An Overview of the CERT Resilience Management Model (CERT-RMM)

Katie Stewart

Senior Engineer

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

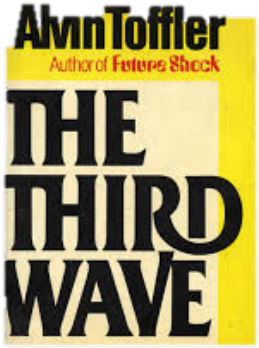
DM18-0487

About me

NC STATE UNIVERSITY

CISCO SYSTEMS

Wharton
UNIVERSITY of PENNSYLVANIA



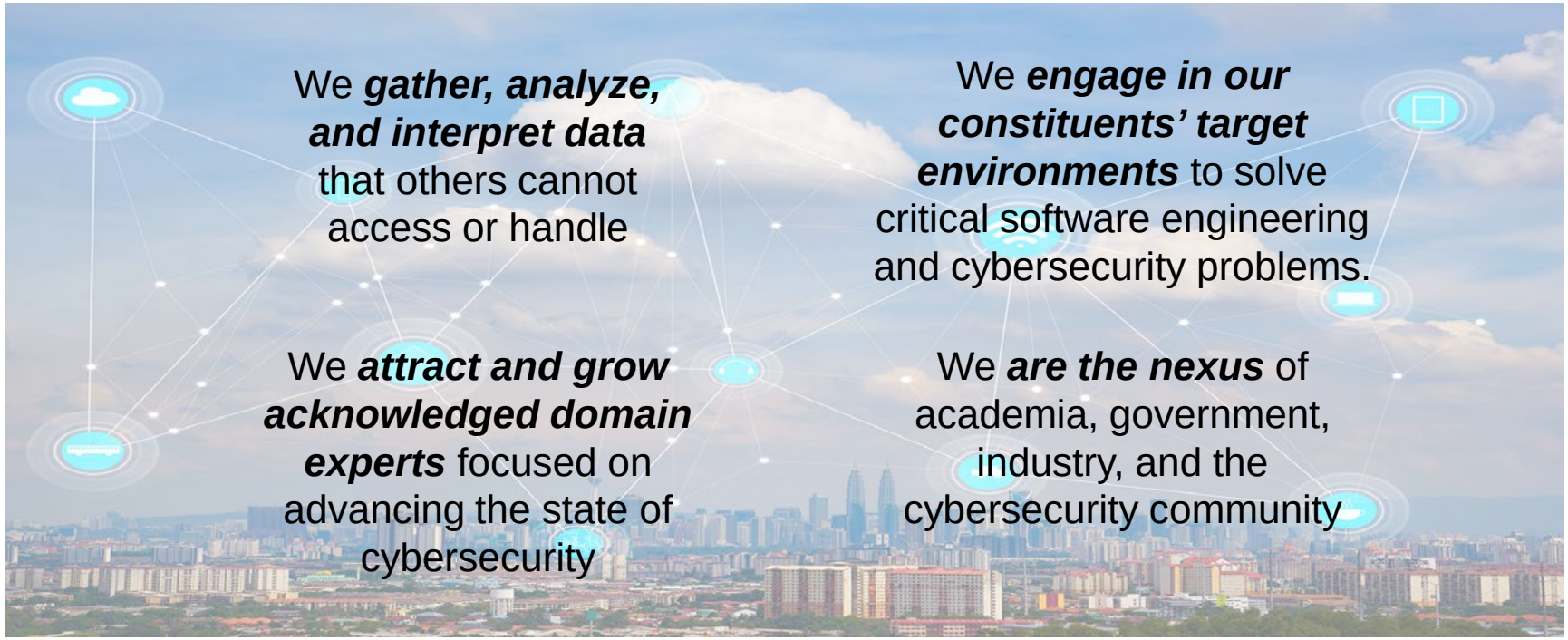
NORTHROP GRUMMAN

Carnegie Mellon University
Software Engineering Institute

CERT Program

Carnegie Mellon University
Software Engineering Institute

Mission: To anticipate and solve the nation's most challenging cybersecurity problems



Cybersecurity Risk and Resilience

To protect and sustain assets that are important to the nation's cyber-dependent mission ensuring that they continue to operate during and recover from disruptive events.

Cybersecurity Assurance: Advance the state of the practice of cybersecurity evaluation (technical and process) and support the ability of critical infrastructure providers and government organizations to achieve missions dependent on cyber assets.

Cybersecurity Risk Management: Research, develop, and deploy processes, tools, and solutions to public and private customers that enable operational surety in times of distress.

Enterprise Threat & Vulnerability Management: Research and develop technical and behavioral policies, processes, and controls to discourage, detect, and contain malicious and non-malicious insider threats

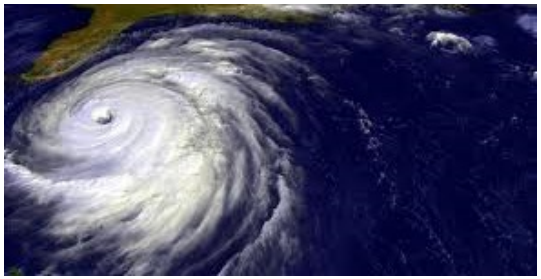
Operational Resilience – *The CliffsNotes Version*

Enterprise Risk Management

Looks across all types of risk activities in the organization and considers all types of risks

Connects risk management to strategic and business drivers

Why do operational risks matter?



Internal Process Failures

- Trust and confidence of employees and customers
- Reputation and image
- Regulatory compliance, fines, legal penalties
- Customer retention and growth
- Life, safety, and health of customers and employees
- Productivity and profitability
- Organizational survival

! ...because they have explicit and direct IMPACT

https://www.bleepingcomputer.com/news/technology/us-telco-fined-3-million-in-domain-renewal-blunder/

Failed Internal Processes – A Closer Look

US Telco Fined $3 Million in Domain Renewal Blunder

By Catalin Cimpanu October 2, 2017 10:50 AM 0

Sorenson Communications, a Utah-based telecommunications provider, received a whopping $3 million fine from the Federal Communications Commission (FCC) on Friday for failing to renew a crucial domain name used by a part of the local 911 emergency service.

The affected service was the Video Relay System (VRS), a video calling service that telecommunication firms must provide to deaf people and others people with vocal disabilities so they can make video calls to 911 services and use sign language to notify operators of an emergency or crime.

- On June 6, 2017, Sorenson Communications failed to renew their domain name which ran their Video Relay System that supports 911 services for the deaf and those with vocal disabilities.
- The system was down for 3 days.
- The FCC investigated and found this was preventable and imposed a $2.7M fee, $250K which was a fine.

https://www.bleepingcomputer.com/news/technology/us-telco-fined-3-million-in-domain-renewal-blunder/

With cyber risk, who is the enemy?

But what about…

- John from accounting
- Your CEO
- Logan your international business developer
- The escalator repair man
- The really smart college grad you just hired

Operational Risk Management

A form of risk affecting day-to-day business operations

A very broad risk category

- From high-frequency low-impact to low-frequency high-impact

Exacerbated by

- Actions of people
- System and technology failures
- Failed internal processes
- External events

Operational Resilience emerges from effective management of operational risk.

What Do We Mean by *Operational Resilience*?

Operational resilience: the organization's ability to adapt to risk that affects its core operational capacities; the **emergent property** of an organization that can **continue to carry out its mission** after *disruption* that does not exceed its *operational* limit

"…the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"
–Presidential Policy Directive – PPD 21
Critical Infrastructure Security and Resilience
February 12, 2013

What Makes an Entity Operationally Resilient?

