Securing Space Systems and Assets

The Need for Multidimensional Protection in the 21st Century

Ron Ross

Complexity

Millions, Billions, and Trillions of Everything

From Earth to Space

Ubiquitous Connectivity Produces Shared Risk

Exfiltrate information

Preposition malicious code

Bring down capability

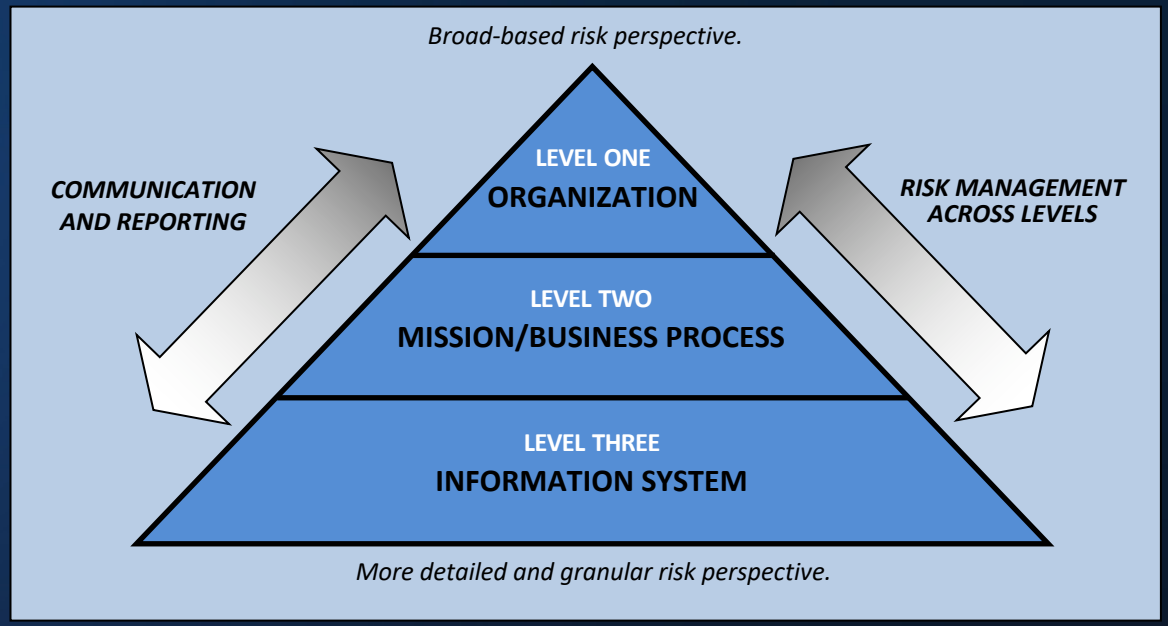
Create deception

Defense Science Board Reports

Space Systems Security: An Organizational Perspective

Key Elements

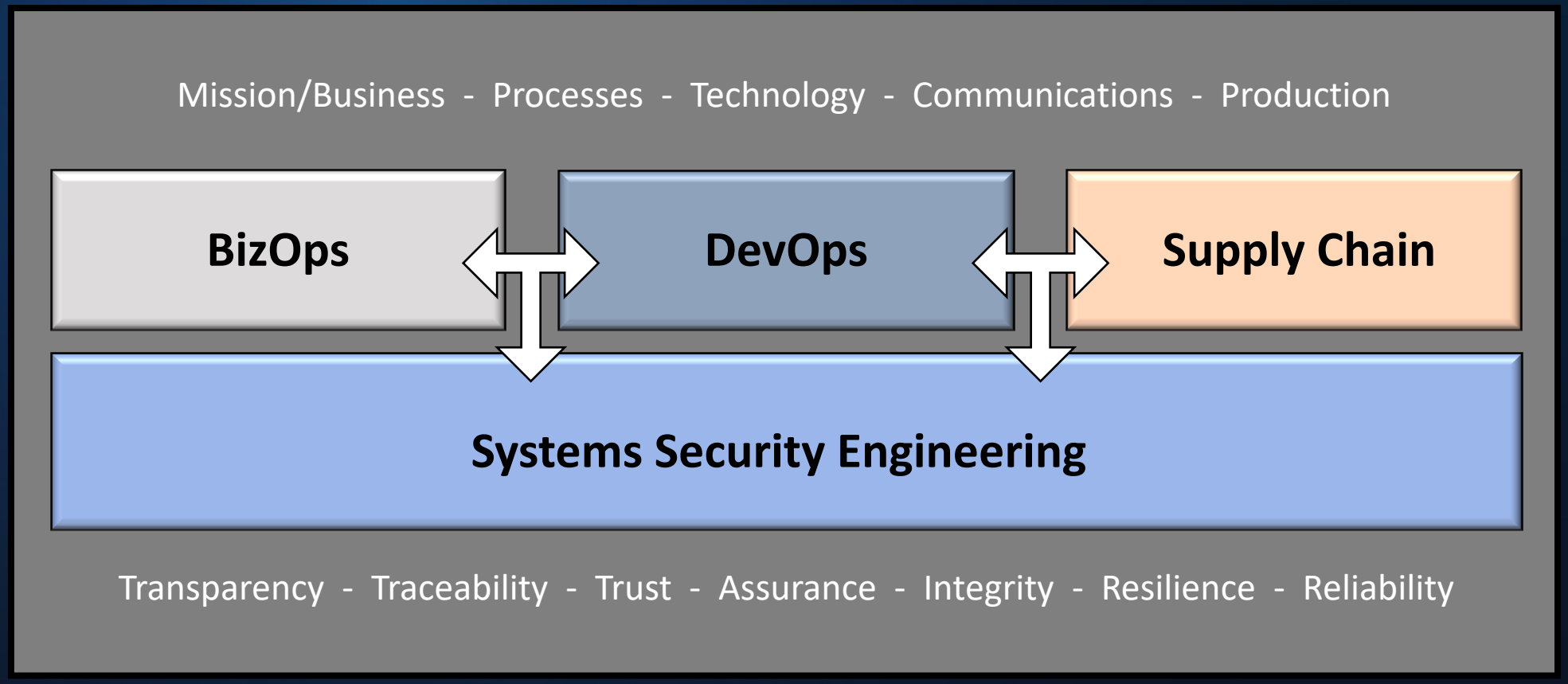
