

OpticCyber.com
Info@OpticCyber.com

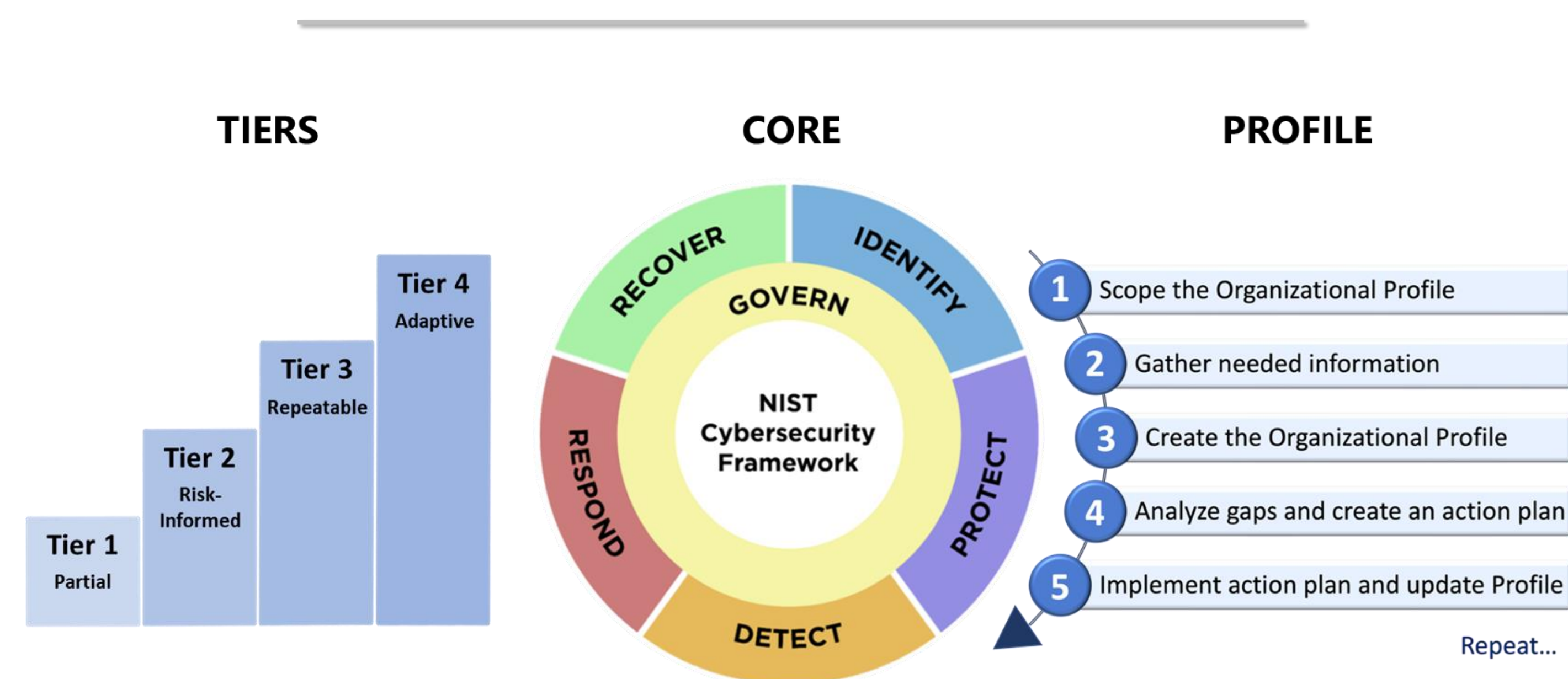
Navigating the NIST Cybersecurity Framework (CSF) 2.0



What is the Cybersecurity Framework (CSF)?

Helps answer the question “*what do I need to do?*” when it comes to cybersecurity.