Operational resilience is an emergent property;
it emerges from things we do:

identifying and mitigating risks to services and related assets

performing service continuity processes and planning

managing IT operations practices

managing and deploying people

protecting (control) and securing important information and technology assets

managing external partners (that support the services supply chain)

managing environmental factors (where the service “lives”)

Cyber Resilience Value Proposition

Management – gaining support for simplifying complex cybersecurity challenges

Efficiency – establishing equilibrium by

- Balancing risk and cost (most bang for your buck)
- Achieving compliance as a by-product of resilience management

Standardization – identifying what to do by

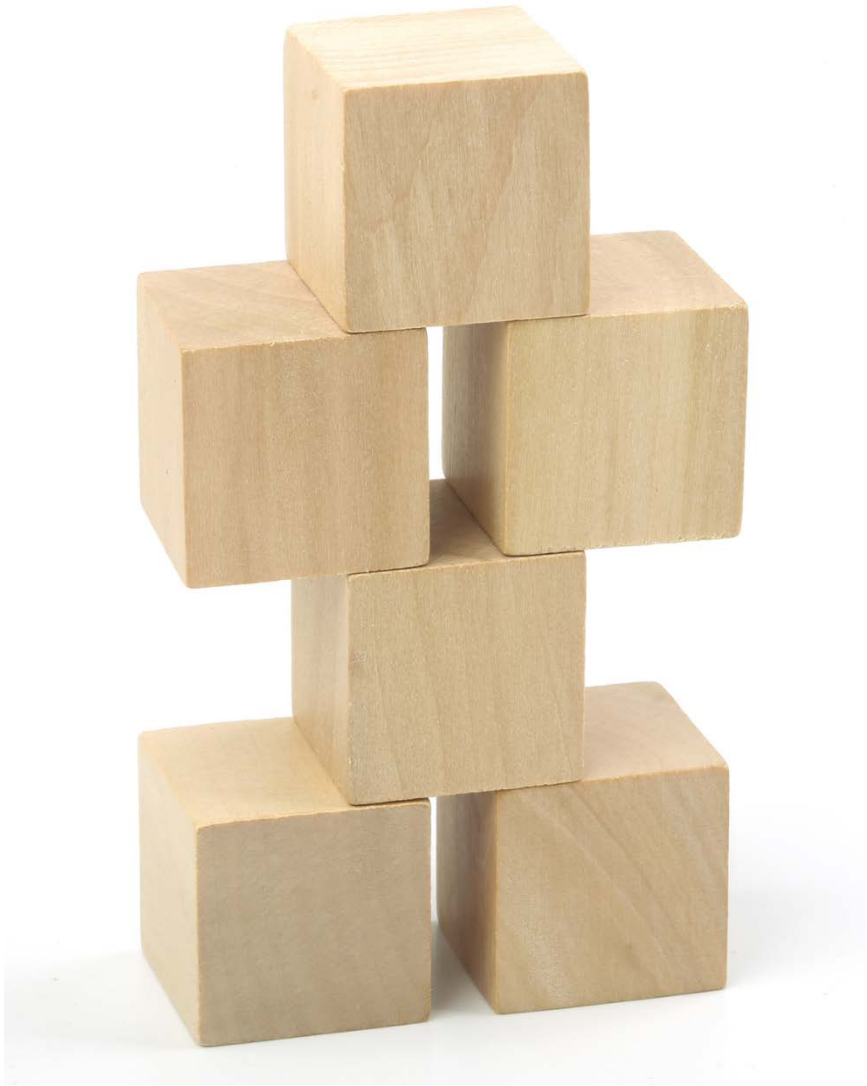
- Using an overarching, standardized approach
- Focusing time and effort on what needs to be protected