- **Mission and business driven security requirements**
- **Traceability of security requirements from the boardroom to implementation**
- **Transparency of security architectures**
- **Assurance and trust in space platforms**



Courtesy: NIST Special Publication 800-37, Revision 2

The Vision

Framework for Securing Space Systems and Assets



NIST Tools for Protecting Space Assets

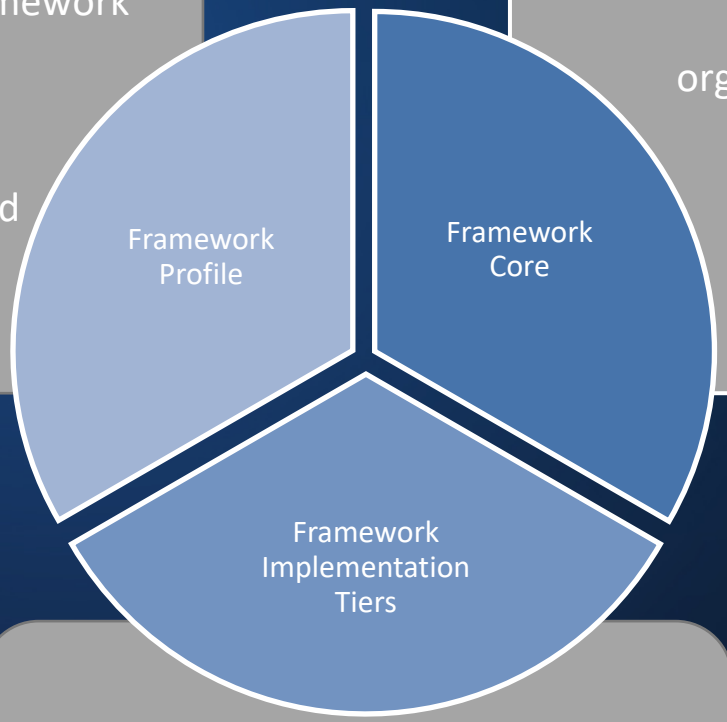
- Frameworks
- Controls
- Engineering Processes
- Technical Guidelines
- Training

