NIST Cybersecurity Framework

CYBR 4400/5400: Principles of Internet Policy, Lecture 6-3

Dr. David Reed, Technology, Cybersecurity, and Policy Program, CU Boulder

Today's Lecture (cont'd)

- Current Events
  - Spies on LinkedIn ...
- Unit #6 Cybersecurity in Crisis: Information and Internet Security
  - 4400/5400B: No Canvas discussion assignment for Unit 6!
  - 5400: No Reading Review assignment for Unit 6!
  - 4400/5400: No homework assignment for Unit 6!
- U.S. Domestic and International Cybersecurity Policy Lecture

Cybersecurity in Crisis: Information and Internet Security (Unit #6)

- Explain U.S. domestic and international cybersecurity policy, and how it relates to the NIST Cybersecurity Framework

- Using the terminology associated with cybersecurity, be able to describe how adversarial cyber operations can result in cyber exploitation

- Explain the economics of cybersecurity, and how this impacts the ability to implement secure networking solutions

Framework for Improving Critical Infrastructure Cybersecurity

March 2017

cyberframework@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Improving Critical Infrastructure Cybersecurity

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

February 12, 2013

Background: Presidential EO 13636 - Improving Critical Infrastructure Cybersecurity (Feb 2013)

- Develop technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

US Domestic Policy on Cybersecurity

Presidential Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May, 2017)

Presidential Executive Order 13800

- Policy to solve four problems
  - Secure federal networks
  - Encourage collaboration with industry to protect critical infrastructure
  - Strengthen deterrence posture of the United States and build international coalitions
  - Build a stronger cybersecurity workforce

Section 1 Cybersecurity of Federal Networks

- Dept/Agency heads accountable for managing cybersecurity risk
  - Undertake risk management measures commensurate with magnitude of harm
    - **<u>Use NIST Cybersecurity framework</u>** and provide report in 90 days
- Focus on assessing and reducing risk to improve cybersecurity using best practices, tools and services that are cloud-based
- Determine to use shared IT services such as email, cloud and cybersecurity services
  - Gather info on IT architectures and plans to determine technical feasibility and cost effectiveness of transitioning all agencies to one or more consolidated network architectures and shared IT services

Section 2 Cybersecurity of Critical Infrastructure

- Focus on how to best support cybersecurity of critical infrastructure through policies and stakeholder engagement
- Discuss with stakeholders how federal capabilities can best support designated critical infrastructure
- Commerce and DHS to promote actions to reduce risks from distributed, automated attacks (i.e., botnets)
- Assess potential scope/duration of power outage associated with significant cyber incident against electric grid

The Cybersecurity Framework...

- Includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.
- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.
- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations.
- Is consistent with voluntary international standards.

The Framework Is for Organizations…

- Of any size, in any sector in (and outside of) the critical infrastructure.
- That already have a mature cyber risk management and cybersecurity program.
- That don't yet have a cyber risk management or cybersecurity program.
- Needing to keep up-to-date managing risks, facing business or societal threats.
- In the federal government, too…since it is compatible with Federal Information Security Management Act (FISMA) requirements and goals.

