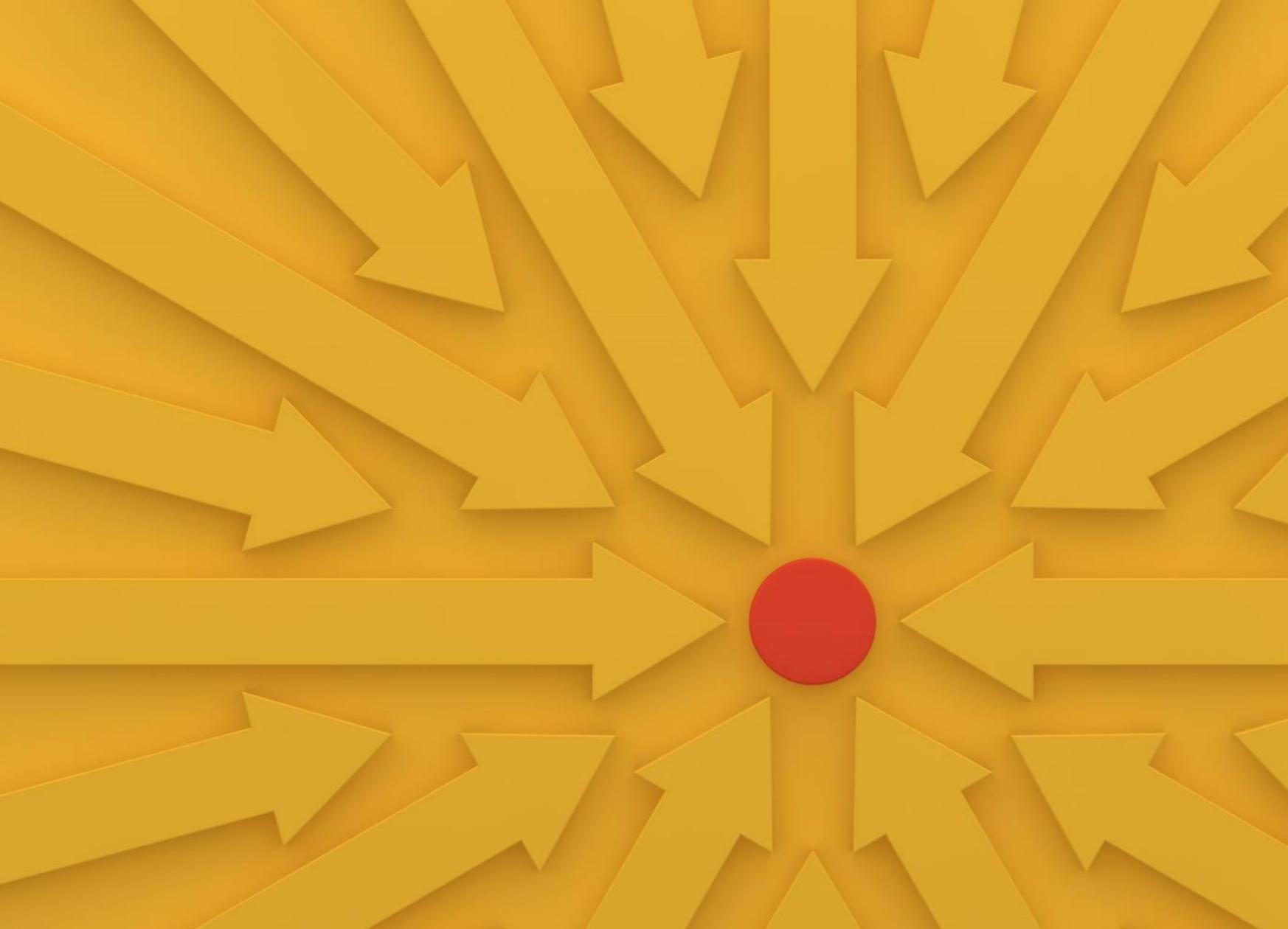
# RISK MANAGEMENT STRATEGY (GV.RM)



# ROLES, RESPONSIBILITIES, & AUTHORITIES (GV.RR)



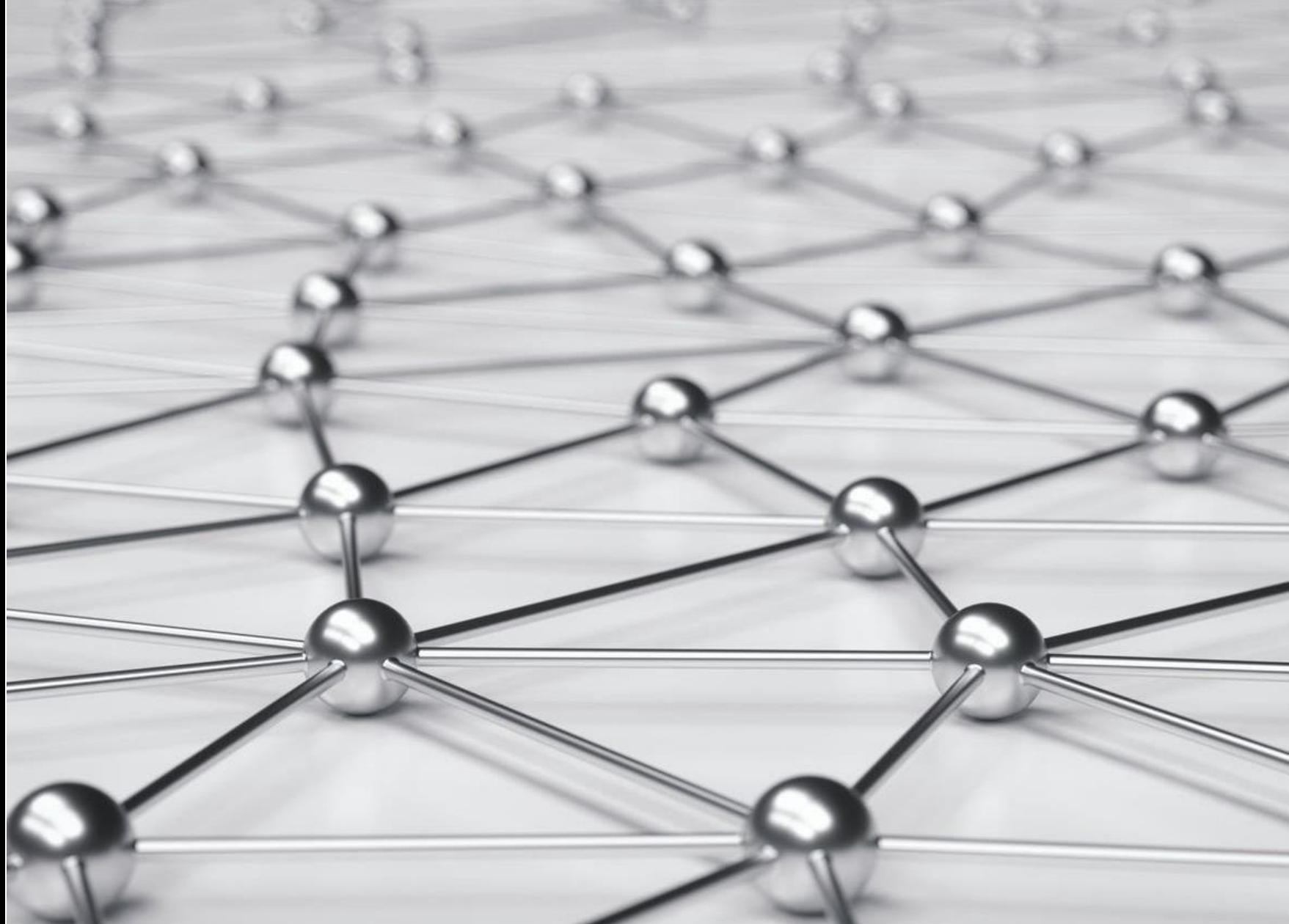
# POLICY (GV.PO)