https://csrc.nist.gov

Cybersecurity Framework

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

Supports prioritization and measurement while factoring in business needs



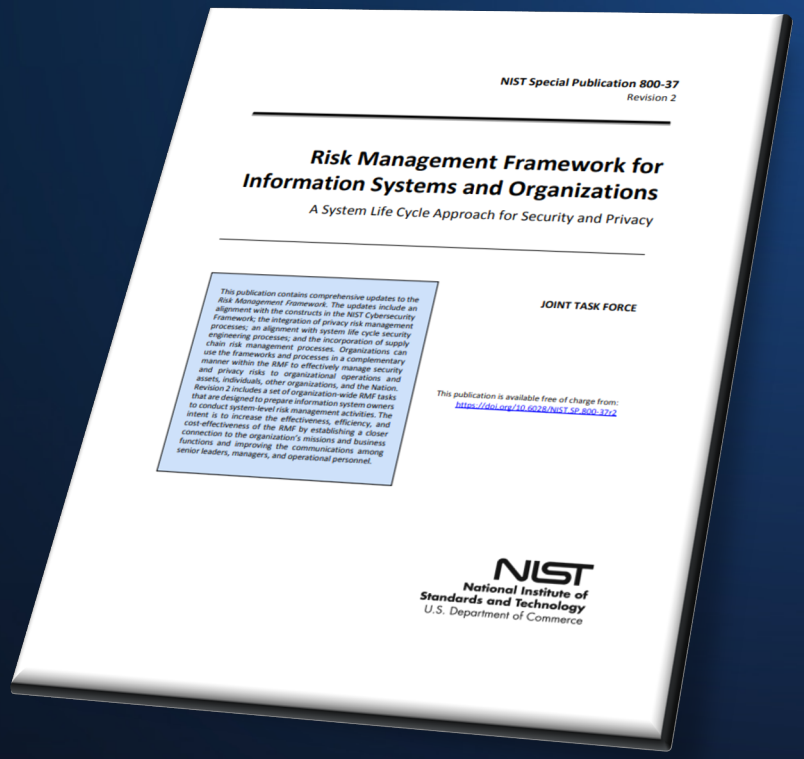
Cybersecurity activities and informative references, organized around particular outcomes

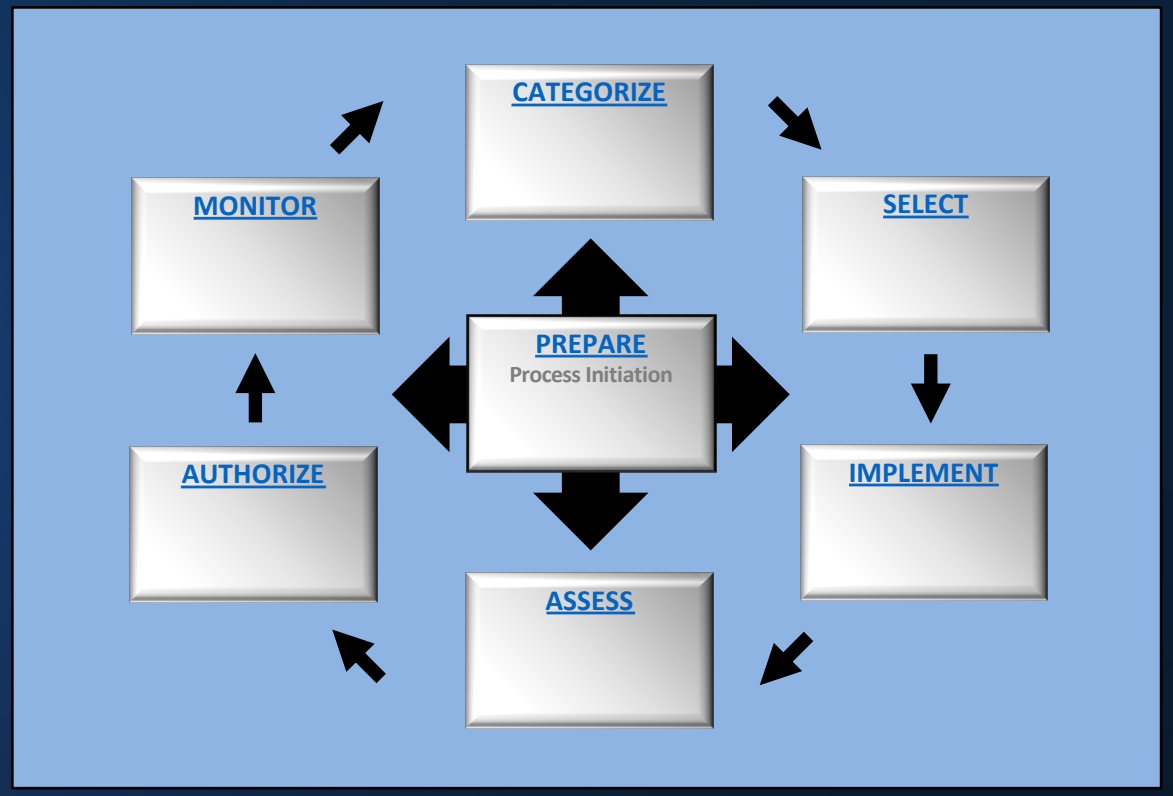
Enables communication of cyber risk across an organization