Continued Improvement of Critical Infrastructure Cybersecurity

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

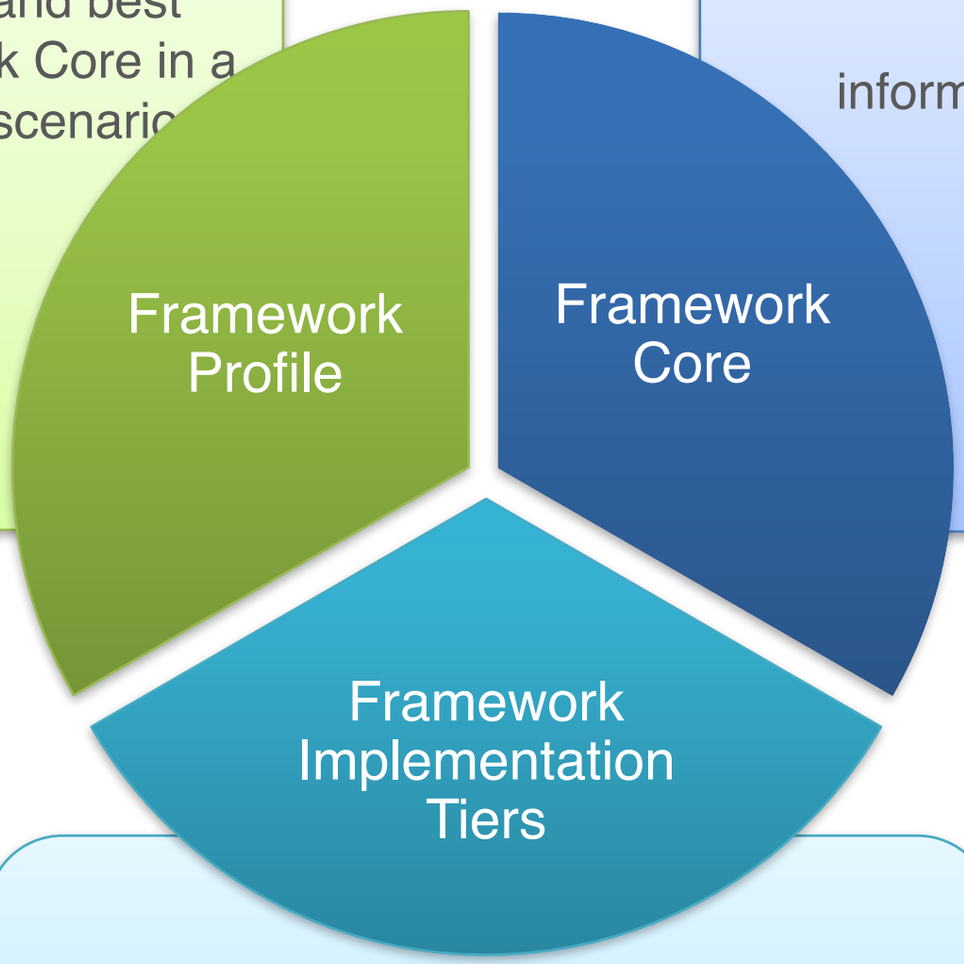
"…on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"

Cybersecurity Enhancement Act of 2014
(P.L. 113-274)
18 December 2014

Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Core

Cybersecurity Framework Component

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	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**

