RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: AST3-R01

CForum:
A Community Driven Solution to Cybersecurity Challenges

Tom Conkle

Cybersecurity Engineer
G2, Inc.
@TomConkle

Greg Witte

Sr. Security Engineer
G2, Inc.
@thenetworkguy

Organizations continued to battle challenges to achieving cybersecurity risk management

Image: Getty #41365208
Used with permission

U.S. Executive Order (EO) 13636 initiated a dialogue to identify challenges and determine effective responses. Industry responded to a NIST RFI:

- Trying to prioritize security activities without context seems like “Whack-a-Mole”
- IT Security budget is a zero-sum game; every dollar spent on compliance is a dollar not spent on risk-management
- Application of security controls needs to be scalable
- Challenge balancing performance and conformance
- Need for better risk dialogue with executive management

What is CForum?

- In the next few slides, we'll provide some details about CForum
- CForum continues the conversation started during the Cybersecurity Framework workshops as:
  - a place to collaborate about measuring and improving cybersecurity
  - an environment for discussing emerging threats to cybersecurity information and operation technology
  - a forum for thought leaders to share information

Cyber.SecurityFramework.org

Community response and dialogue helped refine the challenges and solutions

Framework Principles	Common Points	Initial Gaps
• Flexibility • Global Impact • Risk Mgmt Approaches • Leverage Existing Approaches, Standards, and Best Practices	• Senior Mgmt Engagement • Understanding Threat Environment • Business Risk Assessment • Separation of Business & Operational Systems • Models / Levels of Maturity • Incident Response • Cybersecurity Workforce	• Metrics • Privacy / Civil Liberties • Tools • Dependencies • Industry Best Practices • Resiliency • Critical Infrastructure Cybersecurity Nomenclature

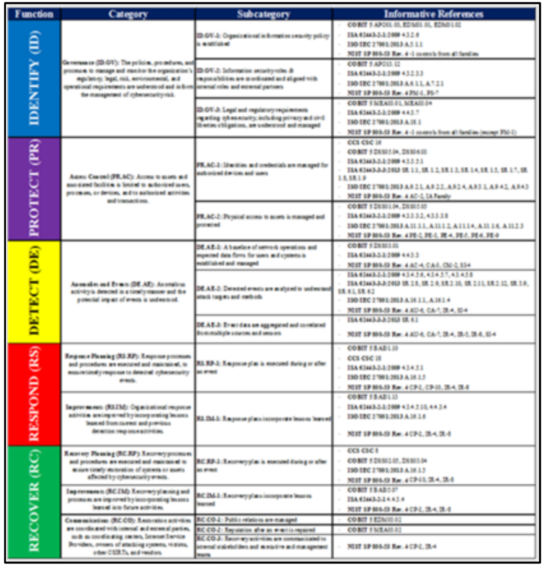
We also need a common language to help normalize and optimize activities

- Goal: Comply once – use many
- NIST identified >450 commonly used standards & practices
- Many of these share categories and families of controls in common
- Keeping up with multiple compliance frameworks is resource intensive and costly
- Need to express requirements and status to supply chain partners

For example:
NIST SP 800-53 Control AC-3, ISO 27002:2013 A.9.4.1, and IEC 15408 FDP_ACC.2 all point to “**access control**” processes

The Cybersecurity Framework is comprised of three primary components

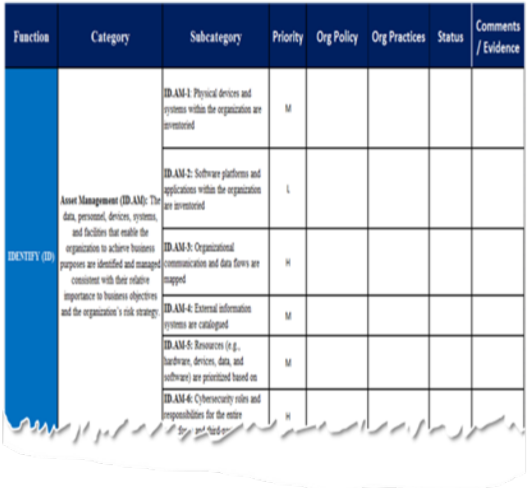
Framework Core



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	· COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	· COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· NIST SP 800-53 Rev. 4 CP-2, IR-4