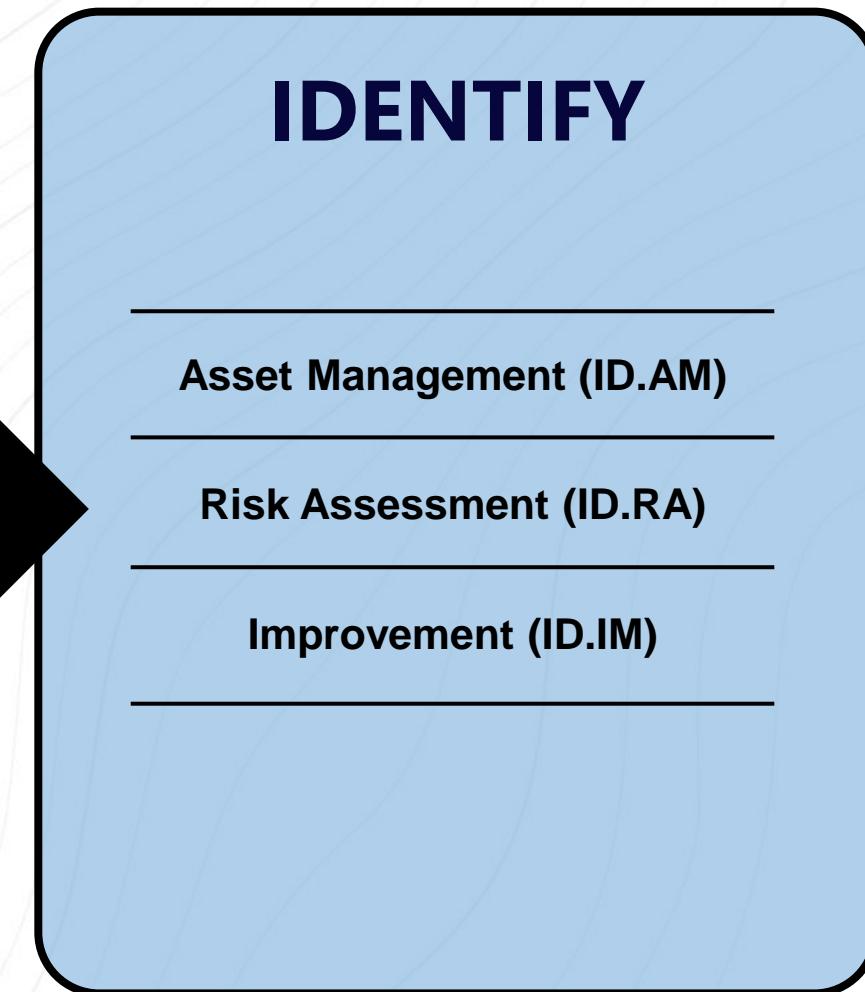
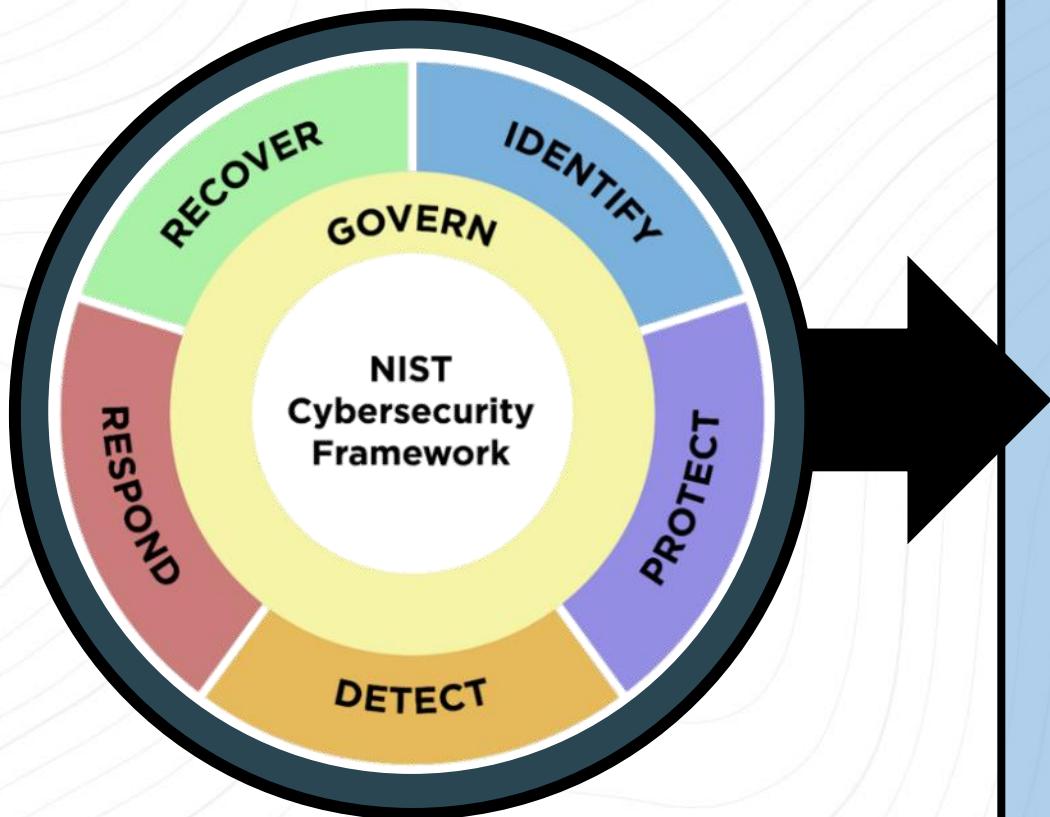
# OVERSIGHT (GV.OV)



# CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (GV.SC)



# What's included in the Identify Function?



# ASSET MANAGEMENT (ID.AM)



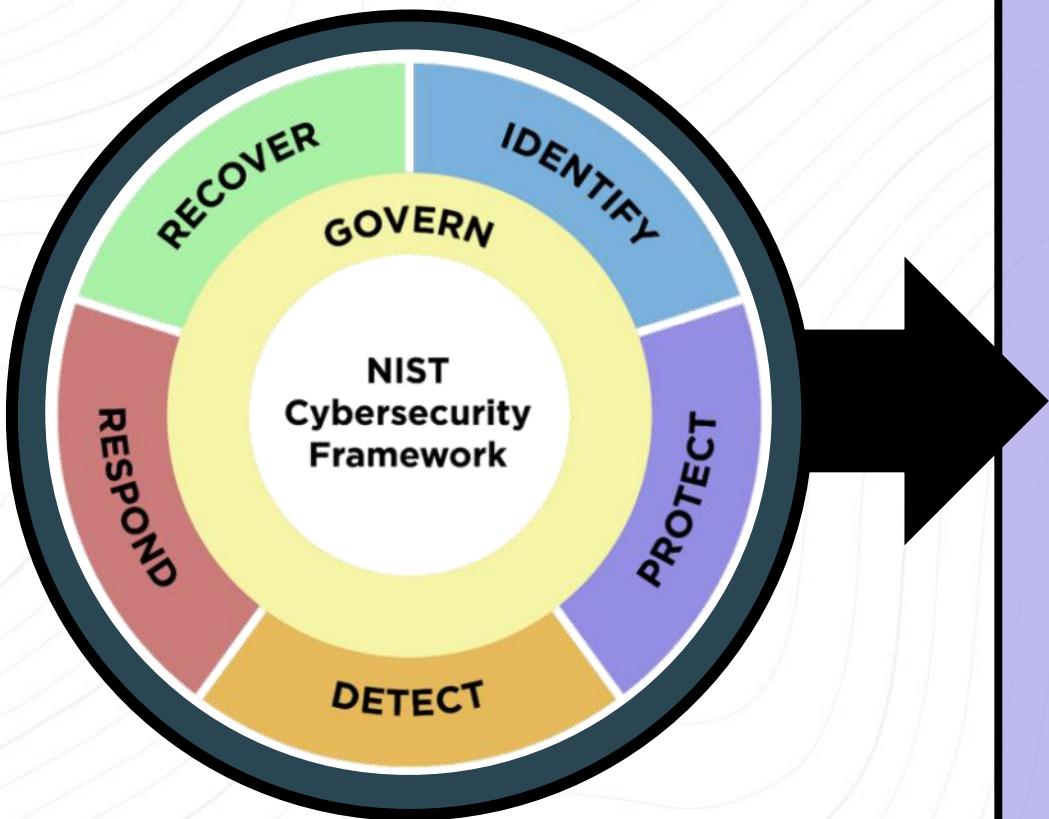
# RISK ASSESSMENT (ID.RA)



# IMPROVEMENT (ID.IM)



# 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)



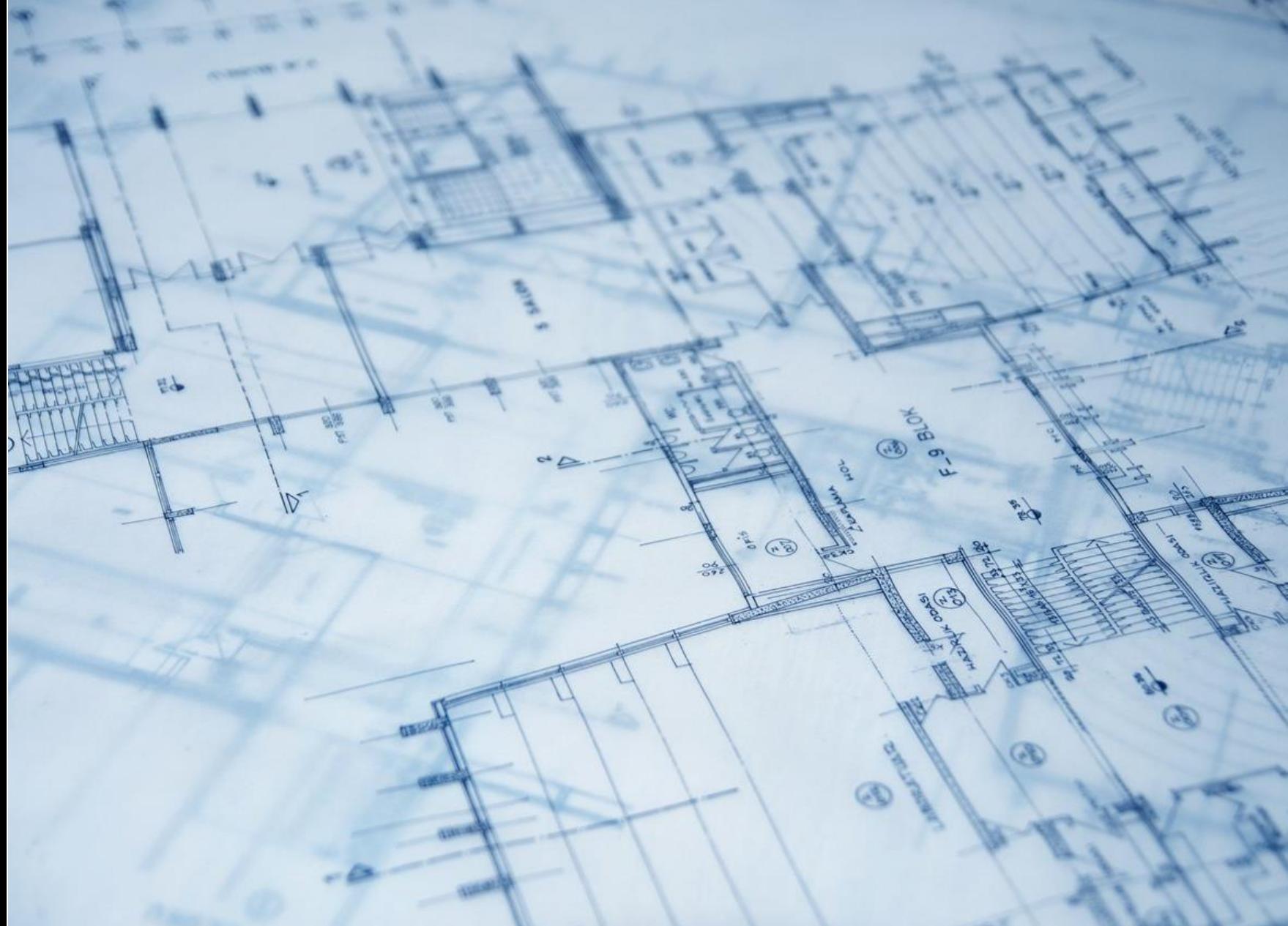
# DATA SECURITY (PR.DS)