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

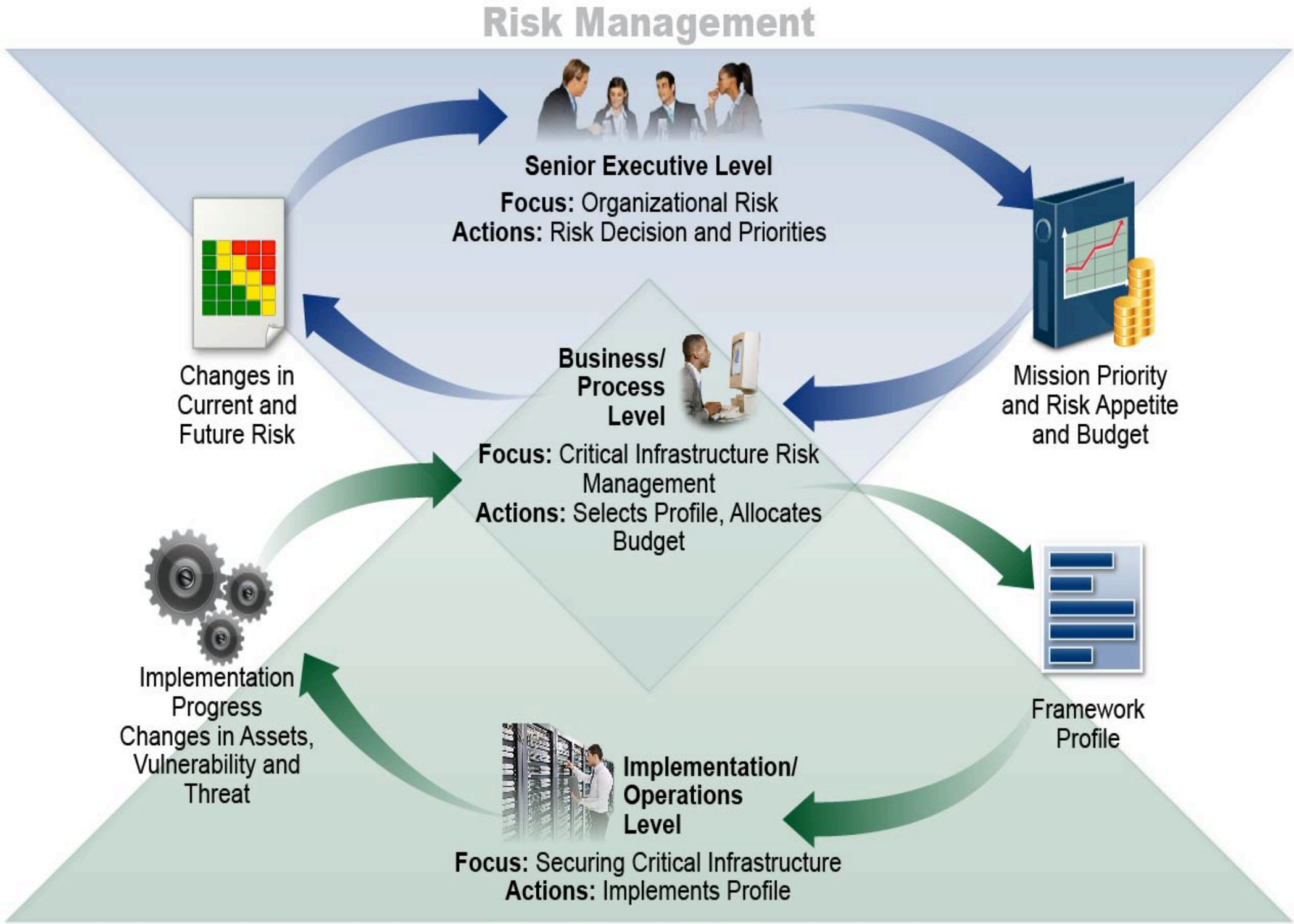
Core

Cybersecurity Framework Component

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	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** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** 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 **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	**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	**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

Supporting Risk Management with Framework



Framework Implementation Tiers

- Framework Implementation Tiers were proposed to reflect how an organization implements the Framework Core functions and manages its risk.

- The Tiers are progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier.

- The Tiers describe increasing degree of rigor in risk management practices and extent actions informed by business needs.

- The Tier characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.

Implementation Tiers

	1	2	3	4
	Partial	Risk Informed	Repeatable	Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization benefits by sharing or receiving information from outside parties			

Example of Organization at Partial Implementation Tier

	1			
	Partial			
Risk Management Process	Cybersecurity risk management is ad hoc and reactive; activities not directly informed by risk objectives			
Integrated Risk Management Program	Limited awareness of organizational risk; lack of any risk management approach, instead using case-by-case strategy. May not have processes that enable cybersecurity info sharing.			
External Participation	May not coordinate or collaborate with other entities			

Example of Organization at Adaptive Implementation Tier

			4
			Adaptive
Risk Management Process	Adapts its practices based on lessons learned and predictive indicators derives from previous cybersecurity activities; continuously improving practices quickly adapt to new threats		
Integrated Risk Management Program	Organization wide approach to managing risk using risk-informed policies; cybersecurity risk management part of organizational culture, evolves from awareness of activities		
External Participation	Actively shares info with partners to ensure accurate, up-to-date info sharing		

Framework Profile

- Alignment of Functions, Categories, and Subcategories with business requirements, risk tolerance, and resources of the organization

- Enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities

- Can be used to describe current state or desired target state of cybersecurity activities

Uses of the Cybersecurity Framework

The Framework is designed to complement existing business and cybersecurity operations, and can be used to:

- Understand security status
- Establish / Improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers
- Identify opportunities for new or revised standards
- Identify tools and technologies to help organizations use the Framework
- Integrate privacy and civil liberties considerations into a cybersecurity program

Key Attributes

It's a framework, not a prescriptive standard

- Provides a common language and systematic methodology for managing cyber risk.
- Is meant to be adapted.
- Does not tell an organization *how* much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.
- Enable best practices to become standard practices for everyone via common lexicon to enable action across diverse stakeholders.

It's voluntary

It's a living document

- It is intended to be updated as stakeholders learn from implementation, and as technology and risks change…more later.
- That's one reason why the Framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principles will not.