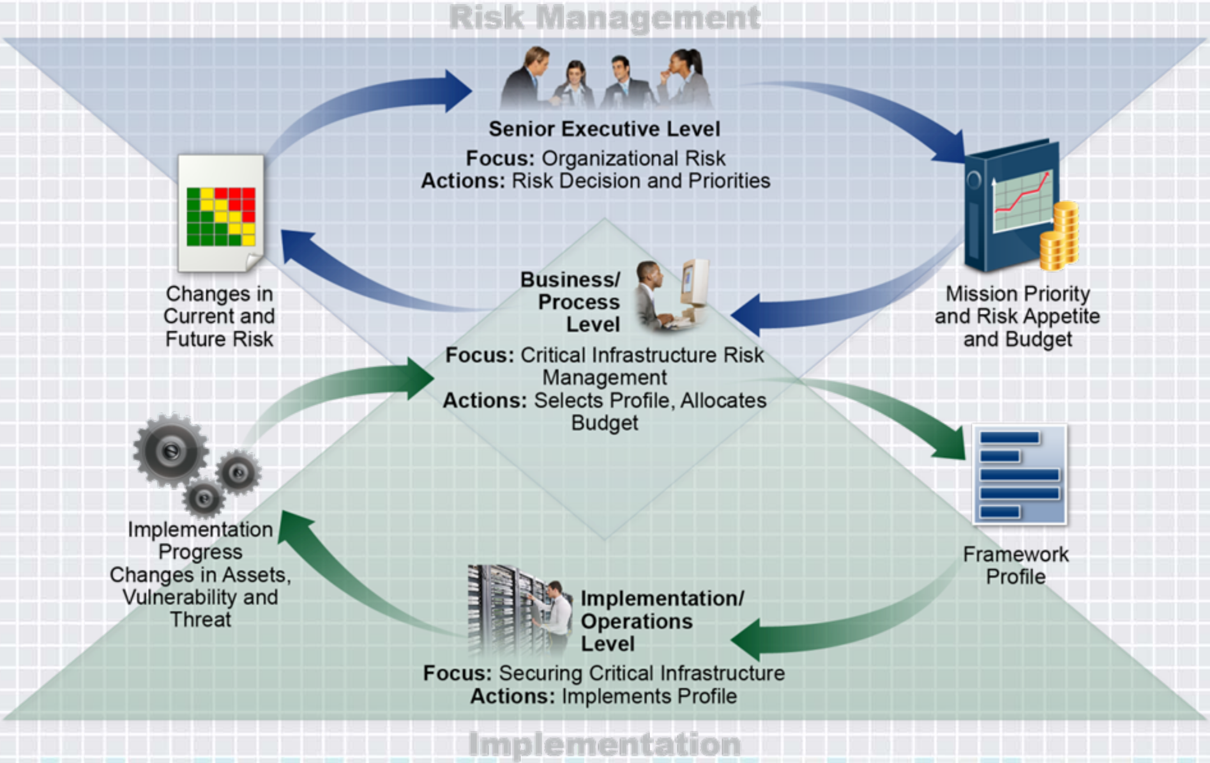
Framework Tiers

Framework Profiles



Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire fo... and third-...	H				

CForum helps users understand how to apply the Framework for communications


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

CForum is an online forum for sharing lessons learned and good practices

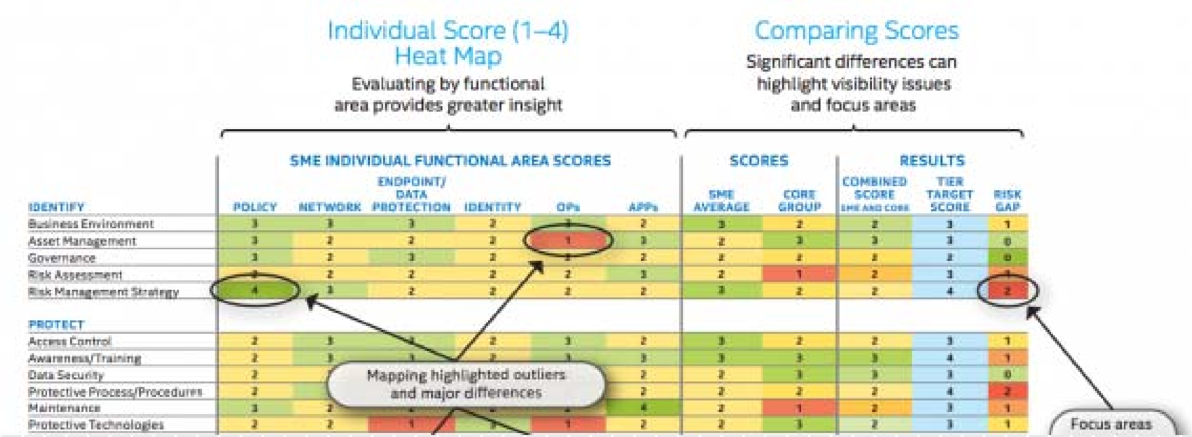
- Industry leaders such as Tony Sager and Mike Brown help spark security conversations
- Several hundred users help ensure a balanced approach
- Relevant topic areas include:
  - Framework specific training and discussion
  - Topics for individual critical information sectors
  - Next iteration of the Framework
  - Implementation Guidance
  - Supply Chain Risk Management