Ecosystem – managing

- Interdependencies
- Internal and external organizational challenges and silos

Converging Resilience Management

Building Blocks of Resilience Management



Services and Products

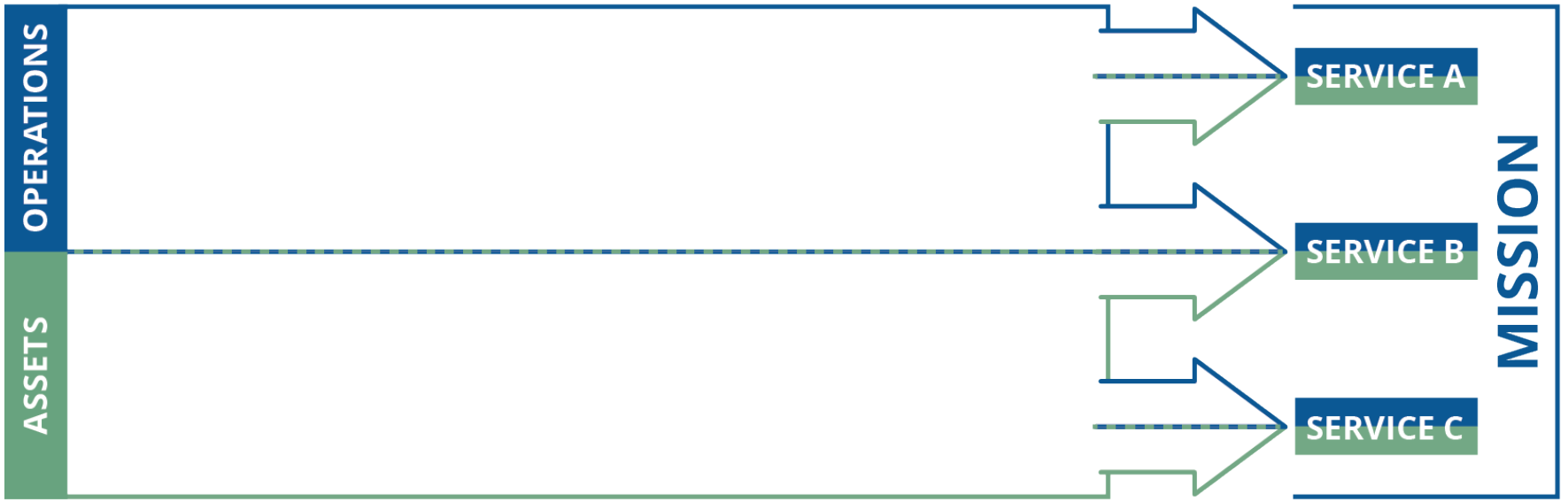
Assets

Resilience Requirements

Protection and Sustainment Activities

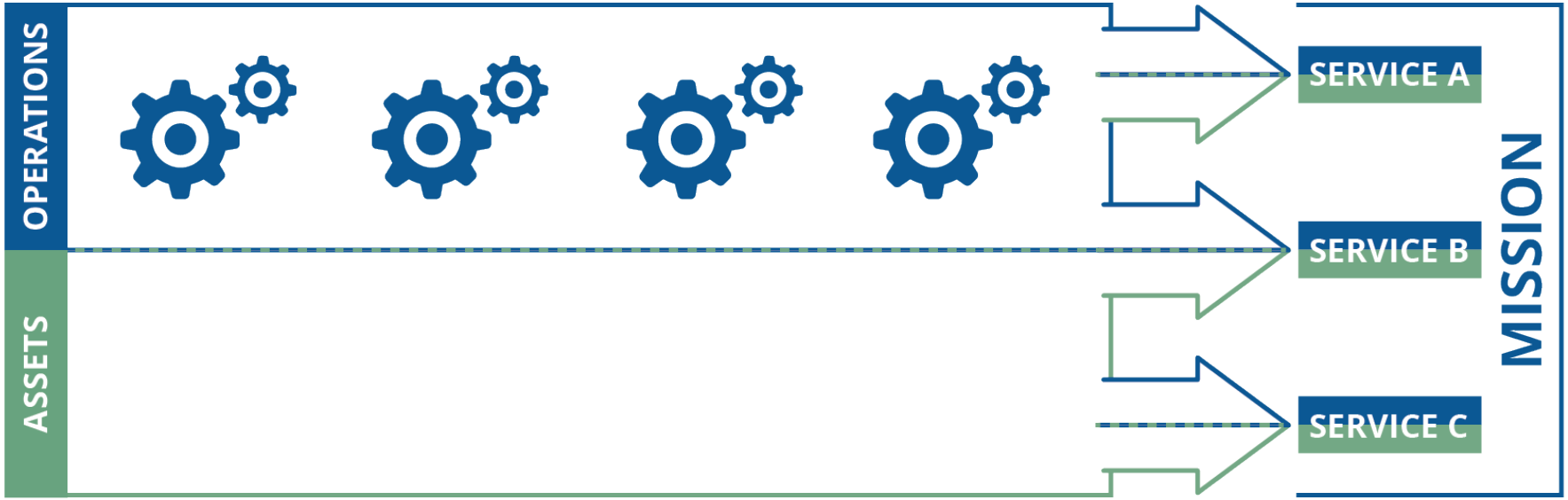
Life-Cycle Coverage

Services and Products



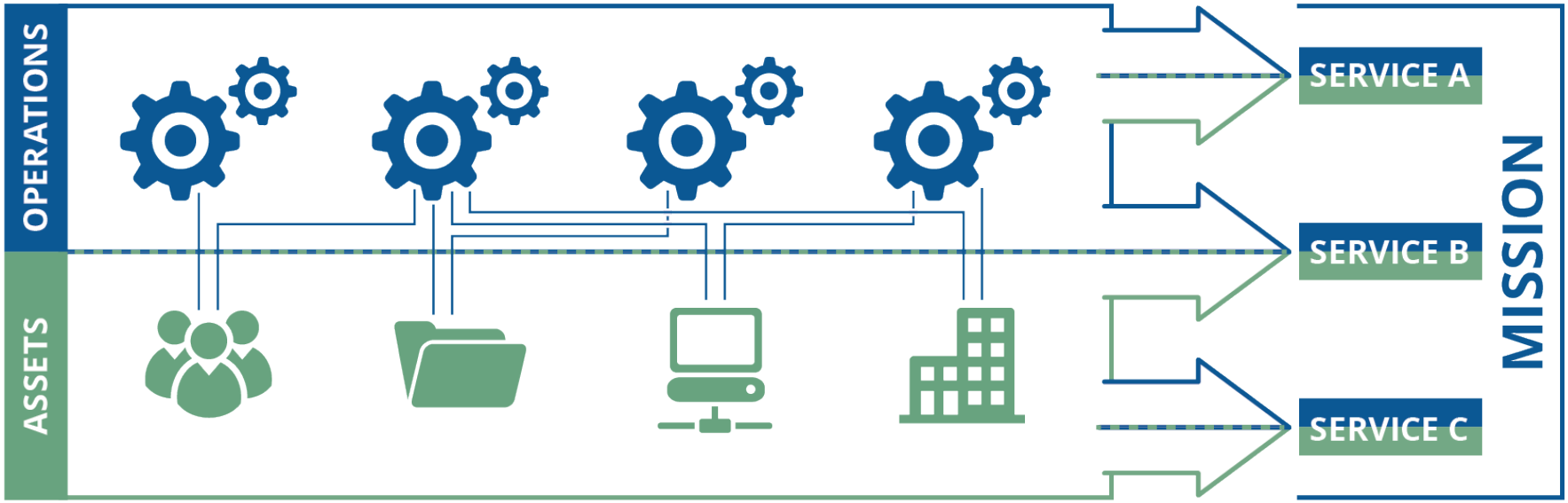
- Outputs of an organization
- Internally or externally focused
- Collectively enable an organization's mission

Productive Activities and Business Processes



- The organization performs these activities to ensure its services are generated.
- A service is made up of one or more productive activities.

Asset Support Services



People: those who operate and monitor the service

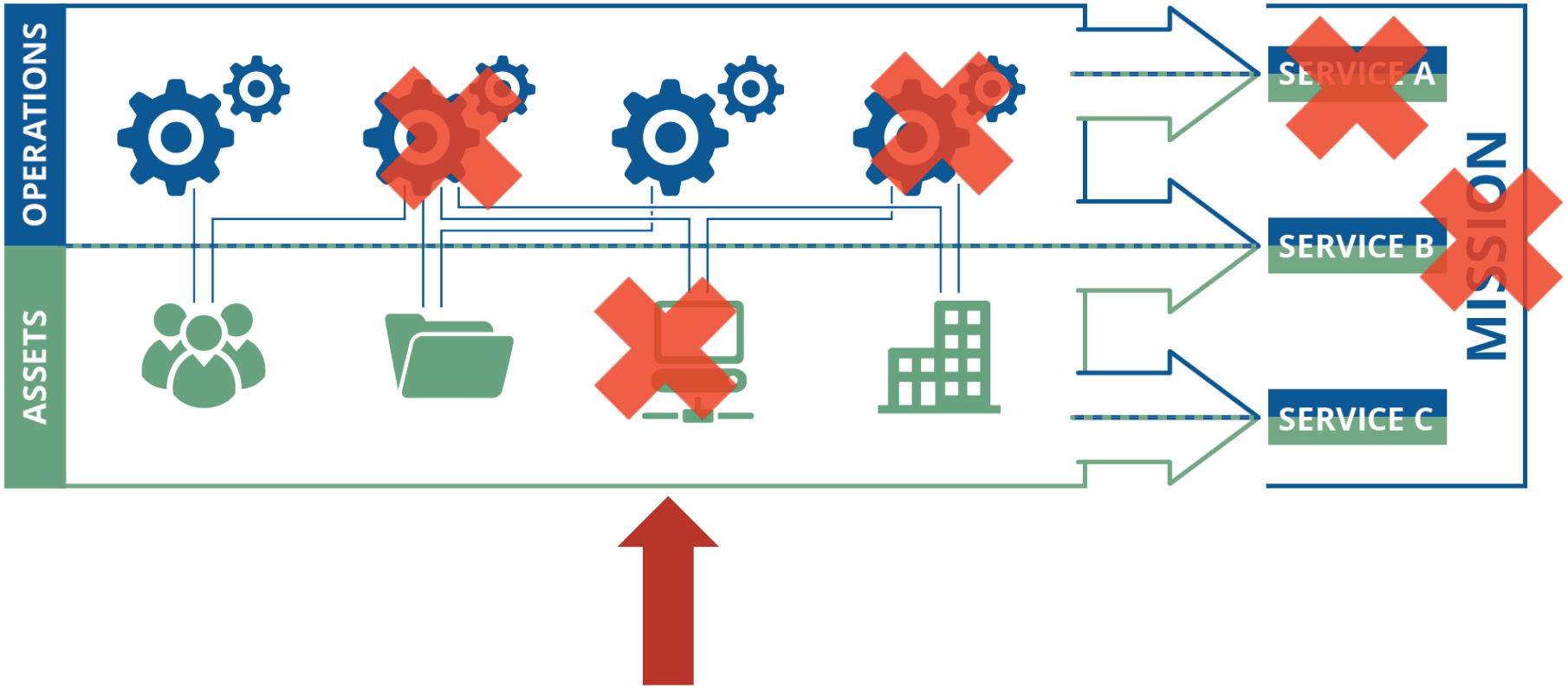
Information: data associated with the service

Technology: tools and equipment that automate and support the service

Facilities: where the service is performed

Assets derive their value from their importance in meeting the service mission.

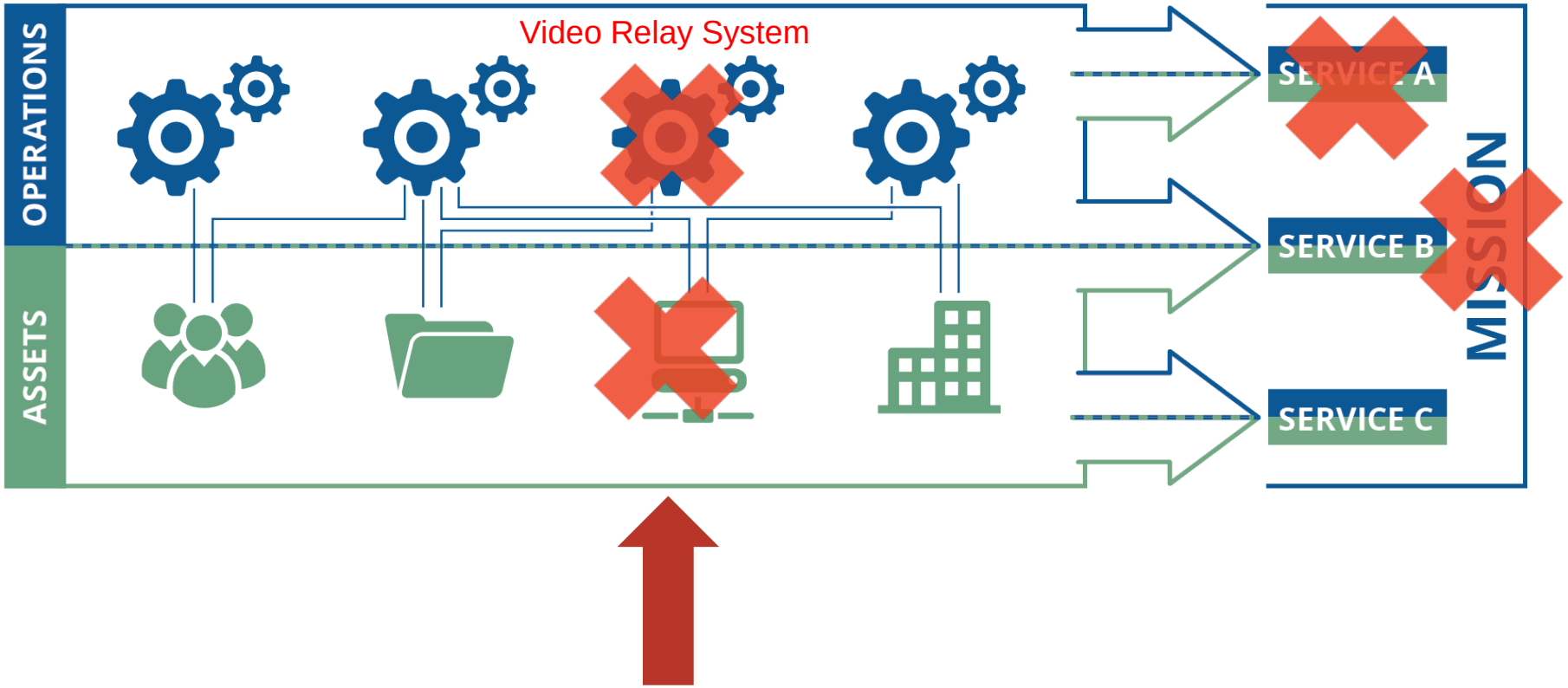
Disruption of Assets Can Lead to Mission Failure



