

# Components of the Cybersecurity Framework

July 2018

[cyberframework@nist.gov](mailto:cyberframework@nist.gov)

# Cybersecurity Framework Components

---

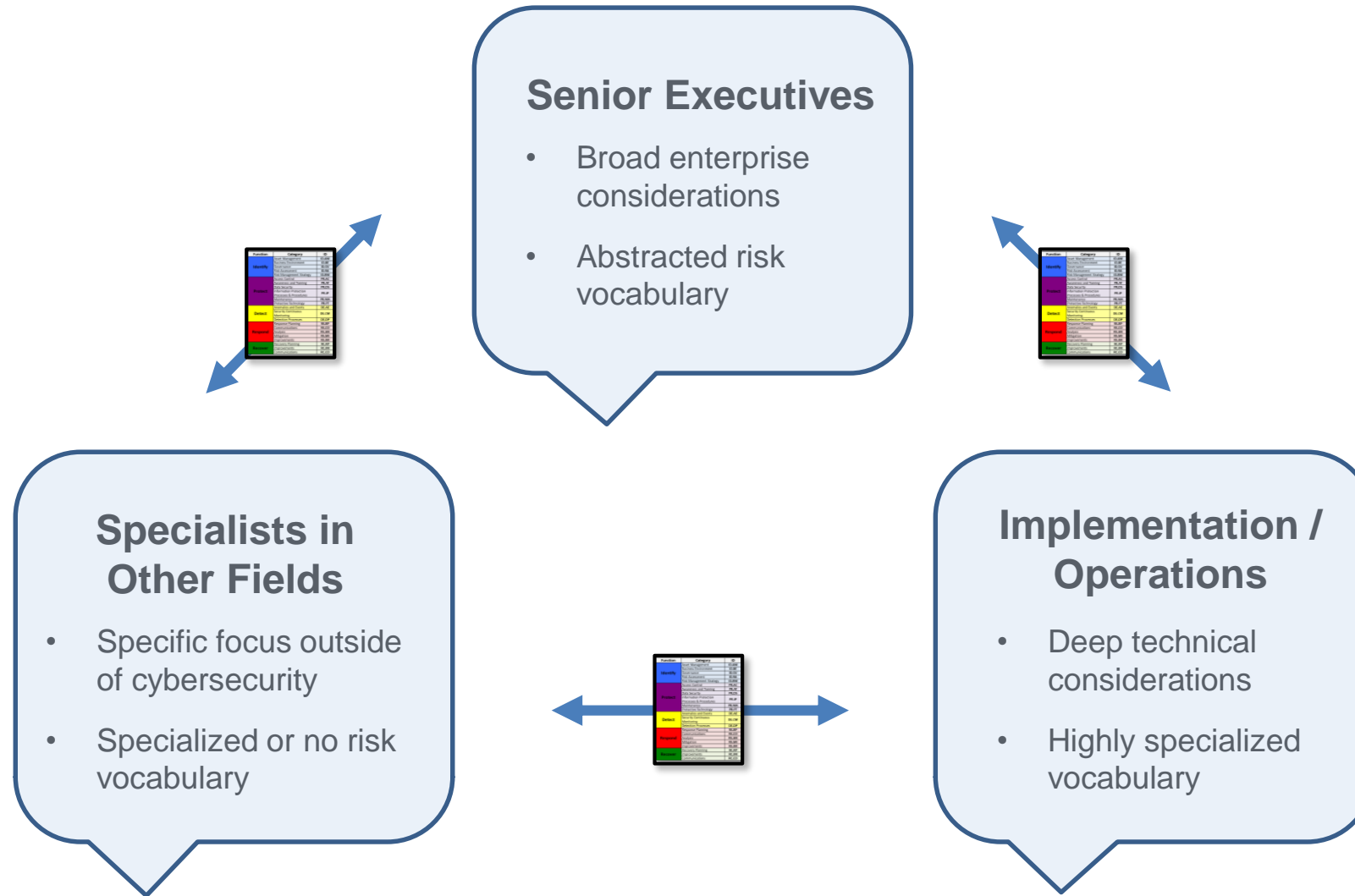
The Framework consists of 3 main components



# Framework Core

	Function	Category	ID
What processes and assets need protection?	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
What safeguards are available?	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
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

# Core: A Translation Layer



# Subcategories & Informative References

Function	Category	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
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
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