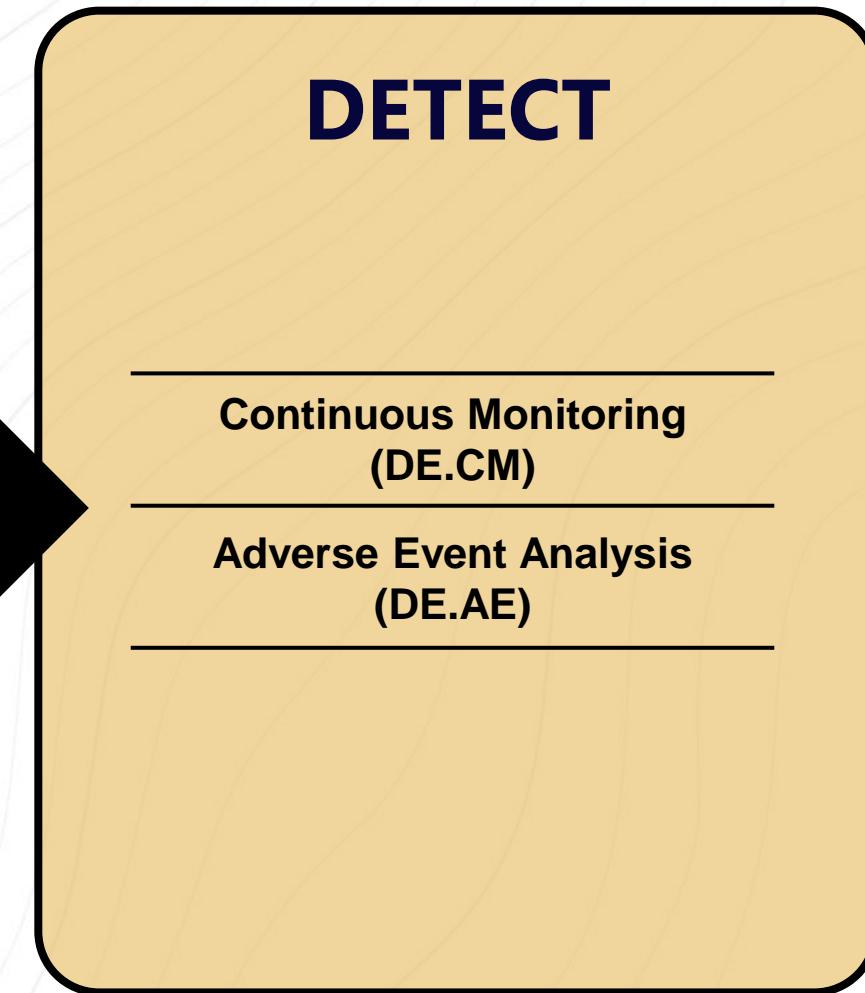
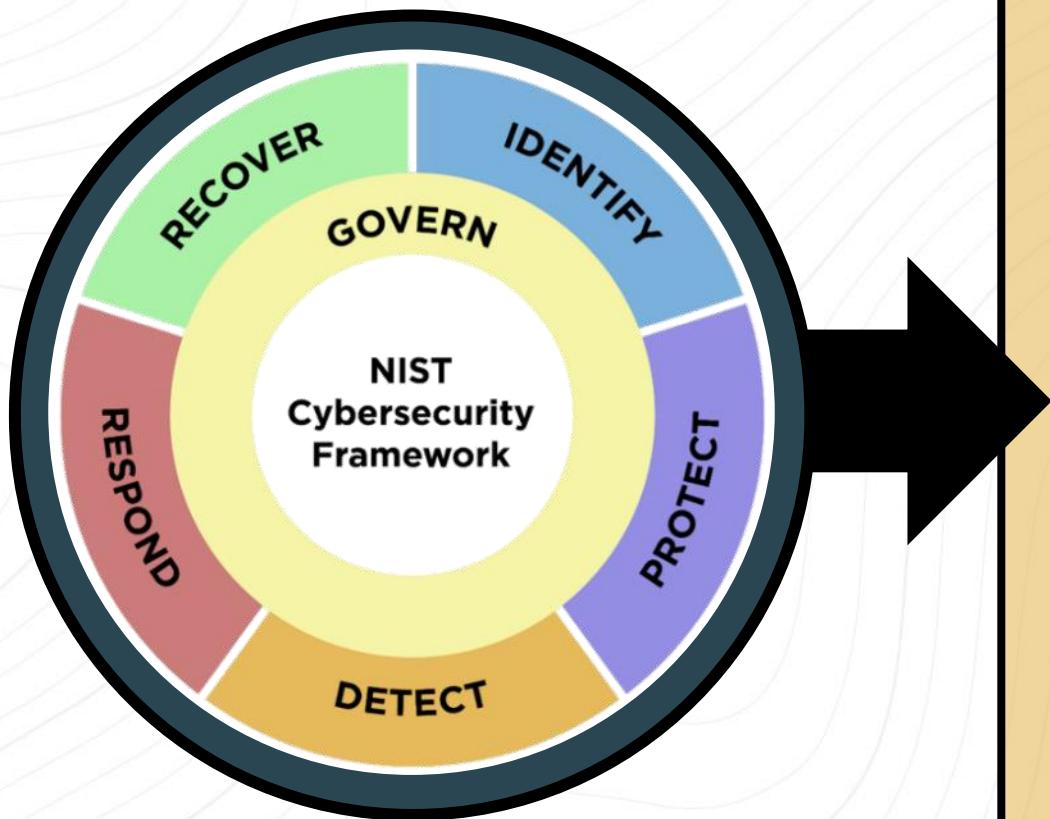
# PLATFORM SECURITY (PR.PS)



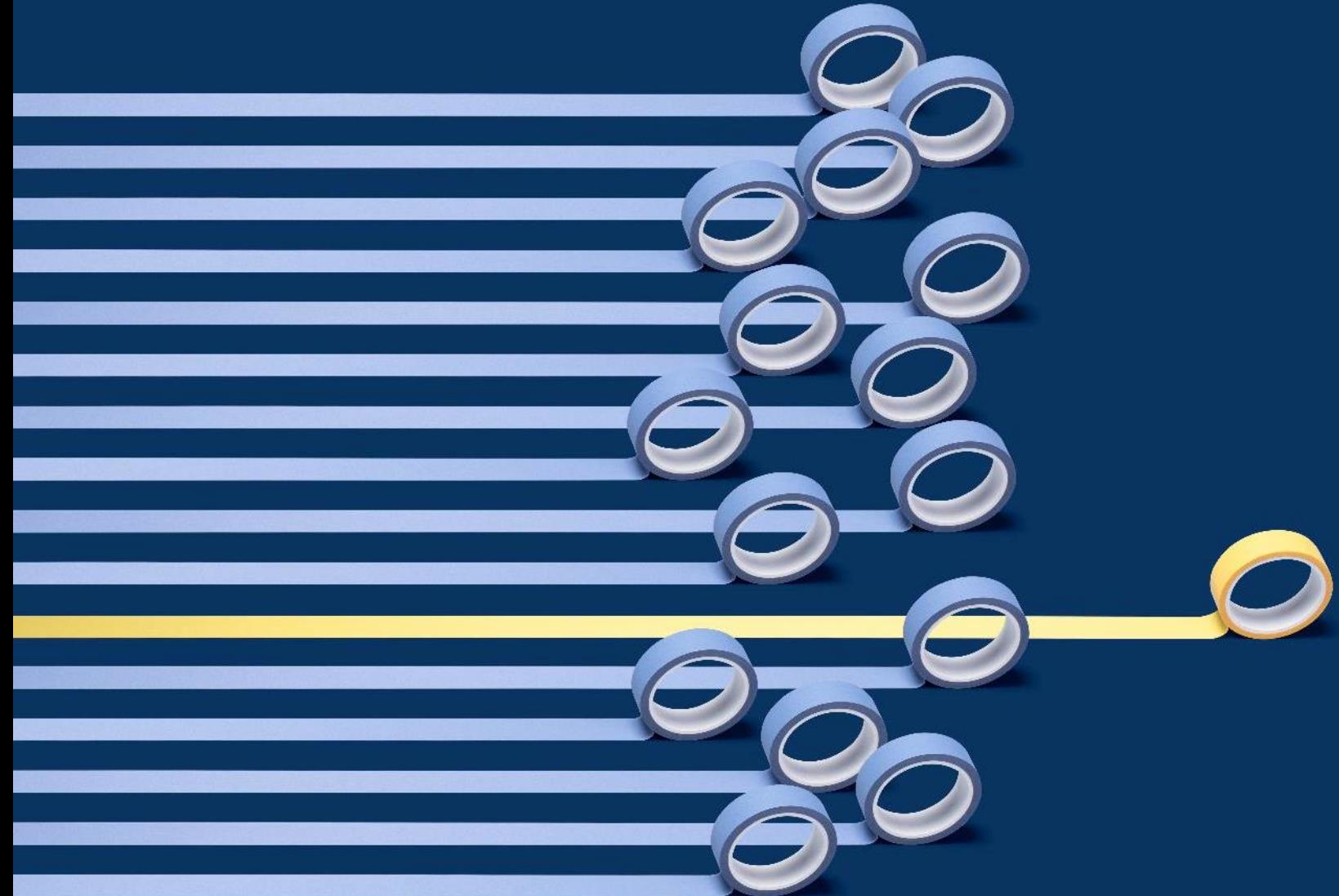
# TECHNOLOGY INFRASTRUCTURE RESILIENCE (PR.IR)



