ASSESSING CYBER RISK

JUSTIN JONES

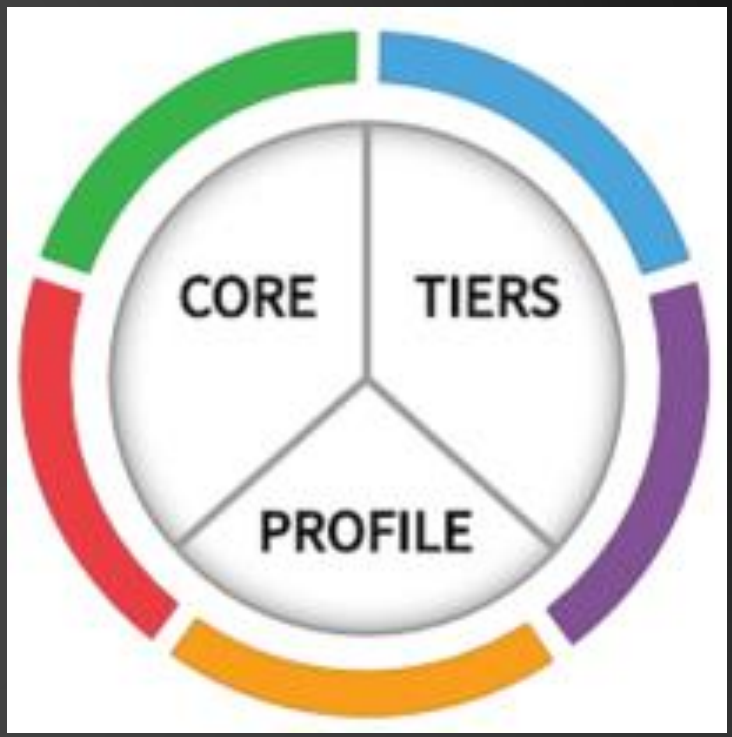
https://www.linkedin.com/in/justin-jones-406/

WHY USE NIST CSF?

- Creates a common language amongst industries and peers
- Provides a mechanism for deeper collaboration to understand the cyber risks that could negatively impact your organization
- Helps maintain compliance and demonstrates due care
- Measures cybersecurity maturity and helps allocate resources effectively to manage cyber risk

WHAT IS THE NIST CSF?

- Comprised of 3 Primary Components
  - Framework Core
  - Implementation Tiers
  - Framework Profiles



https://www.nist.gov/cyberframework/online-learning/components-framework

FRAMEWORK CORE

- Created to be used across all critical infrastructure sectors which include utilities, financial services, healthcare, etc.
- Provides high-level, strategic view of the lifecycle of an organization risk management program
- Not meant to be descriptive and not a checklist
- Living document

FRAMEWORK CORE

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 and 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

https://www.nist.gov/cyberframework/online-learning/components-framework

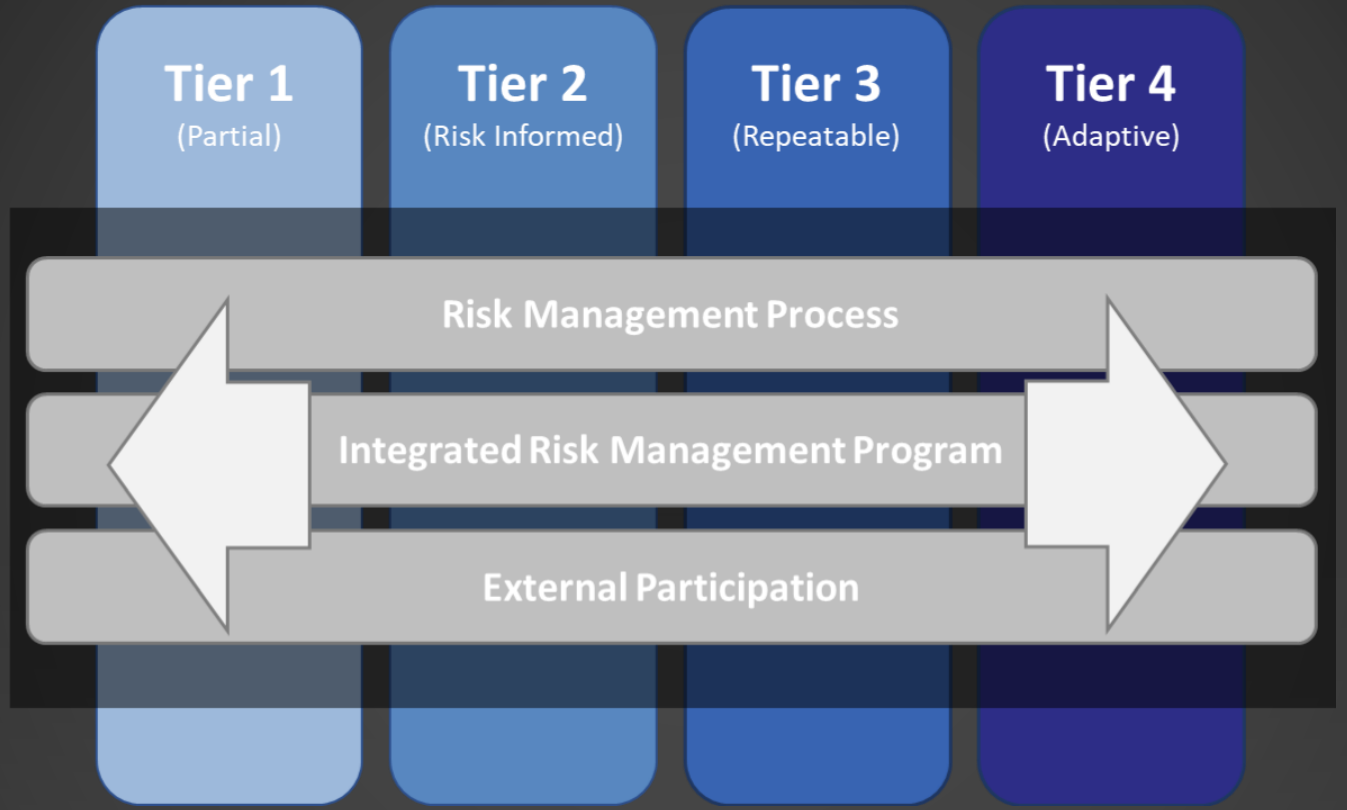
FRAMEWORK CORE EXAMPLE

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 and 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
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

https://www.nist.gov/cyberframework/online-learning/components-framework

IMPLEMENTATION TIERS



https://www.nist.gov/cyberframework/online-learning/components-framework

FRAMEWORK PROFILES

- Helps organizations align and prioritize their cybersecurity program activities
- Consists of the alignment of:
  - Business Objectives
  - Cybersecurity Program Requirements
  - Operating Environment

FRAMEWORK PROFILES

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

Target Profile

https://www.nist.gov/cyberframework/online-learning/components-framework

NIST GAP ANALYSIS PROCESS

1. Prioritize and Scope
2. Orient
3. Create Current Profile
4. Conduct Risk Assessment
5. Create Target Profile
6. Determine, Analyze, and Prioritize Gaps
7. Implement Action Plan

REFERENCES

- NIST CSF Website: https://www.nist.gov/cyberframework
- NIST Small Business Corner: https://www.nist.gov/itl/smallbusinesscyber
- CISA: https://www.cisa.gov/
- CISA Ransomware: https://www.cisa.gov/stopransomware
- ISAC Listing: https://www.nationalisacs.org/member-isacs-3