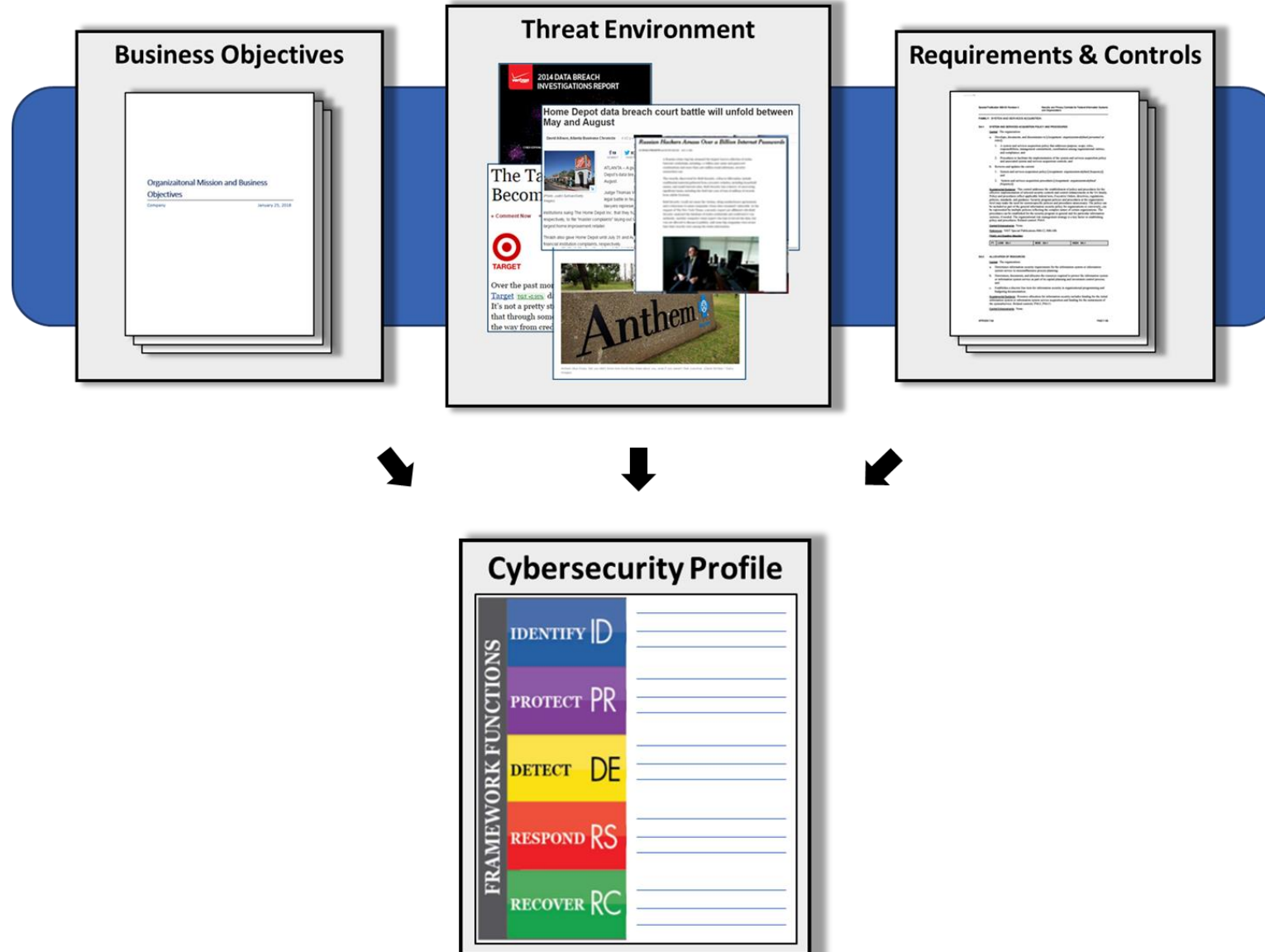
Subcategory	Informative References
<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated	<b>COBIT 5</b> APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 <b>ISO/IEC 27001:2013</b> A.15.1.3, A.15.2.1, A.15.2.2 <b>NIST SP 800-53 Rev. 4</b> CP-2, SA-12
<b>ID.BE-2:</b> The organization's place in critical infrastructure and its industry sector is identified and communicated	<b>COBIT 5</b> APO02.06, APO03.01 <b>NIST SP 800-53 Rev. 4</b> PM-8
<b>ID.BE-3:</b> Priorities for organizational mission, objectives, and activities are established and communicated	<b>COBIT 5</b> APO02.01, APO02.06, APO03.01 <b>ISA 62443-2-1:2009</b> 4.2.2.1, 4.2.3.6 <b>NIST SP 800-53 Rev. 4</b> PM-11, SA-14
<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established	<b>ISO/IEC 27001:2013</b> A.11.2.2, A.11.2.3, A.12.1.3 <b>NIST SP 800-53 Rev. 4</b> CP-8, PE-9, PE-11, PM-8, SA-14
<b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established	<b>COBIT 5</b> DSS04.02 <b>ISO/IEC 27001:2013</b> A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 <b>NIST SP 800-53 Rev. 4</b> CP-2, CP-11, SA-14

# Framework Profiles

- Alignment with business requirements, risk tolerance, and organizational resources
- Enables organizations to **establish a roadmap for reducing cybersecurity risk**
- Used to describe **current state** or **desired target state** of cybersecurity activities



# Building a Profile



# Resource and Budget Decision Making

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	\$\$\$		X
2	High	Large	\$\$	X	
3	Moderate	Medium	\$	X	
...	...	...	...		
98	Moderate	None	\$\$		Reassess

...and supports on-going operational decisions, too



# Resources

*Where to Learn More and Stay Current*

*Framework for Improving Critical Infrastructure Cybersecurity* and related news, information:

[www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

Additional cybersecurity resources:

<http://csrc.nist.gov/>

Questions, comments, ideas:

[cyberframework@nist.gov](mailto:cyberframework@nist.gov)