# What's included in the Detect Function?



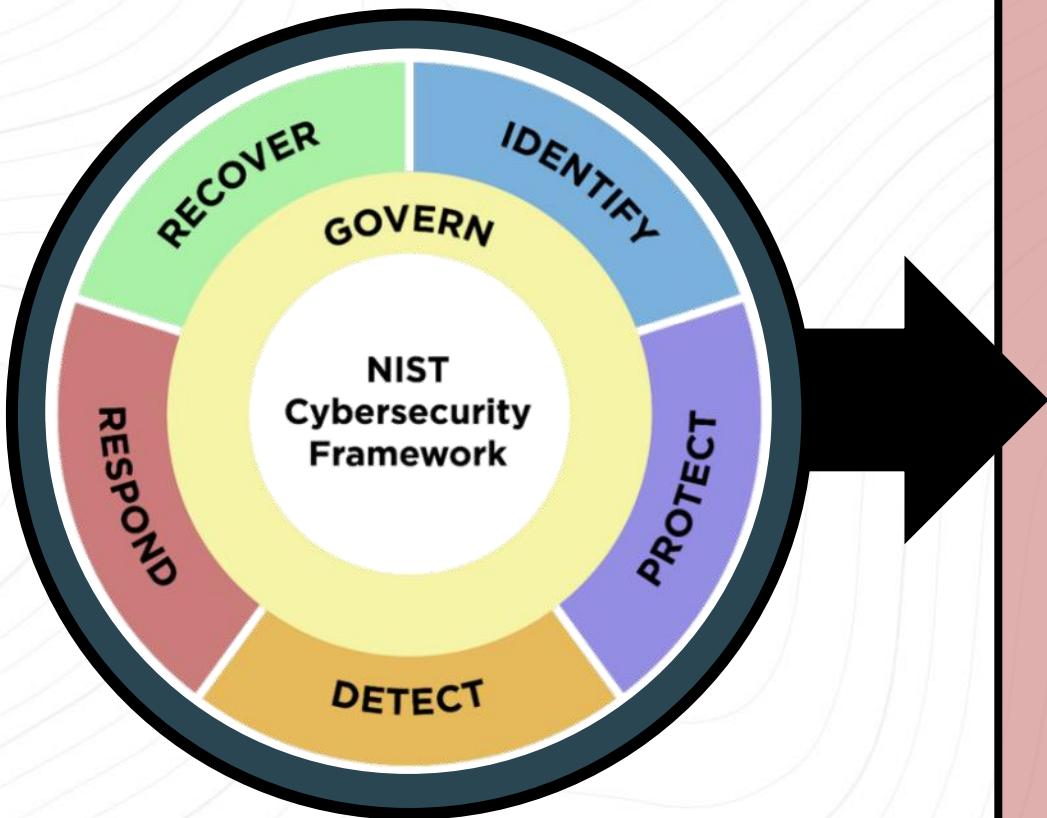
# CONTINUOUS MONITORING (DE.CM)



# 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)



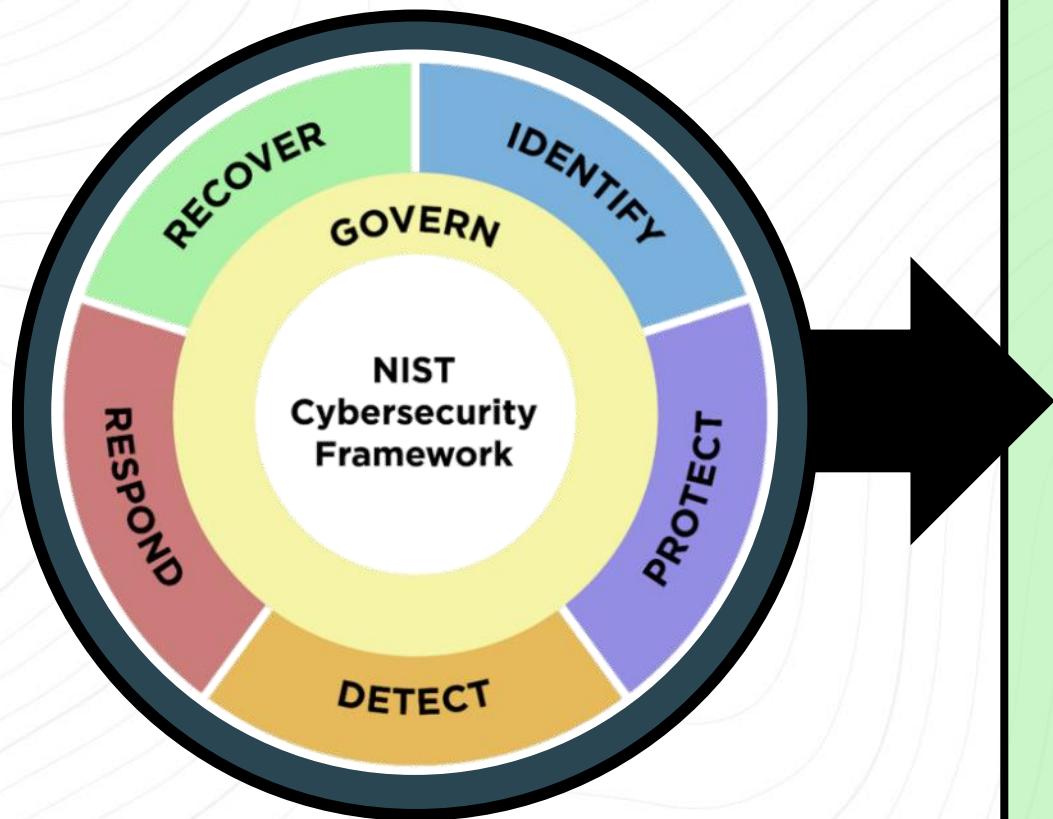
# INCIDENT RESPONSE REPORTING & COMMUNICATION (RS.CO)



# 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
RC	Recover	Improvements	RS.IM
		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?