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

https://www.nist.gov/cyberframework

Managing Risk in Space Systems



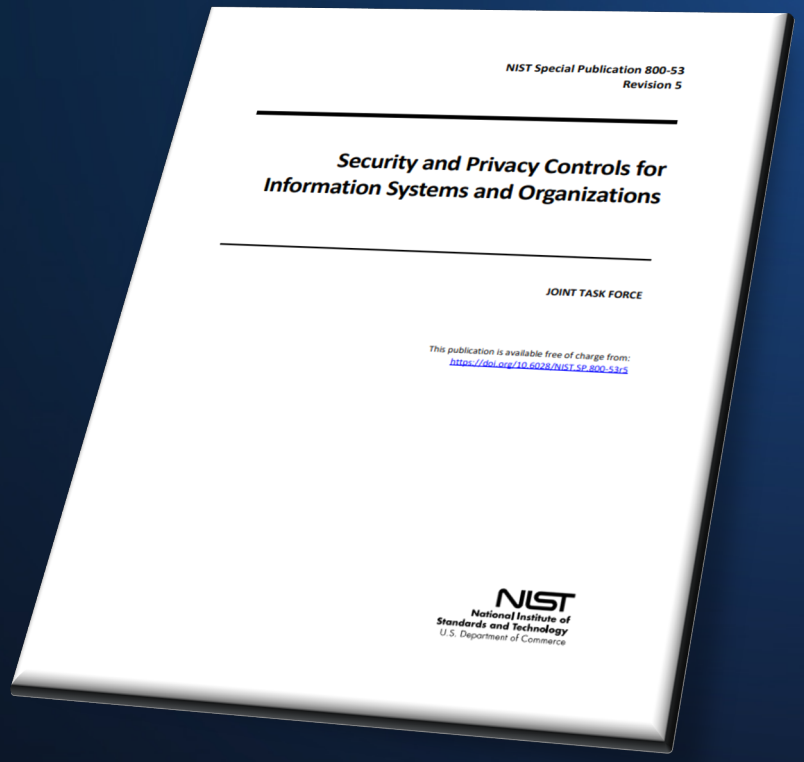


Courtesy: NIST Special Publication 800-37, Revision 2

- **New control selection process supports space systems and cyber-physical systems**

