Resiliency Rules:

7 Steps for Resiliency in Critical Infrastructure Protection

Phil Sodoma
Director, International Security Strategy
Trustworthy Computing Group
Microsoft

Resiliency Rules

7 Steps for Resiliency in Critical Infrastructure Protection

Government, infrastructure owners/operators can collaboratively pursue these core enablers of resiliency and infrastructure security

1. Define Goals and Roles
2. Identify and Prioritize Critical Functions
3. Continuously Assess and Manage Risks
4. Establish and Exercise Emergency plans
5. Create Public-Private Partnerships
6. Build Security/Resiliency into Operations
7. Update and Innovate Technology/Processes

CIP Goals

Establishing Clear Goals is Central to Success

Policy Elements	Sample Statement
Critical Infrastructure Importance	Critical information infrastructures (CII) provide the essential services that support modern information societies and economies. Some CII support critical functions and essential services so vital that the incapacitation, exploitation, or destruction, through natural disaster, technological failure, accidents or intentional attacks could have a debilitating effect on national security and economic well-being.
Critical Infrastructure Risks	CII exploitation, or destruction, through natural disaster, technological failure, accidents or intentional attacks could have a debilitating effect on national security and economic well-being.
CIP Policy Goal/Statement	Prevent or minimize disruptions to critical information infrastructures, no matter the source, and thereby help to protect the people, the economy, essential human and government services, and the national security. In the event disruptions do occur, they should be infrequent, of minimal duration, and manageable.
Public-Private Implementation	Implementing the National CIIP framework includes government entities as well as voluntary public-private partnerships involving corporate and nongovernmental organizations.

CIP Roles

Understanding Roles Promotes Coordination

Government

"What's the goal"

Public-Private Partnership

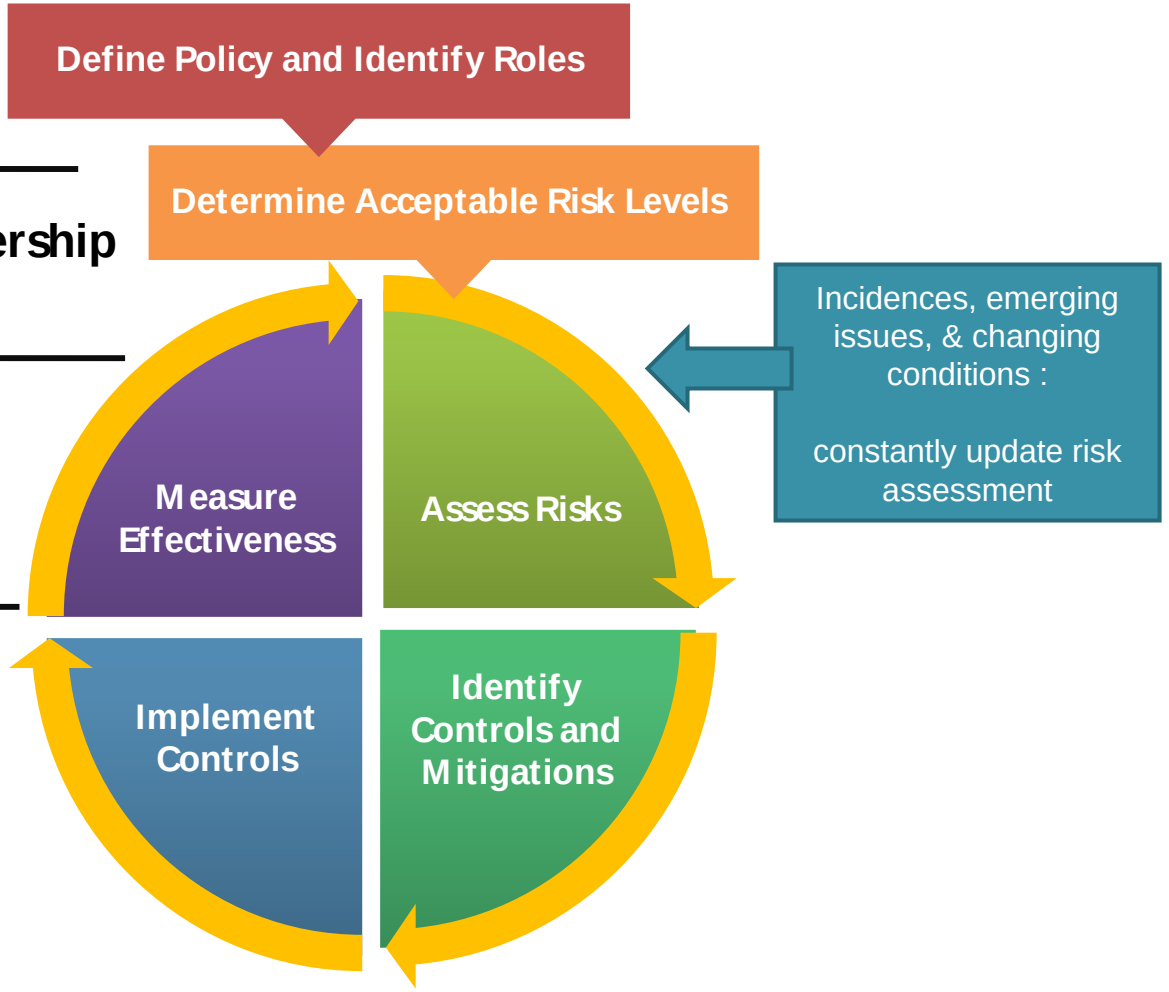
"What's critical"