Map the  
Changes

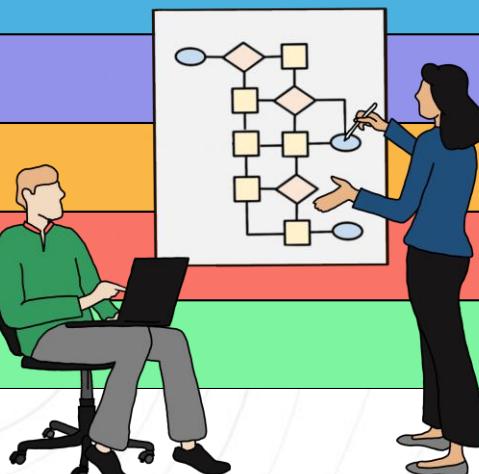
Identify  
Any Gaps

Build a  
Roadmap

# Do the changes affect you?

Map the  
Changes

A	B	C	D	
Function	Category	Subcategory	Implementation Examples	Informative References
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored				CRI Profile v2.0: GV SP 800-221A: GV.PO CSF v1.1: ID.GV
IDENTIFY (ID): The organization's current cybersecurity risks are understood				CRI Profile v2.0: ID CSF v1.1: ID
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used				CRI Profile v2.0: PR CSF v1.1: PR
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed				CRI Profile v2.0: DE CSF v1.1: DE
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken				CRI Profile v2.0: RS CSF v1.1: RS
RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored				CRI Profile v2.0: RC CSF v1.1: RC



# Do the changes affect you?

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
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
Recover (RC)	Incident Recovery Communication	RC.CO

CSF v2.0

# What changes do you need to address?

Identify Any Gaps



Many concepts were expanded to highlight important outcomes for a cybersecurity program.

# What changes do you need to address?

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
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
	Incident Recovery Plan Execution
Recover (RC)	Incident Recovery Communication
	RC.RP

CSF v2.0

Identify  
Any Gaps

# What changes do you need to address?

Identify Any Gaps

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
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
	PR.PS
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
	DE.AE
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	RS.CO
	RS.MI
Recover (RC)	Incident Recovery Plan Execution
	RC.RP
	Incident Recovery Communication
	RC.CO

CSF v2.0

# What changes do you need to address?

Identify Any Gaps

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
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
	PR.IR
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
	DE.AE
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	RS.CO
	RS.MI
Recover (RC)	Incident Recovery Plan Execution
	RC.RP
	Incident Recovery Communication
	RC.CO