https://csrc.nist.gov/projects/risk-management

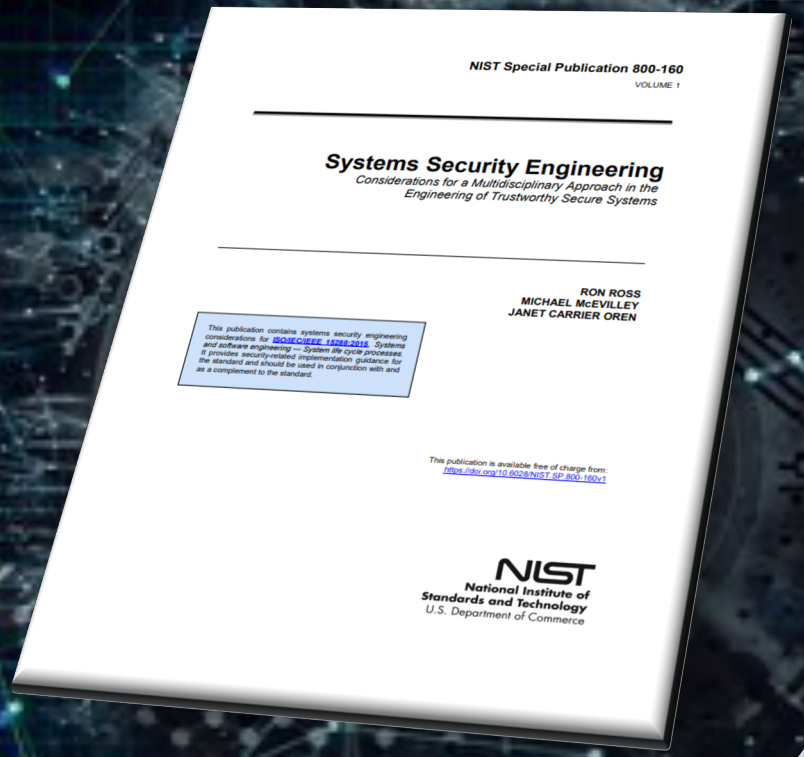
Controls for Space Systems



ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
CP	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Courtesy: NIST Special Publication 800-53, Revision 5

- New privacy control family and privacy integration throughout the control catalog
- New supply chain risk management control family
- Systems security engineering controls
- New state-of-the-practice controls to counter advanced threats



Multidimensional Protection Strategy

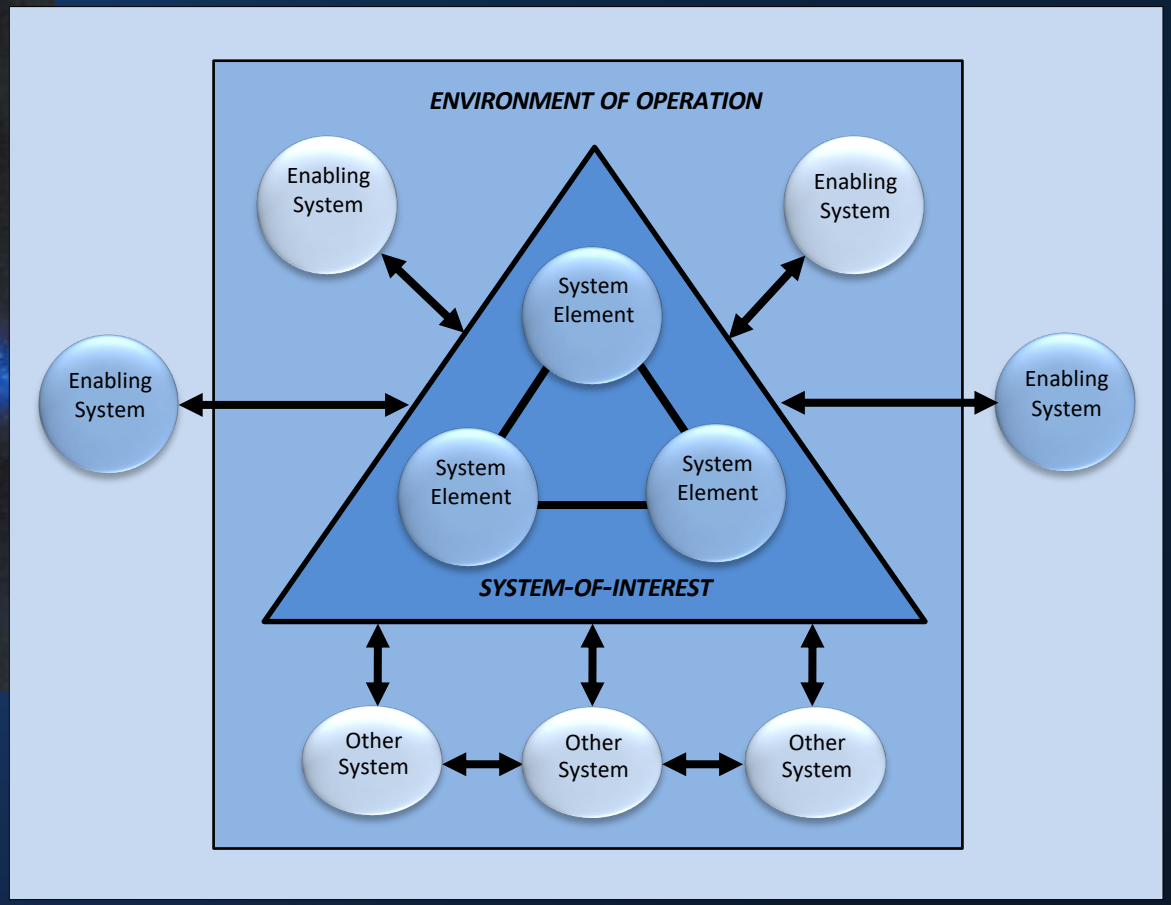
- Penetration-resistant architecture
- Damage-limiting operations
- Designs to achieve cyber resiliency and survivability