Infrastructure

"Prioritize Risks"

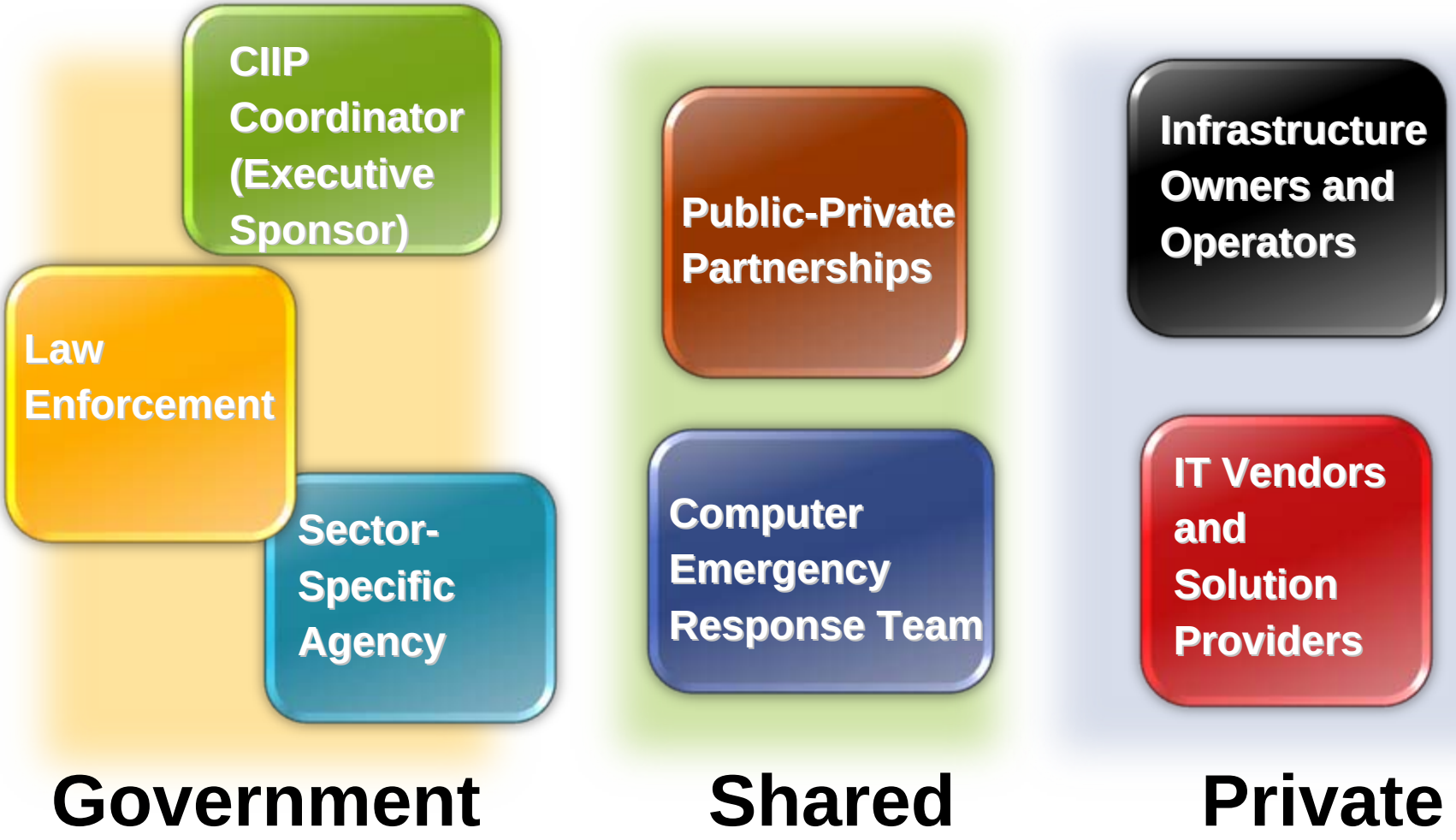
Operators

"Best control solutions"