CSF v2.0

# Where should you start?

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

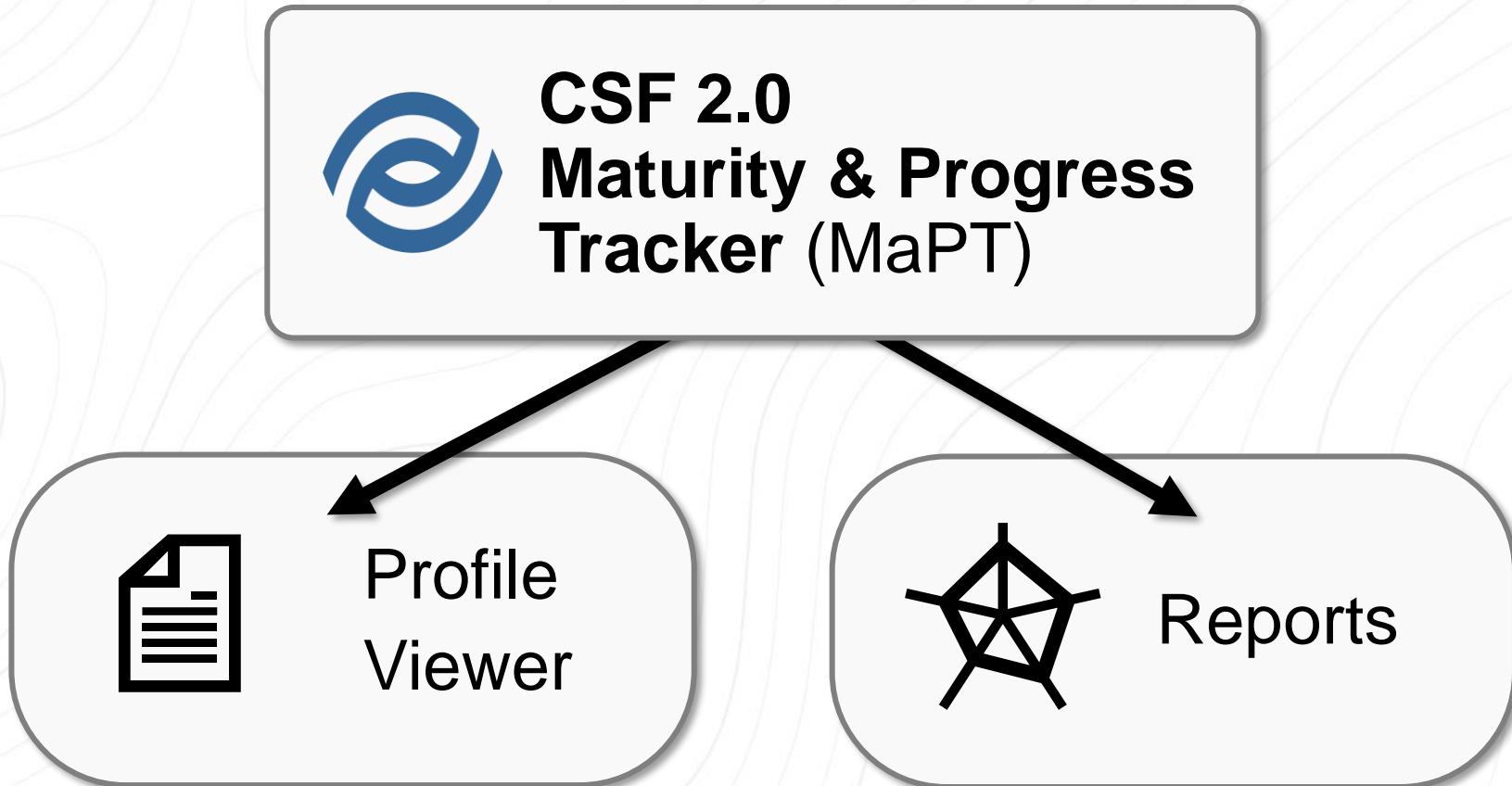


**CSF 2.0  
Maturity & Progress  
Tracker (MaPT)**

**Build a  
Roadmap**



# Build a Roadmap



# Where should you start?



Profile  
Viewer

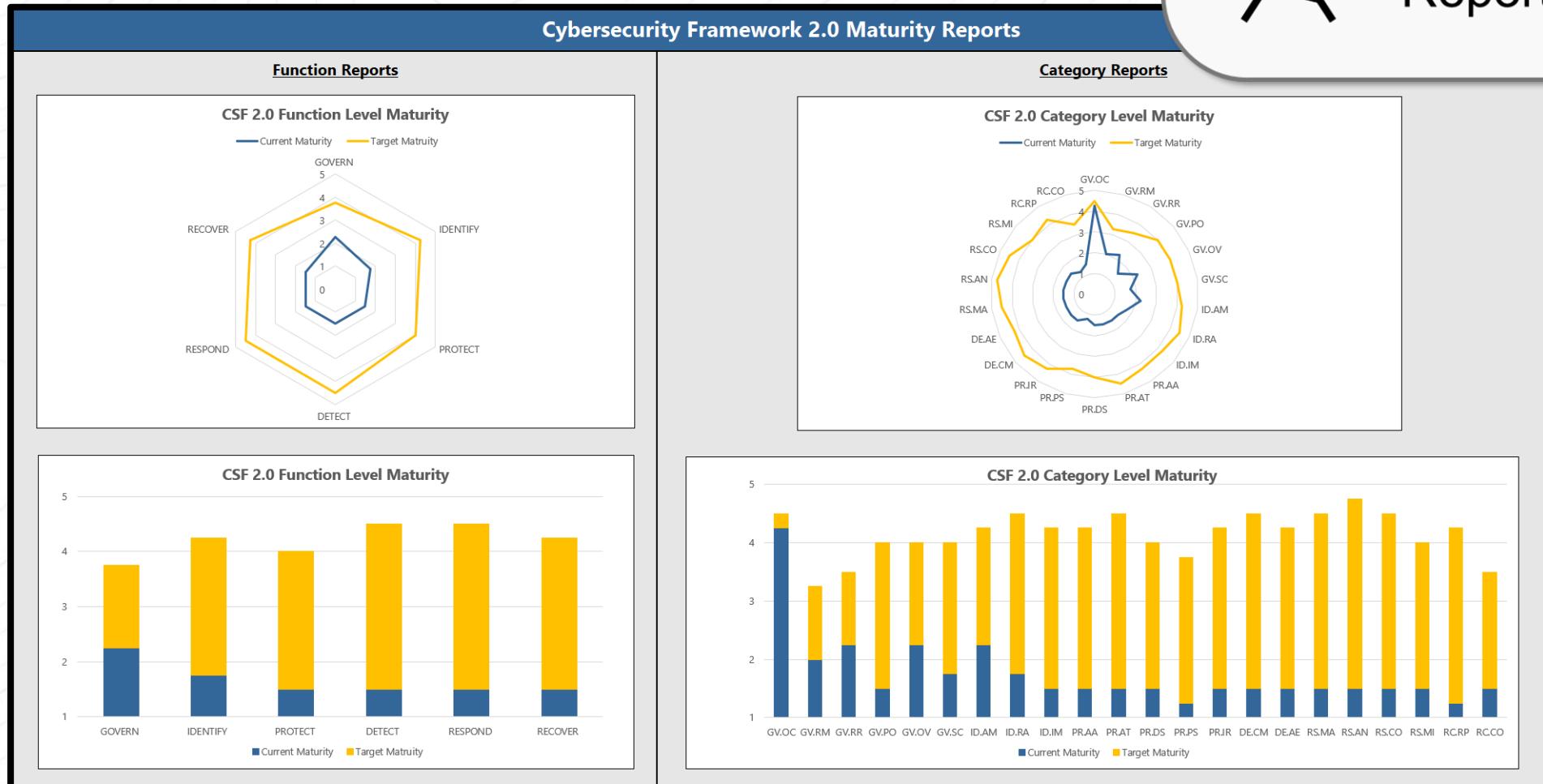
## CSF 2.0 Maturity & Progress Tracker (MaPT)

Cybersecurity Framework v2.0 Core	Current State		Target State		Progress
	Maturity	Description	Maturity	Description	
<b>GOVERN (GV):</b> The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored					
<b>Organizational Context (GV.OC):</b> The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood					
<b>GV.OC-01:</b> <b>The organizational mission is understood and informs cybersecurity risk management</b>	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
<b>GV.OC-02:</b> <b>Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered</b>	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
<b>GV.OC-03:</b> <b>Legal, regulatory, and contractual requirements regarding</b>		Cybersecurity policies and procedures are directly aligned with the		Through transparent reporting and updates on cybersecurity initiatives, the company	

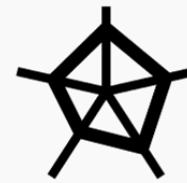
# Where should you start?



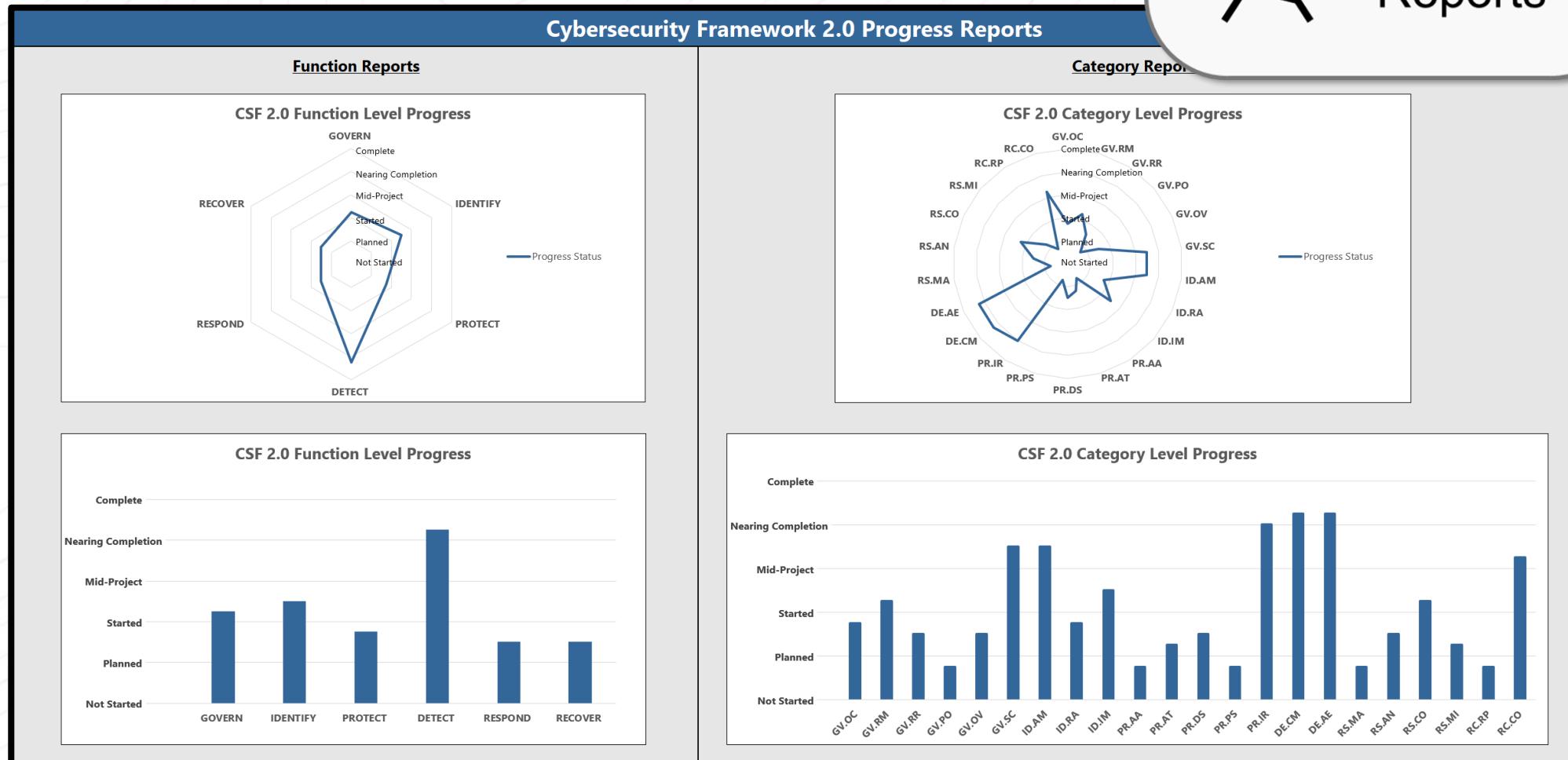
Maturity Reports



# Where should you start?



Progress  
Reports



# Do I measure up?

Map the  
Changes

Identify  
Any Gaps

Build a  
Roadmap

# Resources Roundup

# 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

# 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
<b>Organizational Context (GV.OC):</b> The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	<b>GV.OC-01:</b> The organizational mission is understood and informs cybersecurity risk management	<b>Ex1:</b> 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
	<b>GV.OC-02:</b> Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	<b>Ex1:</b> Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) <b>Ex2:</b> 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)
	<b>GV.OC-03:</b> Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	<b>Ex1:</b> 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) <b>Ex2:</b> Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information <b>Ex3:</b> Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements
	<b>GV.OC-04:</b> Critical objectives, capabilities, and services that	<b>Ex1:</b> 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