Stop the incursion…
Limit the damage after the incursion has occurred…
Continue to operate even in a degraded or debilitated state.

Space Assets

Systems Engineering View

Critical interdependencies and relationships among internal system elements, systems within enterprise environments, and systems in external environments that affect security solutions.



Courtesy: NIST Special Publication 800-160, Volume 1

Systems Security Engineering

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

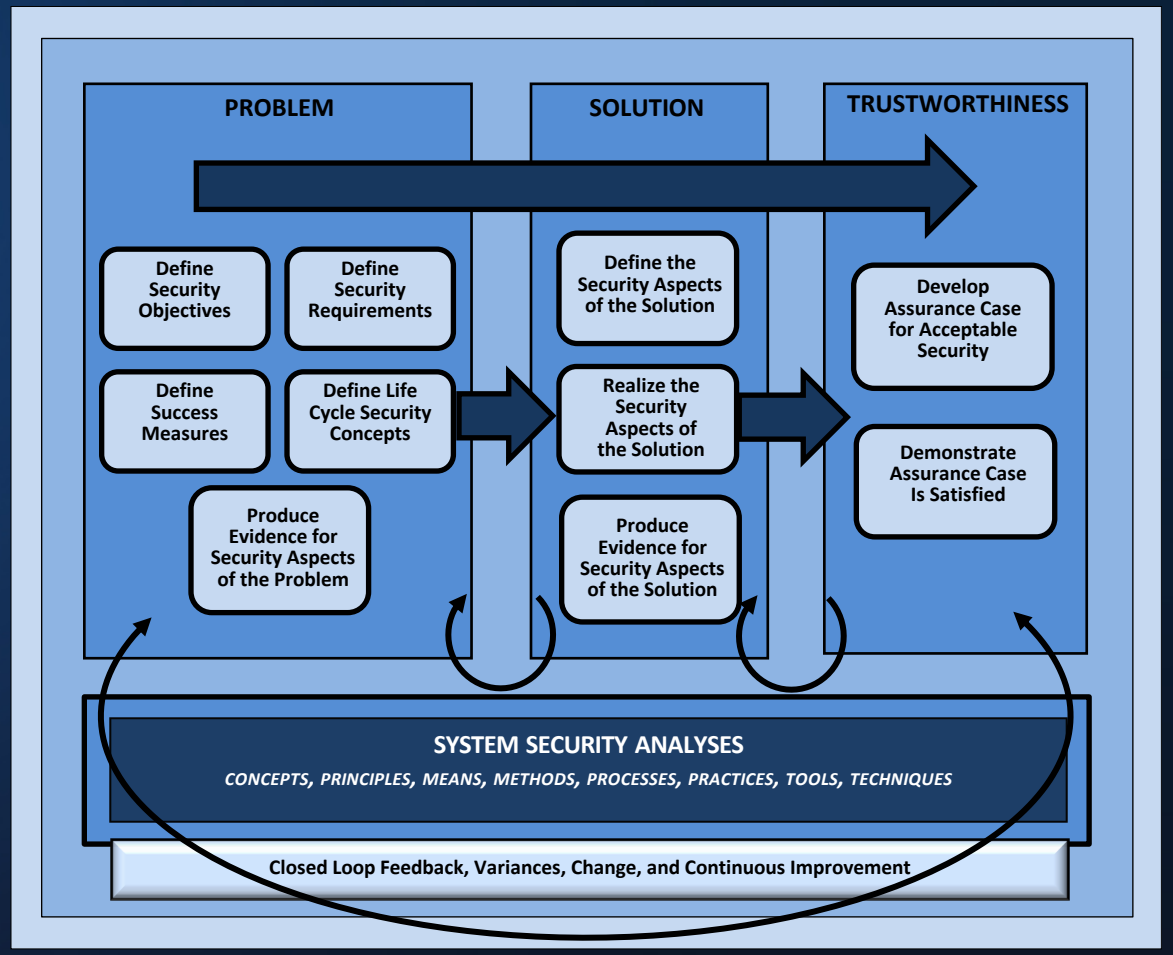
- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - Architecture definition
        - Design definition
          - System analysis
            - Implementation
            - Integration
          - Verification
        - Transition
      - Validation
    - Operation
  - Maintenance
- Disposal