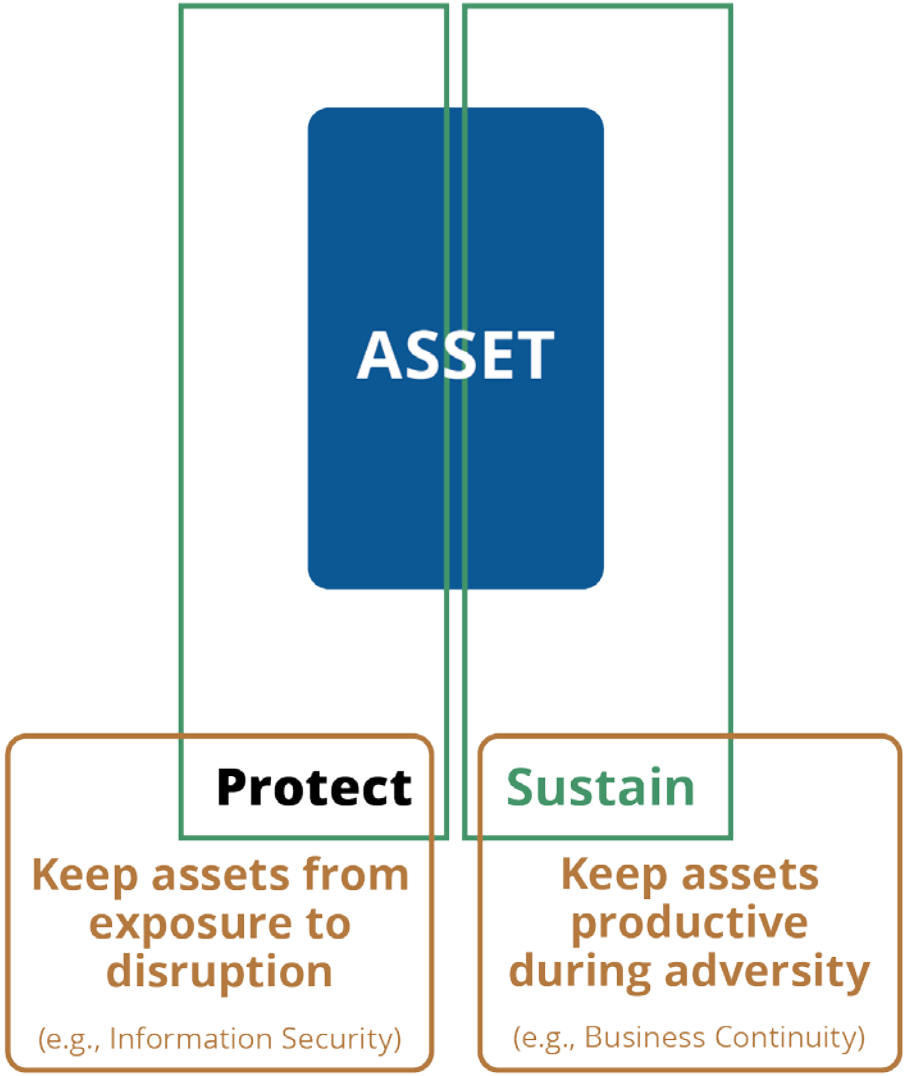
Realized operational risk resulting in asset disruption

Sorenson Communications

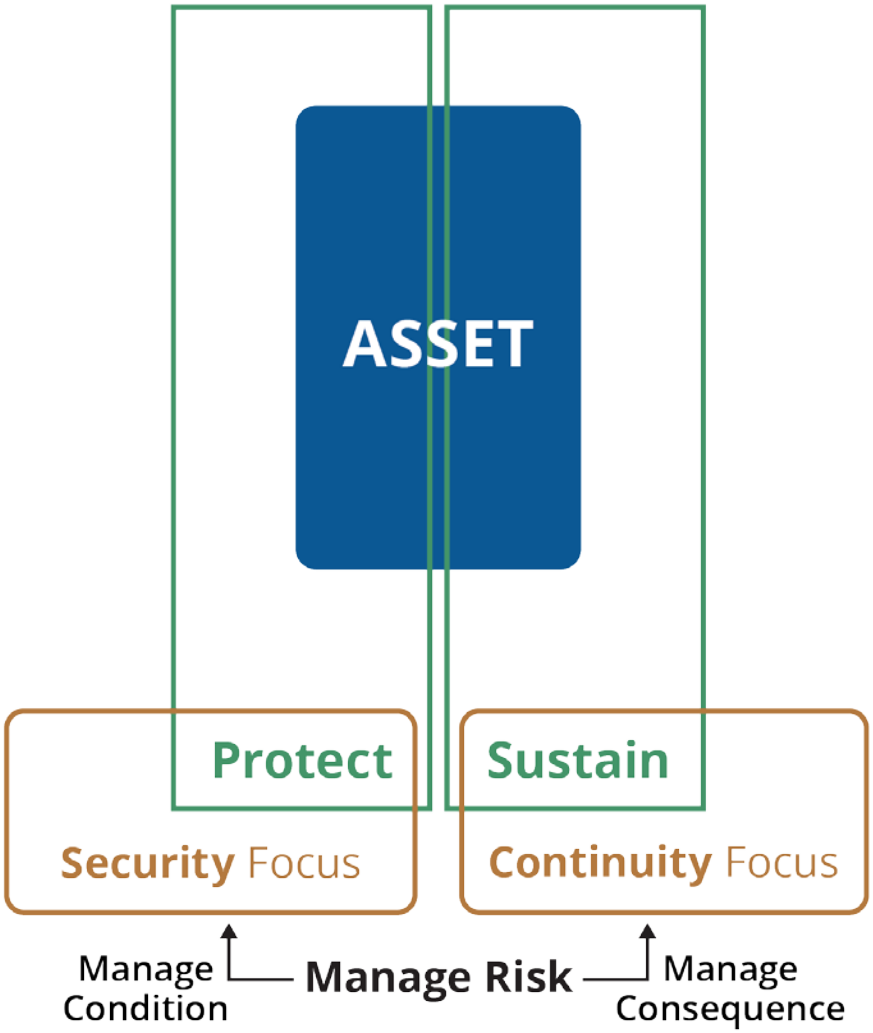
Provide 911 capability to deaf and those with vocal disabilities



Operational Resilience Starts at the Asset Level



Efficiency in Operational Resilience (or Operational Risk Management)



The optimal mix of protection and sustainment strategies

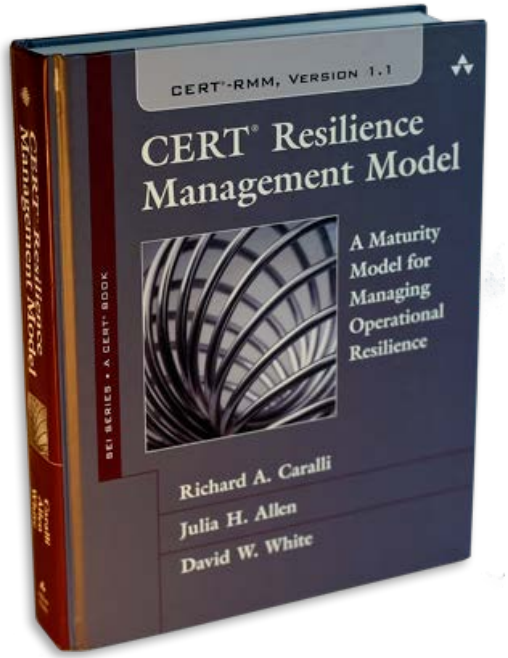
Depends on the **value** of the asset to the service and the **cost** of deploying and maintaining the strategy

The management challenge of operational resilience

CERT-RMM
The 10,000ft View

What Is CERT-RMM?