## 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		
<b>GV.OC-01:</b> The organizational mission is understood and informs cybersecurity risk management	<b>Ex1:</b> 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	
<b>GV.OC-02:</b> Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	<b>Ex2:</b> Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) <b>Ex3:</b> 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](http://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

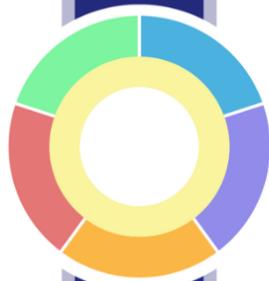
For organizations with specific common goals

## MAPPINGS

See how NIST's work interrelates and shares themes

# 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
<b>Organizational Context (GV.OC):</b> The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	<b>GV.OC-01:</b> The organizational mission is understood and informs cybersecurity risk management	<b>Ex1:</b> 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
	<b>GV.OC-02:</b> Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	<b>Ex1:</b> Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) <b>Ex2:</b> 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. This 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](https://nist.gov/cyberframework)

Quickly find what you need, including:

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

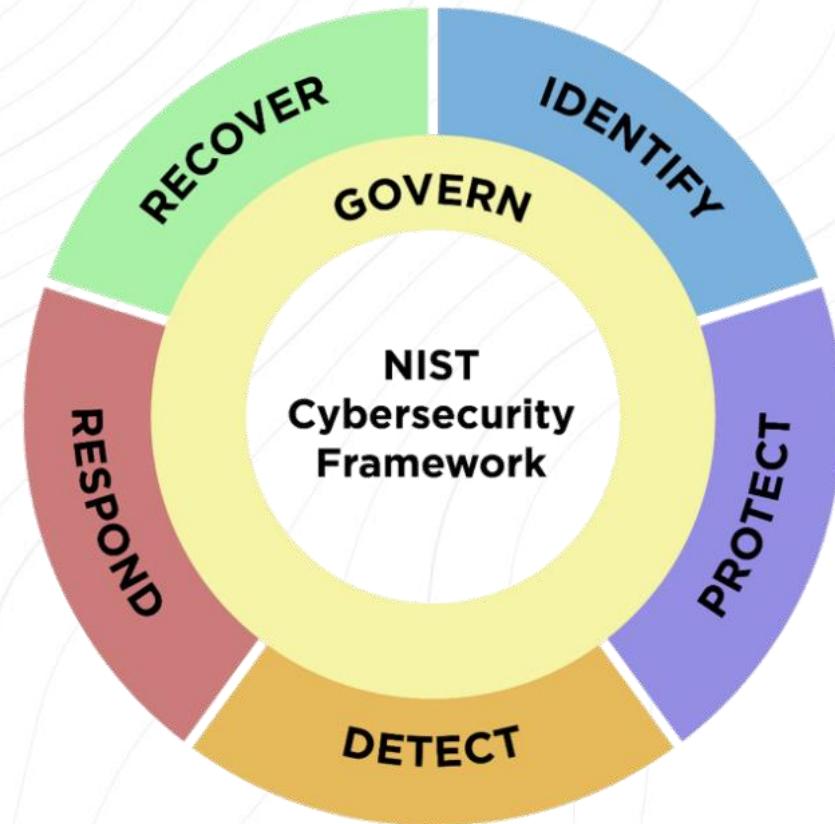
Function	Category	Subcategory	Implementation Examples	Informed References		
A IDENTIFY (ID): The organization's current cybersecurity risks are understood				CIS Controls: 1.1 CIS Profile Version 2.0: ID-AM-01 CIS Profile Version 2.0: ID-AM-01.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1		
		<b>ID.AM:</b> Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business objectives are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	<b>ID.AM-01:</b> Inventories of hardware managed by the organization are maintained  <b>ID.AM-02:</b> Inventories of software, services, and systems managed by the organization are maintained	<b>ID.AM-01:</b> Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices <b>ID.AM-02:</b> Constantly monitor networks to detect new assets  <b>ID.AM-01:</b> Inventories of software managed by the organization are maintained <b>ID.AM-02:</b> Constantly monitor all platforms, including containers and virtual machines, for software  <b>ID.AM-03:</b> Representations of the organization's authorized network communication and internal and external network data flows are maintained	CIS Controls: 1.1 CIS Profile Version 2.0: ID-AM-01 CIS Profile Version 2.0: ID-AM-01.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1  CIS Controls: 2.1 CIS Profile Version 2.0: ID-AM-02 CIS Profile Version 2.0: ID-AM-02.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1  CIS Controls: 3.8 CIS Profile Version 2.0: ID-AM-03 CIS Profile Version 2.0: ID-AM-03.01	
			<b>ID.AM-01:</b> Inventories of hardware managed by the organization are maintained  <b>ID.AM-02:</b> Inventories of software, services, and systems managed by the organization are maintained	<b>ID.AM-01:</b> Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices <b>ID.AM-02:</b> Constantly monitor networks to detect new assets  <b>ID.AM-01:</b> Inventories of software managed by the organization are maintained <b>ID.AM-02:</b> Constantly monitor all platforms, including containers and virtual machines, for software  <b>ID.AM-03:</b> Representations of the organization's authorized network communication and internal and external network data flows are maintained	CIS Controls: 1.1 CIS Profile Version 2.0: ID-AM-01 CIS Profile Version 2.0: ID-AM-01.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1  CIS Controls: 2.1 CIS Profile Version 2.0: ID-AM-02 CIS Profile Version 2.0: ID-AM-02.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1  CIS Controls: 3.8 CIS Profile Version 2.0: ID-AM-03 CIS Profile Version 2.0: ID-AM-03.01	
				<b>ID.AM-01:</b> Inventories of hardware managed by the organization are maintained  <b>ID.AM-02:</b> Inventories of software, services, and systems managed by the organization are maintained	<b>ID.AM-01:</b> Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices <b>ID.AM-02:</b> Constantly monitor networks to detect new assets  <b>ID.AM-01:</b> Inventories of software managed by the organization are maintained <b>ID.AM-02:</b> Constantly monitor all platforms, including containers and virtual machines, for software  <b>ID.AM-03:</b> Representations of the organization's authorized network communication and internal and external network data flows are maintained	CIS Controls: 1.1 CIS Profile Version 2.0: ID-AM-01 CIS Profile Version 2.0: ID-AM-01.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1  CIS Controls: 2.1 CIS Profile Version 2.0: ID-AM-02 CIS Profile Version 2.0: ID-AM-02.01 Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1  CIS Controls: 3.8 CIS Profile Version 2.0: ID-AM-03 CIS 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](mailto:Info@OpticCyber.com)



**Tom Conkle**  
Cybersecurity Engineer  
[Info@OpticCyber.com](mailto:Info@OpticCyber.com)



# THANK YOU!