CForum can help identify others' examples of use that can save your organization time

- Apply the Framework's flexibility to achieve organizational cybersecurity goals
- Learn how different organizations use it in different ways with different tools to achieve Framework outcomes

The Cybersecurity Framework in Action: An Intel Use Case

- Intel Corporation described how they used the Framework model to create a heat map for communicating and prioritizing cybersecurity activity among internal functional areas



Individual Score (1–4) Heat Map

Evaluating by functional area provides greater insight

Comparing Scores

Significant differences can highlight visibility issues and focus areas

	SME INDIVIDUAL FUNCTIONAL AREA SCORES						SCORES		RESULTS		
IDENTIFY	POLICY	NETWORK	ENDPOINT/ DATA PROTECTION	IDENTITY	OPs	APPs	SME AVERAGE	CORE GROUP	COMBINED SCORE SME AND CORE	TIER TARGET SCORE	RISK GAP
Business Environment	3	3	3	2	3	2	3	2	2	3	1
Asset Management	3	2	2	2	1	3	2	3	3	3	0
Governance	3	2	3	2	2	2	2	2	2	2	0
Risk Assessment	2	2	2	2	2	3	2	1	2	3	1
Risk Management Strategy	4	3	2	2	2	2	3	2	2	4	2
PROTECT											
Access Control	2	3	3	2	3	2	3	2	2	3	1
Awareness/Training	2	3	3	2	3	3	3	3	3	4	1
Data Security	2	[illegible]	[illegible]	[illegible]	[illegible]	2	2	3	3	3	0
Protective Process/Procedures	2	[illegible]	[illegible]	[illegible]	[illegible]	2	2	2	2	4	2
Maintenance	3	2	2	2	2	4	2	1	2	3	1
Protective Technologies	2	2	1	3	1	2	2	3	2	3	1

Mapping highlighted outliers and major differences

Focus areas

http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

AWWA Guidance and Cybersecurity Tool

American Water Works Association has developed Process Control System Security Guidance for the Water Sector and a supporting Cybersecurity Use-Case Tool.

The AWWA's cybersecurity resources are designed to provide actionable information for utility owner/operators based on their use of process control systems.

http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx

Homeland Security provides valuable resources to apply the Framework model

- DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides the Cyber Security Evaluation Tool (CSET)
- Numerous resources from the Critical Infrastructure Cyber Community (C^{3}) Voluntary Program

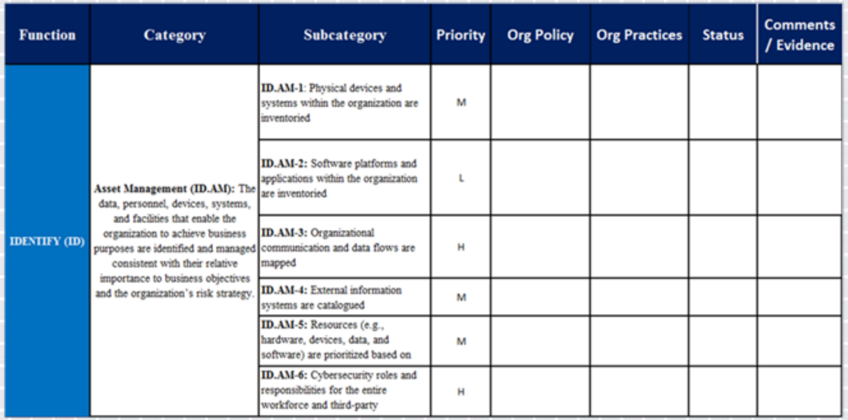
https://ics-cert.us-cert.gov/Assessments

https://www.us-cert.gov/ccubedvp

CForum provides a venue for sharing risk information with other organizations

- ISACs and Sector Coordinating organizations use CForum to share information about emerging threats, and successful incident response methods
- Organizations can compare notes about how to characterize risks & threats
- Users should not share corporate or sensitive data, but general information can protect the community

Why re-invent the wheel? Leverage shared templates to accelerate improvement



Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party	H				

- Take advantage of lessons learned by others
- Jump start use of cybersecurity resources by using shared templates
- Identify opportunities for consistency within and across critical infrastructure sectors

Continue the conversation!

- Federal agencies are jump starting but aren't the long-term solution - management will eventually transfer to "Industry"
- Industry needs to own and lead cybersecurity management practices
- Businesses bring real-world understanding of the challenges and solutions
- Take advantage of the examples and lessons learned
- Help provide topics that speak the language of business

Cyber.SecurityFramework.org