The CERT Resilience Management Model (CERT-RMM) is a **process improvement model** for **managing operational resilience**.



Free for download:
www.cert.org/resilience

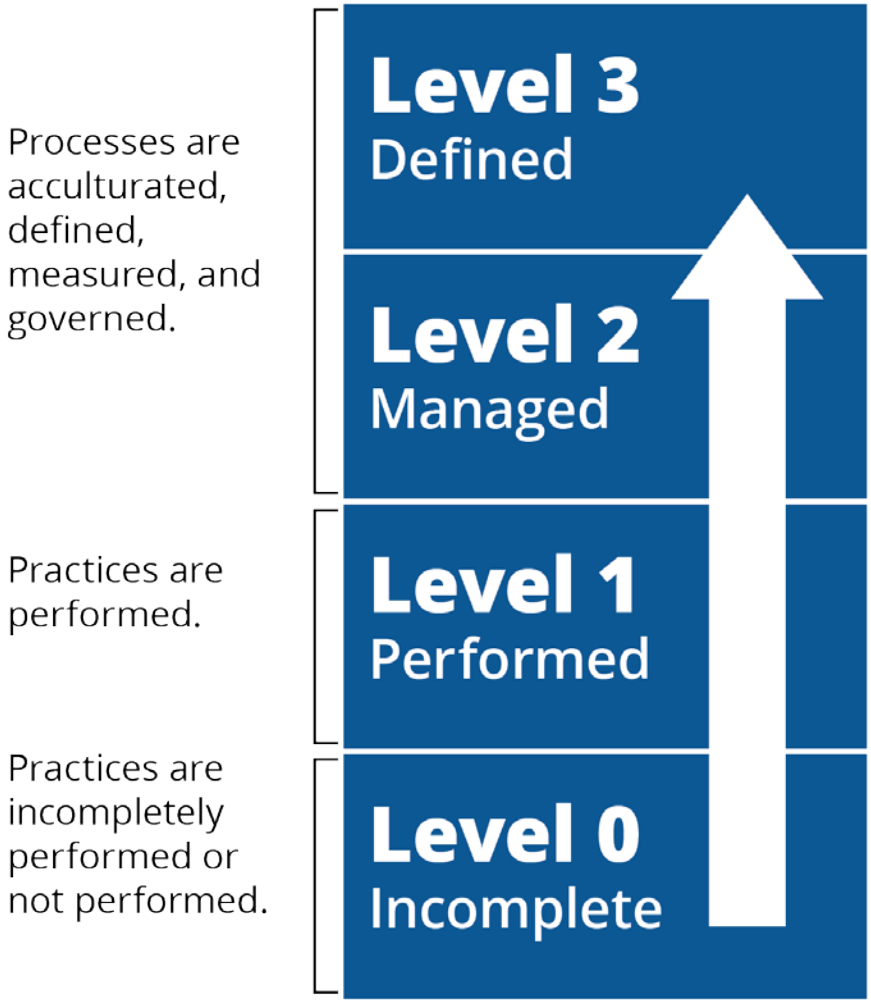
It provides guidelines and practices for

- Converging security, business continuity, disaster recovery, and IT ops
- Implementing, managing, and sustaining operational resilience activities
- Managing operational risk through process
- Measuring and institutionalizing the resilience process

It is a common vernacular and basis for planning, communicating, and evaluating improvements.

It is organized into 26 process areas.

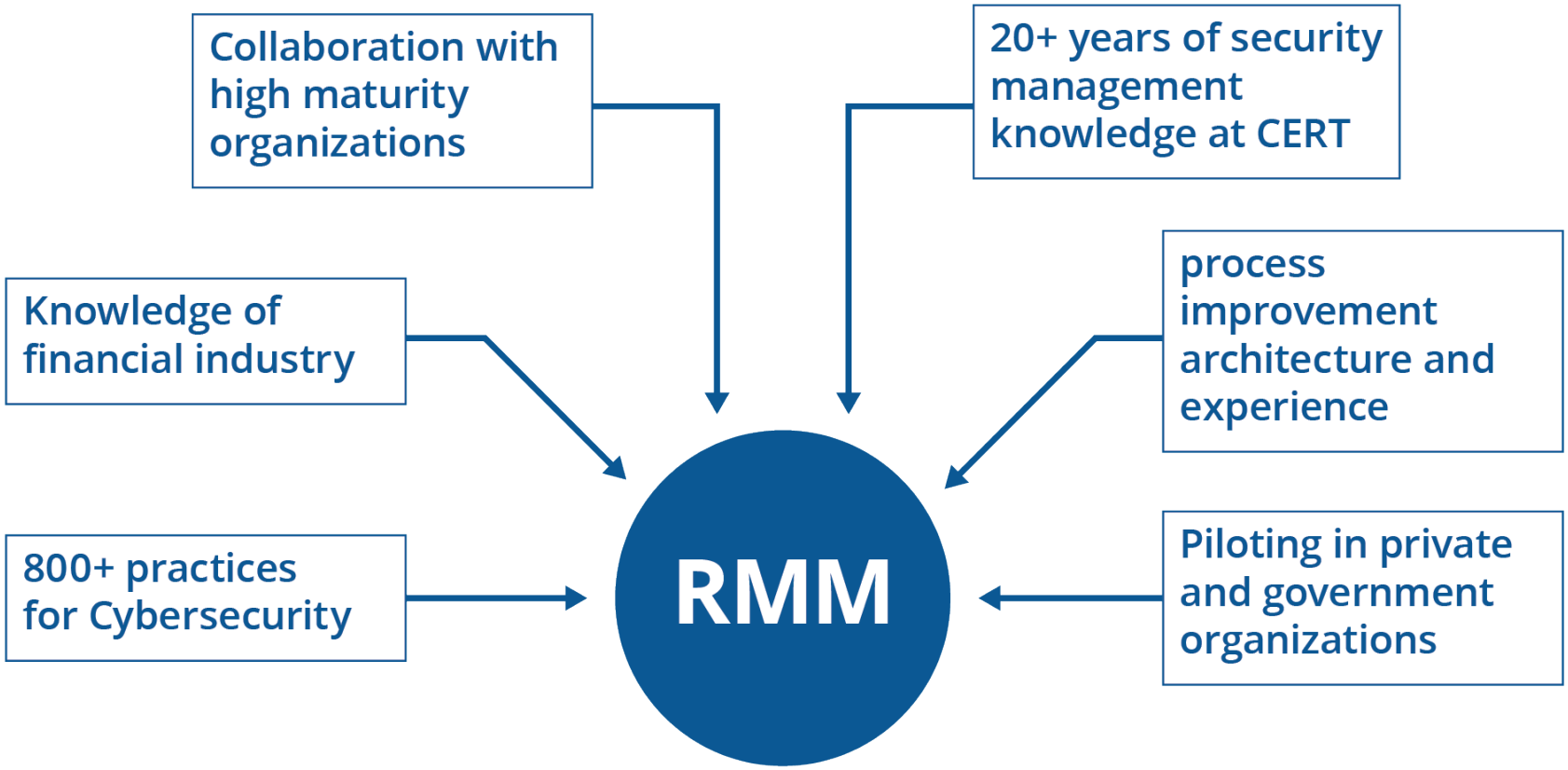
Institutionalizing Resilience Management



Benefits of a process approach

- Work is accomplished in a consistent manner, and outcomes are predictable.
- People develop their potential more fully and are more effective within the organization.
- By defining, measuring, and controlling the process, improvements are more successful and sustained.