NIST SP 800-160 Volume 1

Systems Security Engineering

Characteristics

- Disciplined and structured development process
- Integrates security into the system life cycle
- Applied to all elements in the system stack
- Can be tailored and implemented in agile development processes
- Provides needed traceability of requirements and transparency into development processes leading to greater trust in systems and system elements



Courtesy: NIST Special Publication 800-160, Volume 1

Systems Security Engineering

Key Concerns

- Architecture
- Assurance
- Behavior
- Cost
- Criticality
- Design
- Effectiveness
- Emergence
- Ergonomics
- Exposure
- Fit-for-purpose
- Human performance
- Life cycle concepts
- Penetration resistance
- Performance
- Privacy
- Protection needs
- Requirements
- Risk
- Security objectives
- Strength of function
- Security performance
- Threat
- Trades
- Training
- Uncertainty
- Vulnerability
- Verification
- Validation

Cyber Resiliency

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

CYBER RESILIENCY SOLUTION

RISK MANAGEMENT STRATEGY

Programmatic

- Organizational Level
- Mission/Business Process Level
- System Level

Inform selection and prioritization

Why

Interpret, determine priorities of, and define strategies for achieving

GOALS

- Anticipate
- Withstand
- Recover
- Adapt

OBJECTIVES

- Understand
- Prevent/Avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-architect

Can be further decomposed into sub-objectives and capabilities.

What

Inform selection and prioritization

How

Selection, prioritization, and application informed by programmatic, operational, and technical considerations, including threat considerations.

STRATEGIC DESIGN PRINCIPLES

Inform selection and prioritization

STRUCTURAL DESIGN PRINCIPLES

APPROACHES

TECHNIQUES

Inform selection and prioritization

Cyber resiliency relationships with other specialty engineering disciplines

On the Horizon

2021 Initiatives

- **Update NIST Publication 800-53A to provide assessment procedures for security and privacy controls**
- **New web-based, automated control content development and delivery system**
- **DevSecOps and systems security engineering framework**

“If a full on ‘turn the lights off’ cyber war were to happen today, we would lose. Think about that. We would lose a cyber war. With a few clicks of the mouse, and in just a few seconds, hackers in Beijing or Moscow could turn off our electricity, millions would lose heat, groceries would spoil, banking machines would not work, and people could not get gasoline. It would be what we have seen down in Texas, but on national scale and with no end in sight. That we have escaped a digital catastrophe thus far is not due to skill. It is due to blind luck and restraint from our adversaries.”

Mike Rogers, February 23, 2021
Former Member of Congress, House Intelligence Committee
https://thehill.com/opinion/cybersecurity/539826-we-would-not-survive-true-first-strike-cyberattack

Questions?

Ron Ross

Email: **ron.ross@nist.gov**

Mobile: **(301) 651-5083**

Web: **http://csrc.nist.gov**

Twitter: **https://twitter.com/ronrossecure**

LinkedIn: **https://www.linkedin.com/in/ronrossecure**