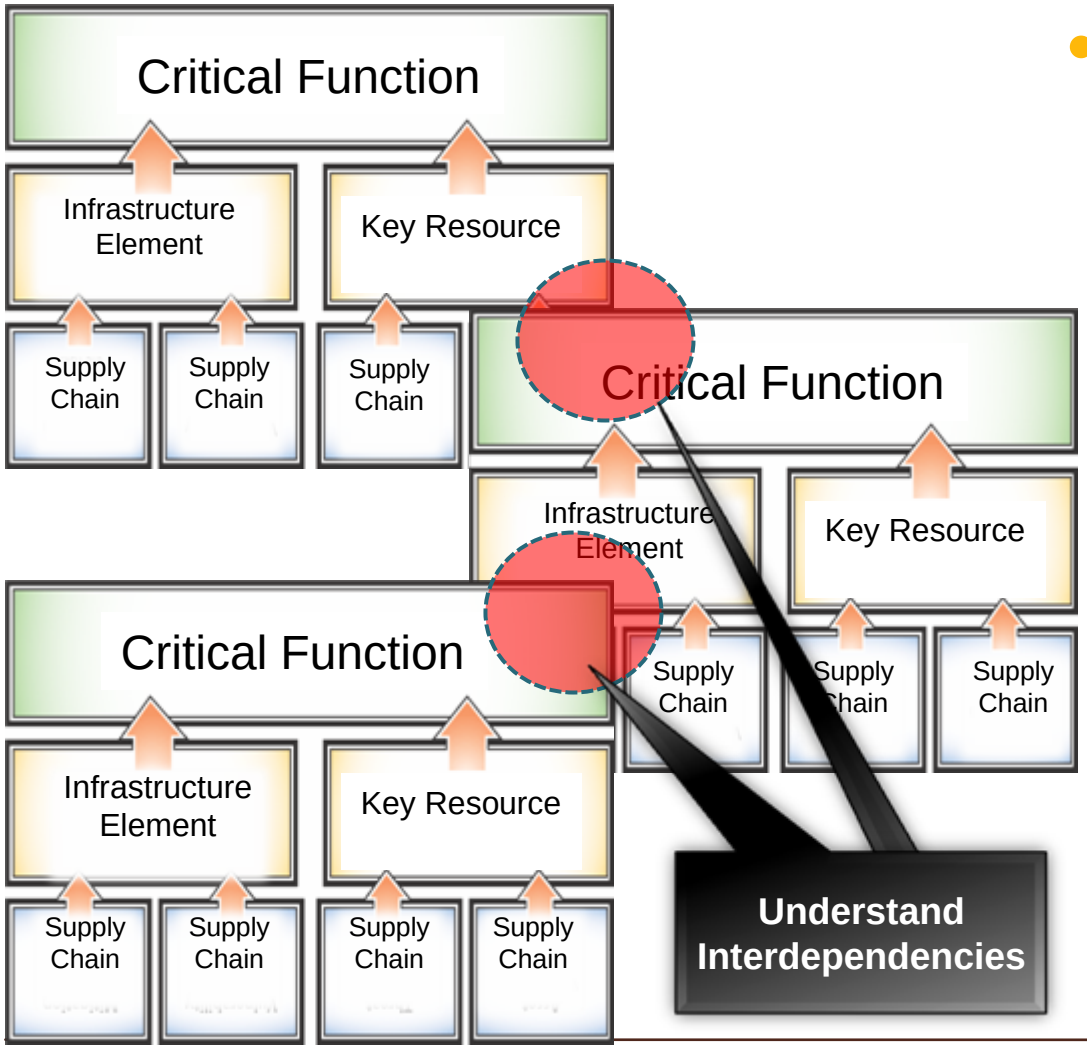
Define Roles

Understanding roles and objectives promotes trust and efficiency



Identify and Prioritize Critical Functions

Collaborate to understand Interdependencies



- Establish an open dialogue to understand the critical functions, infrastructure elements, and key resources necessary for:
  - delivering essential services,
  - maintaining the orderly operations of the economy, and
  - helping to ensure public safety.