How Was CERT-RMM Developed?



CERT-RMM combines best practices for cybersecurity from leading organizations and numerous standards and codes of practice.

26 Process Areas in 4 Categories

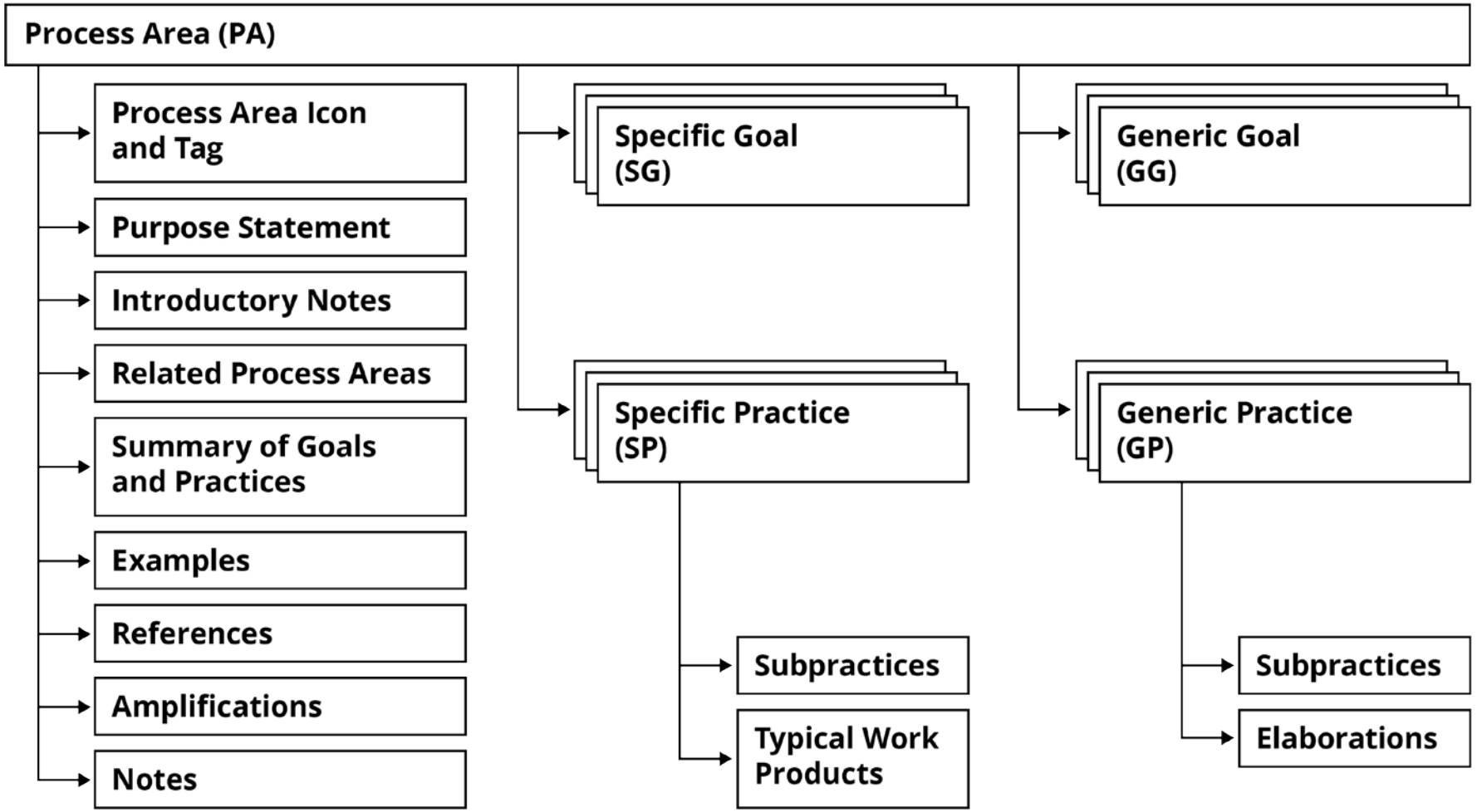
Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

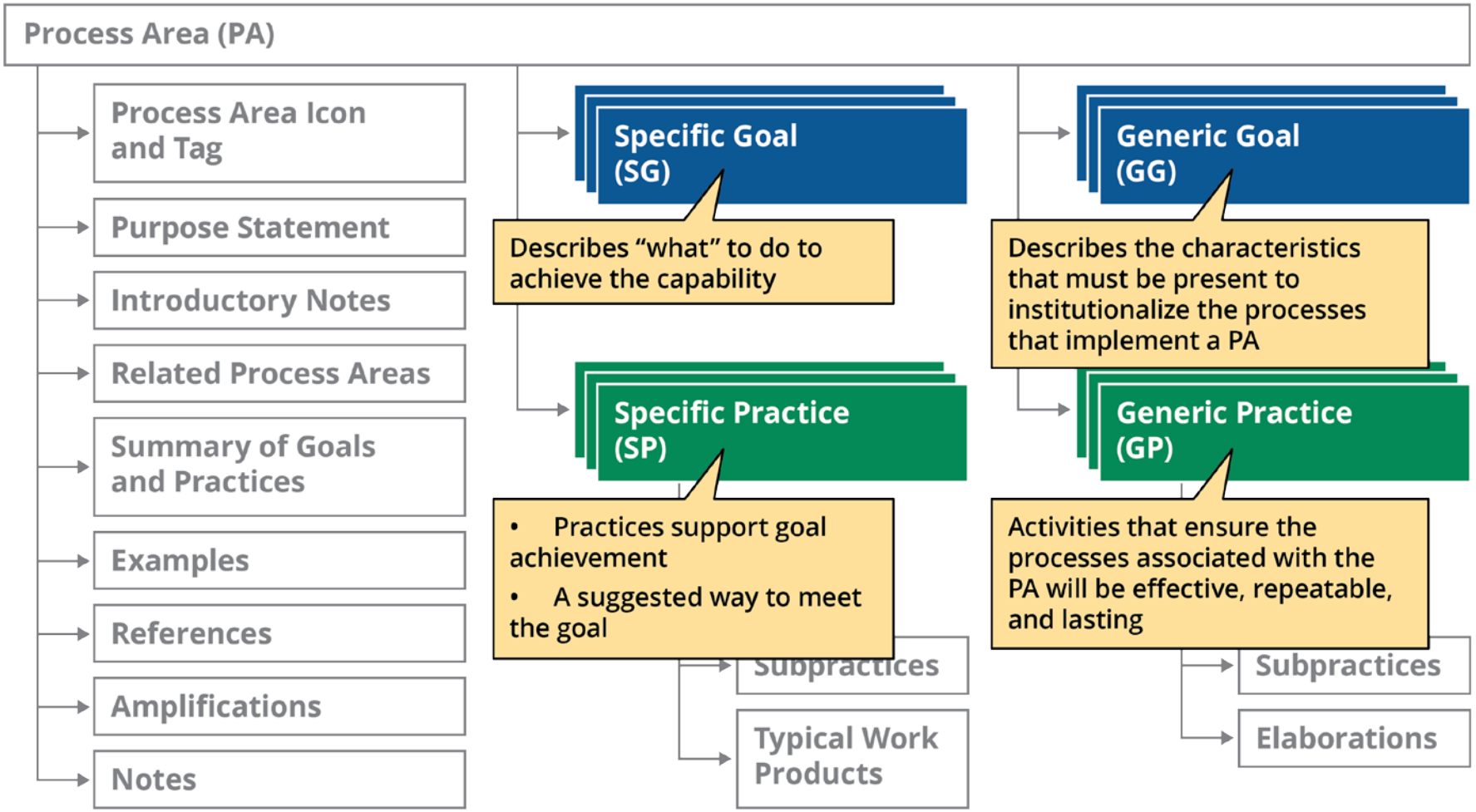
Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