- Flexible Framework
- Outcome Based
- Common Language
- Structured Approach

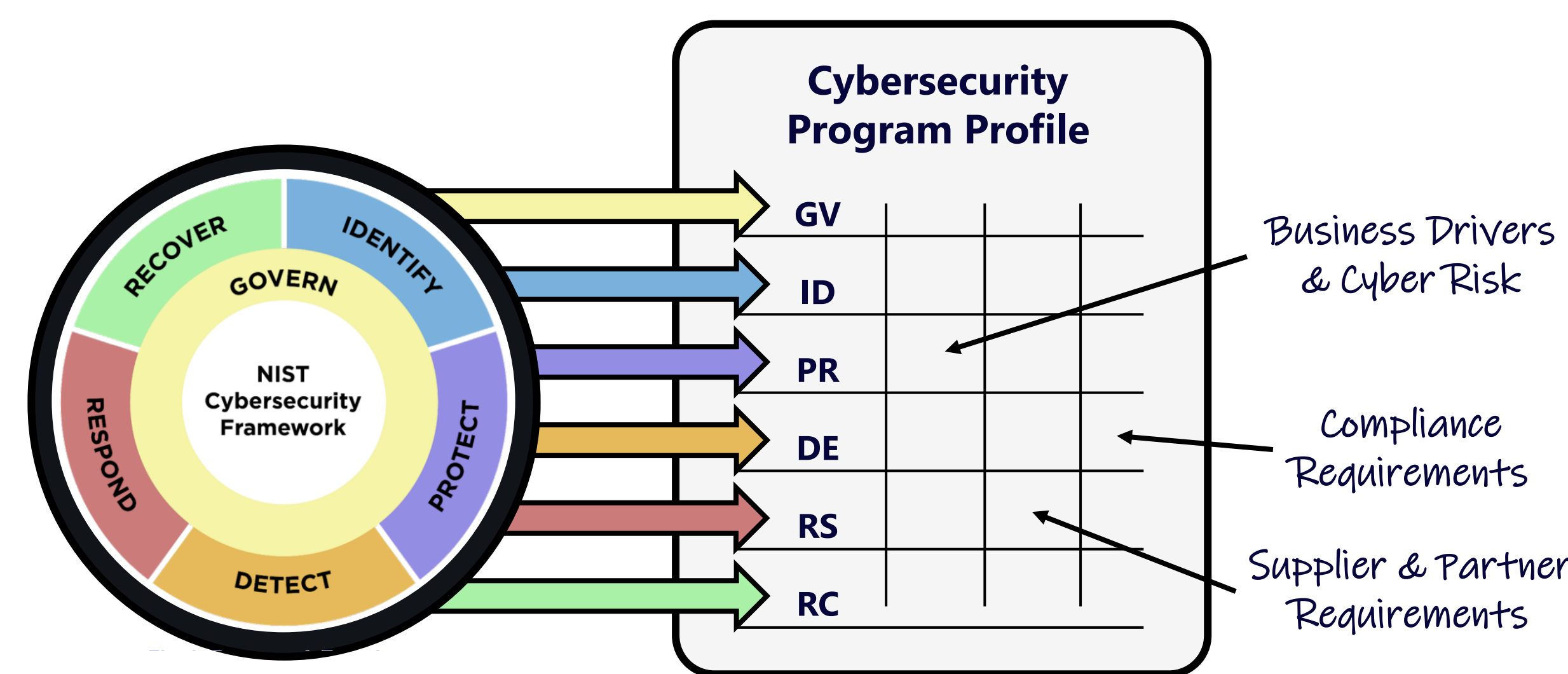


The **Tiers** help measure “how well” cyber capabilities are being managed & the rigor required to manage cyber risk.

The **Core** is a set of cybersecurity outcomes that tell us “*what*” needs to be done to manage a cybersecurity program.

The **Profiles** are the mechanism for capturing what is being done today as well as what needs to be done in the future.

The CSF acts as the common language to align requirements & streamline efforts.



The CSF provides a framework for managing both business drivers & risks along with compliance & partner requirements.