Continuously Assess and Manage Risks

Protection is the Continuous Application of Risk Management

- Evaluate Program Effectiveness
- Leverage Findings to Improve Risk Management

- Identify Key Functions
- Assess Risks
- Evaluate Consequences

Incidences, emerging issues, & changing conditions :

constantly update risk assessment

- Define Functional Requirements
- Evaluate Proposed Controls
- Estimate Risk Reduction/Cost Benefit
- Select Mitigation Strategy

- Seek Holistic Approach
- Organize by Control Effectiveness
- Implement Defense-in-Depth

Establish and Exercise Emergency plans

Improve Operational Coordination

- Public- and private-sector organizations alike can benefit from developing joint plans for managing emergencies, including recovering critical functions in the event of significant incidents, including but not limited to:
  - natural disasters
  - terrorist attacks
  - technological failures
  - accidents.
- Emergency response plans can mitigate damage and promote resiliency.
- Effective emergency response plans are generally short and highly actionable so they can be readily tested, evaluated, and implemented.
- Testing and exercising emergency response plans promotes trust, understanding, and greater operational coordination among public- and private-sector organizations.
- Exercises also provide an important opportunity to identify new risk factors that can be addressed in response plans or controlled through regular risk management functions.

Create Public-Private Partnerships

Collaboration is key to protecting critical infrastructure

- Voluntary public-private partnerships
  - Promote trusted relationships needed for information sharing and collaborating on difficult problems
  - Leverage the unique skills of government and private sector organizations
  - Provide the flexibility needed to collaboratively address today's dynamic threat environment

Build Security & Resiliency into Infrastructure

Security is a continuous process

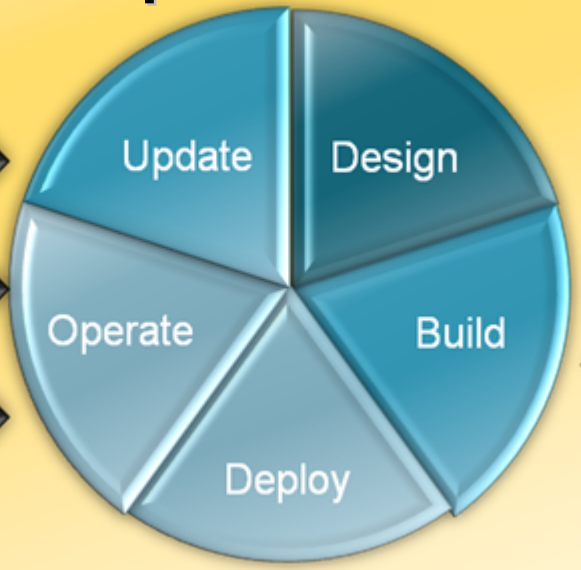
Building security and resiliency into infrastructure operations

Critical Functions
(Global, National, Local)

Infrastructure Operations

Security Controls

- **Management**
- **Technical**
- **Operational**



Fosters increased security and resiliency for the critical functions that support safety, security and commerce at all levels

Update and Innovate Technology/Processes

Mitigate threats by keeping technology current and practices innovative

- Cyber threats are constantly evolving
- Policymakers, enterprise owners, and infrastructure operators can prepare for changes in the threat landscape by:
  - Monitoring trends
  - Keeping systems updated
  - Maintaining the latest versions of software that have been built for the current threat environment

Questions?

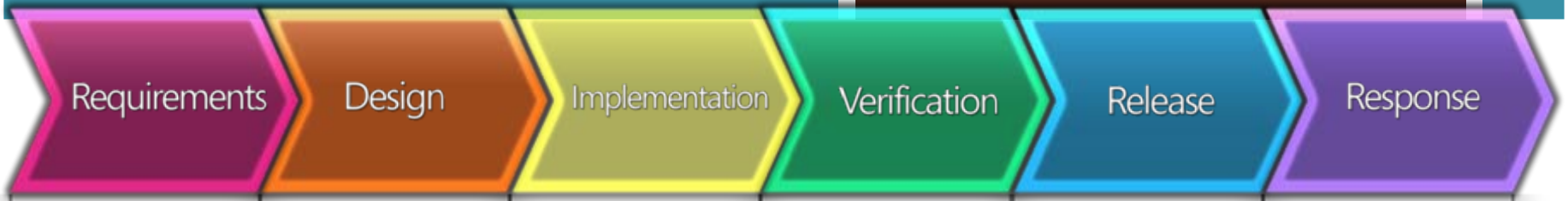
Appendix

Security Development Lifecycle (SDL)

Security is a continuous process

The Security Development Lifecycle

Driving Change Across Microsoft



Product Inception
- Assign security advisor
- Identify security milestones
- Plan security integration into product

Design
- Define security architecture and design guidelines
- Document elements of software attack surface
- **Threat Modeling**

Standards, best practices, and tools
- Apply coding and testing standards
- Apply security tools (fuzzing tools, static-analysis tools, etc.)

Security Push
- Security code reviews
- Focused security testing
- Review against new threats
- Meet signoff criteria

Final Security Review
- Independent review conducted by the security team
- Penetration testing
- Archiving of compliance info

RTM and Deployment
- Signoff

Security Response
- Plan and process in place
- Feedback loop ~~back~~ into the development process
- Postmortems

Microsoft Innovations Drive Comprehensive Security