Process Area Structure and Components



Process Area Structure & Components



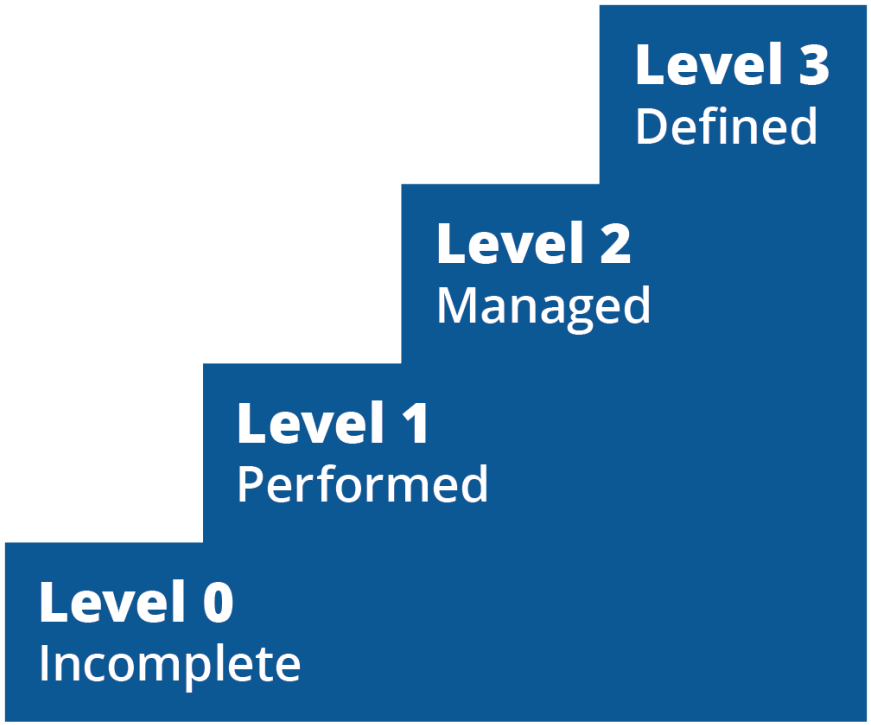
Process Maturity for Cyber Resilience

Process maturity can help answer some important questions when managing cyber resilience:

- How well are we performing today?
- Can we repeat our successes?
- Do we consistently produce expected results?
- Can we adapt seamlessly to changing risk environments?
- Are our processes stable enough to support us during times of stress?
- Can we predict how we will perform during times of stress?

Process maturity is about “making it stick.”

What Is a Maturity Model?



Maturity models have levels arranged in a scale that defines transitions from one level to another.

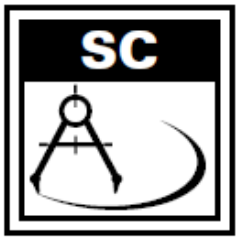
Attributes define each level; if an organization demonstrates these attributes, it has achieved that level.

Having measurable transitions between the levels enables an organization to use the scaling to

- Define its current state
- Define its future, more “mature” state
- Identify the attributes it must attain to reach that future state

Example: Service Continuity Process Area

SERVICE CONTINUITY



Purpose

The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Introductory Notes

The continuity of an organization's service delivery is a paramount concern in the organization's operational resilience activities. The organization can invest considerable time and resources in attempting to prevent a range of potential disruptive events, but no organization can mitigate all risk. As a result, the organization must be prepared to deal with the consequences of a disruption to its operations at any time. Significant disruption can result in dire circumstances for the organization, even bankruptcy or termination.

Example: Service Continuity Process Area

Summary of Specific Goals and Practices

SC:SG1 Prepare for Service Continuity
- SC:SG1.SP1 Plan for Service Continuity
- SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity

SC:SG2 Identify and Prioritize High-Value Services
- SC:SG2.SP1 Identify the Organization's High-Value Services
- SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies
- SC:SG2.SP3 Identify Vital Organizational Records and Databases

SC:SG3 Develop Service Continuity Plans
- SC:SG3.SP1 Identify Plans to Be Developed
- SC:SG3.SP2 Develop and Document Service Continuity Plans
- SC:SG3.SP3 Assign Staff to Service Continuity Plans
- SC:SG3.SP4 Store and Secure Service Continuity Plans
- SC:SG3.SP5 Develop Service Continuity Plan Training

SC:SG4 Validate Service Continuity Plans
- SC:SG4.SP1 Validate Plans to Requirements and Standards
- SC:SG4.SP2 Identify and Resolve Plan Conflicts

Example: Service Continuity Process Area

SC:SG2.SP1 *IDENTIFY THE ORGANIZATION'S HIGH-VALUE SERVICES*

The high-value services of the organization and their associated assets are identified.

The identification and prioritization of the organization's high-value services as strategic planning activities are addressed in the Enterprise Focus process area. This practice is included here to emphasize the importance of prioritizing high-value services as a foundational activity in the identification and development of service continuity plans.

Typical work products

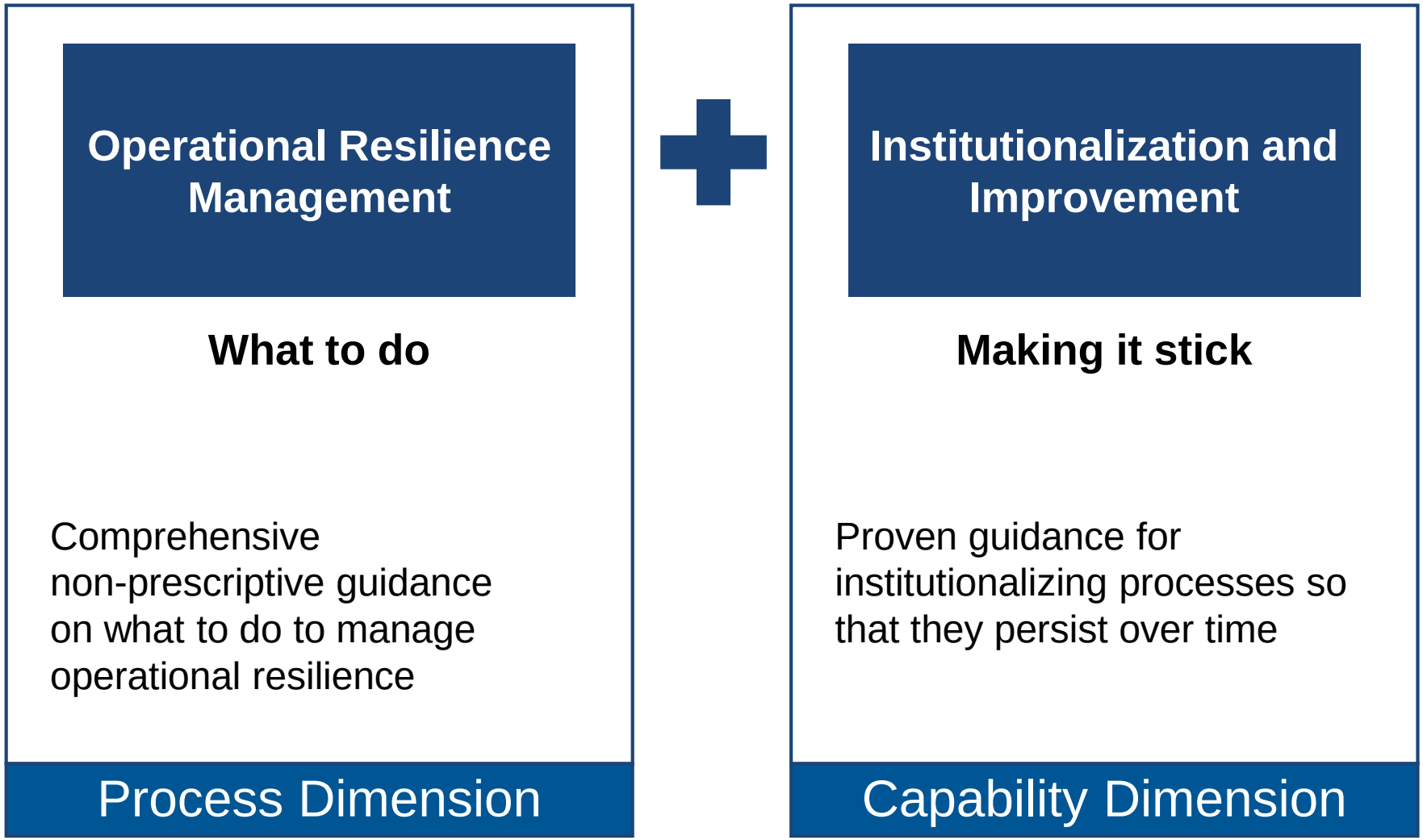
1. Prioritized list of high-value organizational services, activities, and associated assets
2. Results of security risk assessment and business impact analyses

Subpractices

1. Identify the organization's high-value services, associated assets, and activities.
2. Analyze and document the relative value of providing these services and the resulting impact on the organization if these services are interrupted.

   Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the consequences of risks to high-value services are identified and analyzed in risk assess-

CERT-RMM Approach



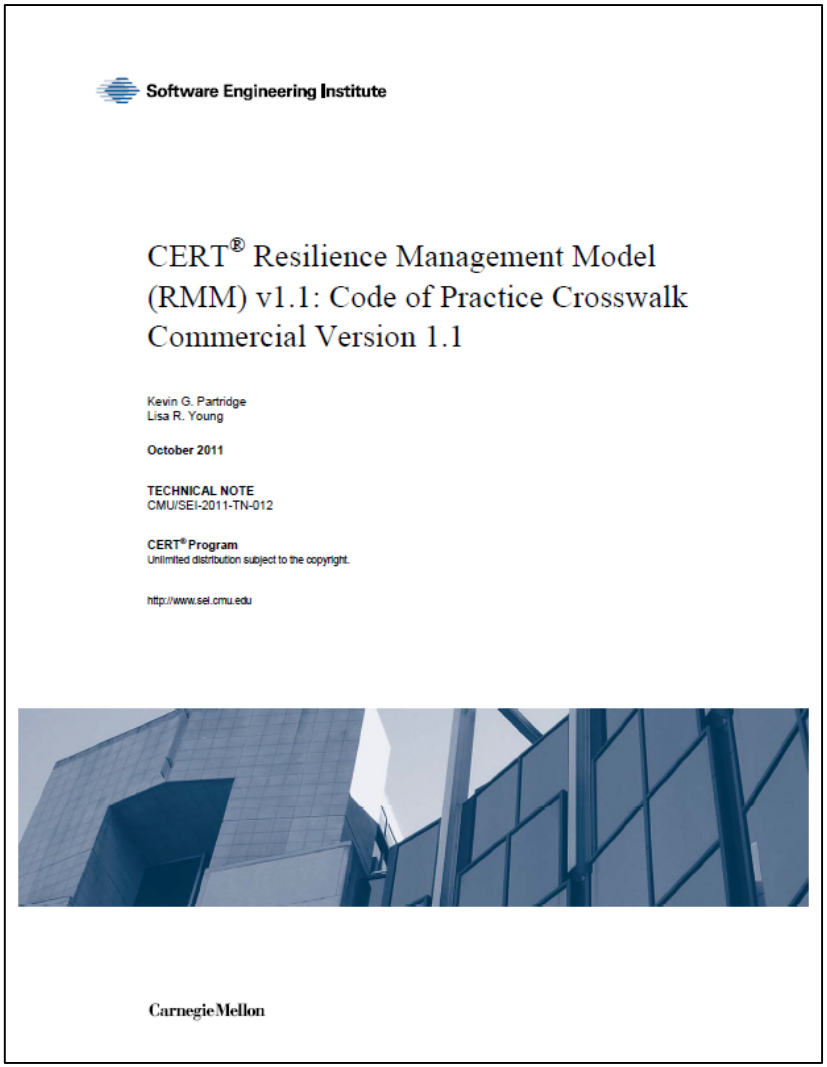
Want to know more? www.cert.org

Research Areas Include:

- Cyber Intelligence
- Digital Forensics
- Enterprise Risk Management
- Insider Threat
- Measurement and Analysis
- Network Situational Awareness
- Secure Development
- System and Platform Evaluation

Questions?

Code of Practice Crosswalk

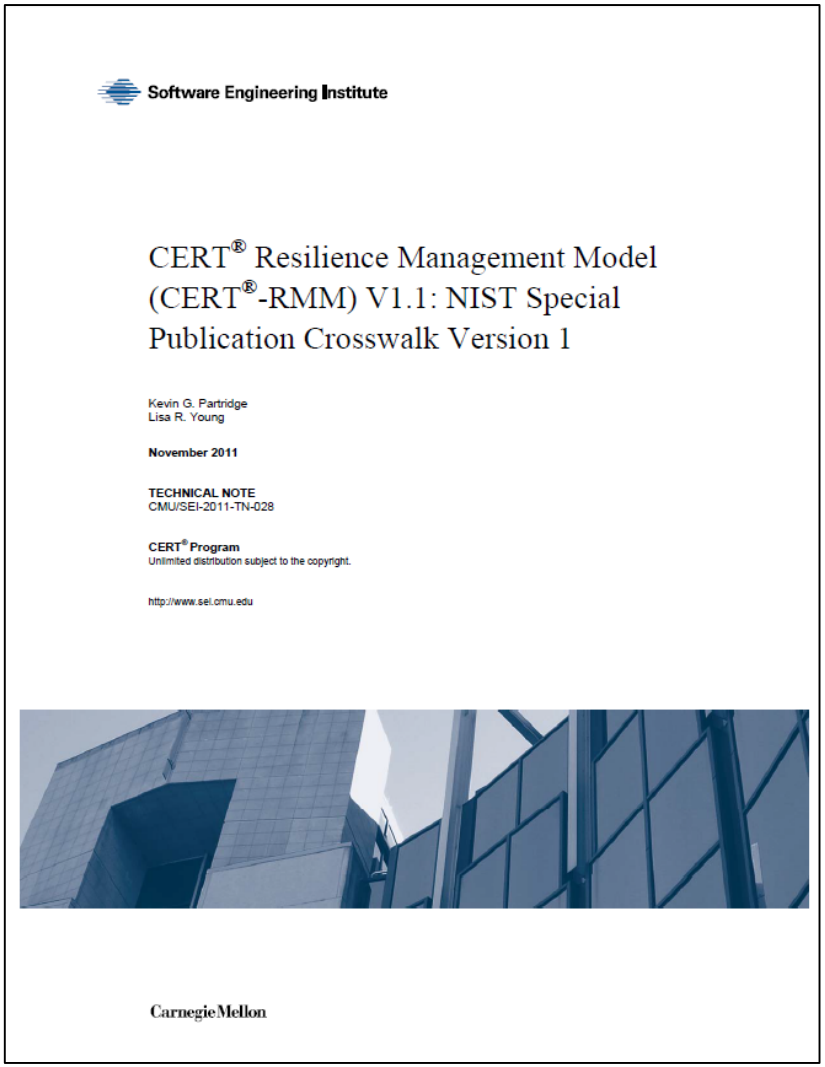


A supplementary document that links CERT-RMM subpractices to commonly used codes of practice

Currently includes references to

- ISO 31000: 2009
- BS25999-1:2006
- CobiT 4.1
- CMMI –DEV v1.2
- CMMI –SVC v1.2
- FFIEC BCP Handbook
- ISO 20000-2:2005(E)
- ISO 24762:2008(E)
- ISO 27002:2005
- ISO 27005:2008
- PCI DSS v1.2.1: 2009
- NFPA 1600:2007
- ANSI/ASIS SPC.1-2009

NIST SP 800 Series Crosswalk


Software Engineering Institute

CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1

Kevin G. Partridge
Lisa R. Young

November 2011

TECHNICAL NOTE
CMU/SEI-2011-TN-028

CERT® Program
Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

Carnegie Mellon

A supplementary document that links CERT-RMM subpractices to NIST special publications in the 800 series

Currently includes references to

- NIST SP 800-18
- NIST SP 800-30
- NIST SP 800-34
- NIST SP 800-37
- NIST SP 800-39
- NIST SP 800-53
- NIST SP 800-53A
- NIST SP 800-55
- NIST SP 800-60
- NIST SP 800-61
- NIST SP 800-70
- NIST SP 800-137