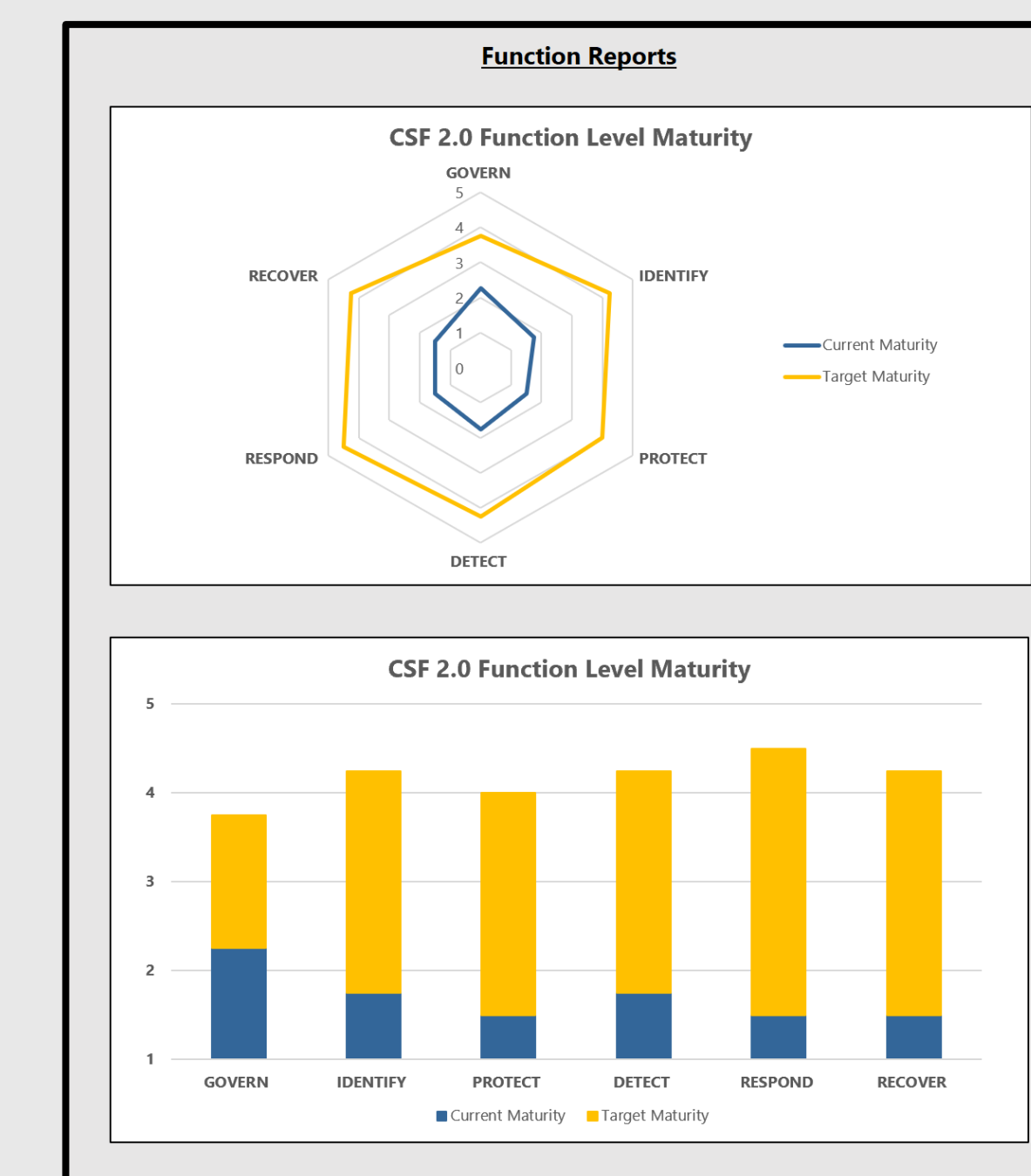
We use the CSF as the “Rosetta Stone” for cybersecurity across academic institutions.

So... how does the framework help higher education?

Leverage the CSF to drive efficiencies & improve communication across institutions of higher education.

Universities face unique cybersecurity & privacy challenges due to their complex structures & functions.

- Set a common baseline to ensure a minimum level of cybersecurity across diverse units
- Define tailored goals for areas with unique responsibilities & requirements
- Maximize resources by finding commonality & learning from others’ successes
- Communicate through a consistent approach



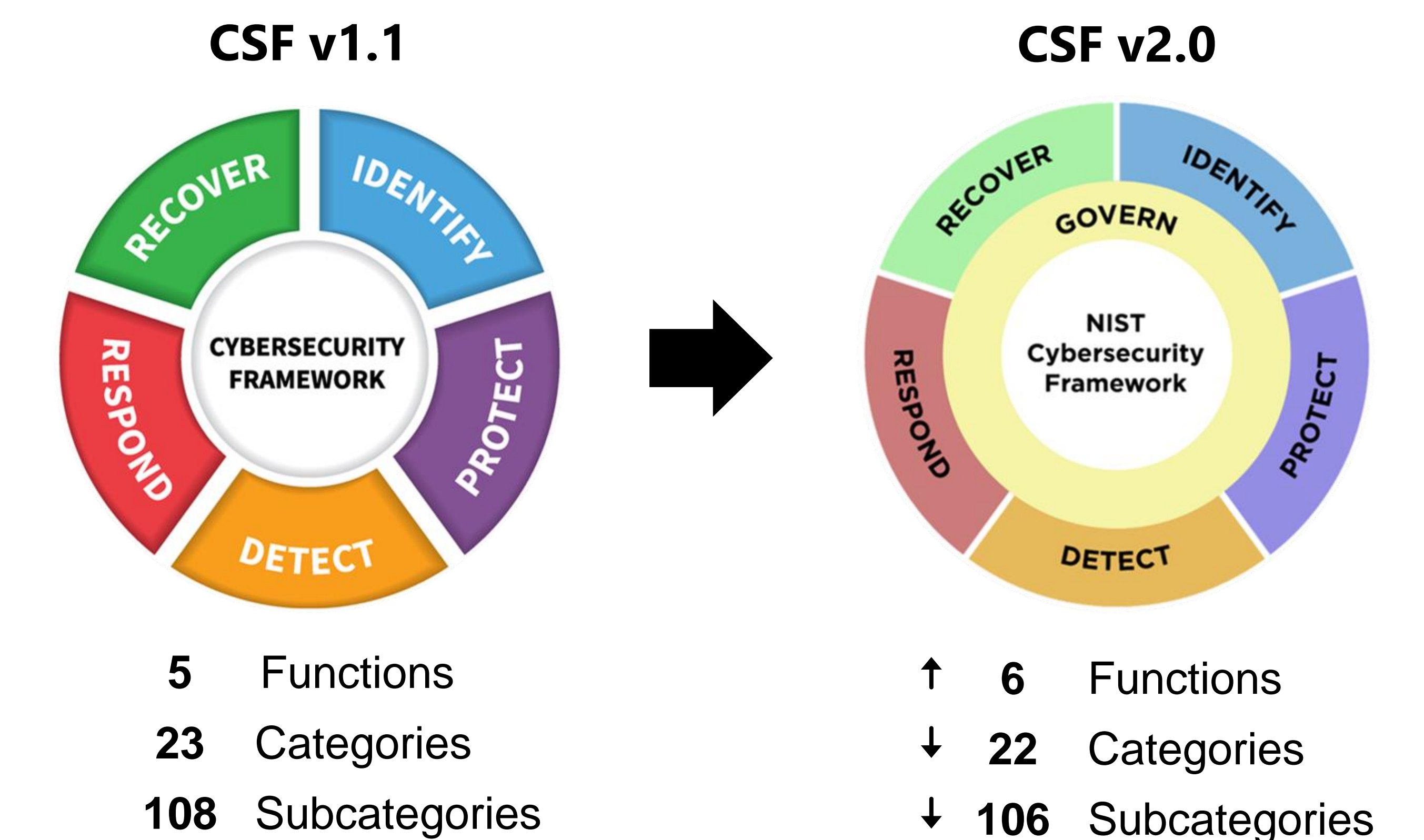
Use Cases:

- 1 Tailored cybersecurity assessment tool to align departments
 - Gain insight into current capabilities through a questionnaire
 - Track progress towards targets
 - Identify efficiencies through groups that already have mature capabilities
- 2 Tracked & reported cybersecurity maturity and progress improvement across a school
 - Define common targets & capture current state to identify gaps
 - Measure maturity improvements & track progress over time

CSF 2.0 Maturity & Progress Tracker (MaPT)					
Function	Category	ID	Current State	Target State	Progress
GOVERN (GV)	Organizational Context	GV-OC
IDENTIFY (ID)	Asset Management	ID-AM
PROTECT (PR)	Information Protection Processes & Procedures	PR-IP
DETECT (DE)	Security Continuous Monitoring	DE-CM
RESPOND (RS)	Incident Response Reporting and Communication	RS-CO
RECOVER (RC)	Recovery Planning	RC-PP

Maturity and Progress Tracker (MaPT)

This update marks the first major change in a decade resulting in the CSF v2.0.



The update streamlined & clarified the critical cybersecurity concerns of today.

- New Govern Function
- Expanded in areas like Incident Response, Risk Management, & Supply Chain Cybersecurity
- Consolidated many Categories & Subcategories

Function	Category	ID	Function	Category	Category Identifier
GOVERN (GV)	Organizational Context	GV-OC	GOVERN (GV)	Risk Management Strategy	GV-AM
	Business Environment	GV-BE		Policies, Responsibilities, and Authorities	GV-PR
	Governance	GV-GV		Overnight	GV-OV
IDENTIFY (ID)	Asset Management	ID-AM	IDENTIFY (ID)	Asset Management	ID-AM
	Risk Assessment	ID-RA		Risk Assessment	ID-RA
	Supply Chain Risk Management	ID-SC		Cybersecurity Supply Chain Risk Management	GV-SC
PROTECT (PR)	Information Protection Processes & Procedures	PR-IP	PROTECT (PR)	Improvement	ID-IM
	Maintenance	PR-MA		Identity Management, Authentication & Access Control	PR-AA
	Protective Technology	PR-PT		Awareness and Training	PR-AT
DETECT (DE)	Security Continuous Monitoring	DE-CM	DETECT (DE)	Data Security	PR-DS
	Detection Processes	DE-DP		Platform Security	PR-PS
	Response Processes	RS-RP		Technology Infrastructure Resilience	PR-IR
RESPOND (RS)	Communications	RS-CO	RESPOND (RS)	Continuous Monitoring	DE-CM
	Analysis	RS-AN		Adverse Event Analysis	DE-AE
	Mitigation	RS-MI		Incident Management	RS-AM
RECOVER (RC)	Recovery Planning	RC-PP	RECOVER (RC)	Incident Analysis	RS-AN
	Improvements	RC-IM		Incident Response Reporting and Communication	RS-CO
	Communications	RC-CO		Incident Mitigation	RS-MI

Now what?

- Capture what you’re doing today against the CSF 2.0 to better understand your current cybermaturity.
- Streamline your efforts through a common Profile to drive communications & ensure a secure future for your organization!