Киберсигурност и устойчив бизнес

Упражнение 04

Съдържание

01 **Създаване на Policy файлове**

работа в екипи

02 **CERT-RMM накратко**

видове практики

Създаване на Policy файлове

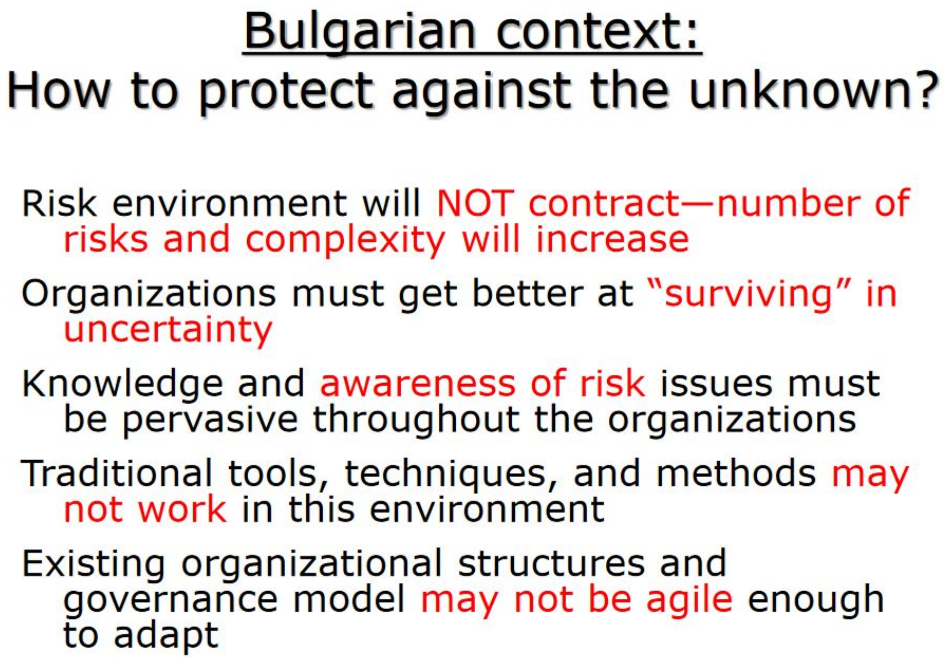
Създаване на Policy файлове

Примери

(*погледнете read-me.txt в папка “templates-policies”*)

CERT-RMM накратко

CERT-RMM накратко



Bulgarian context:

How to protect against the unknown?

Risk environment will NOT contract—number of risks and complexity will increase

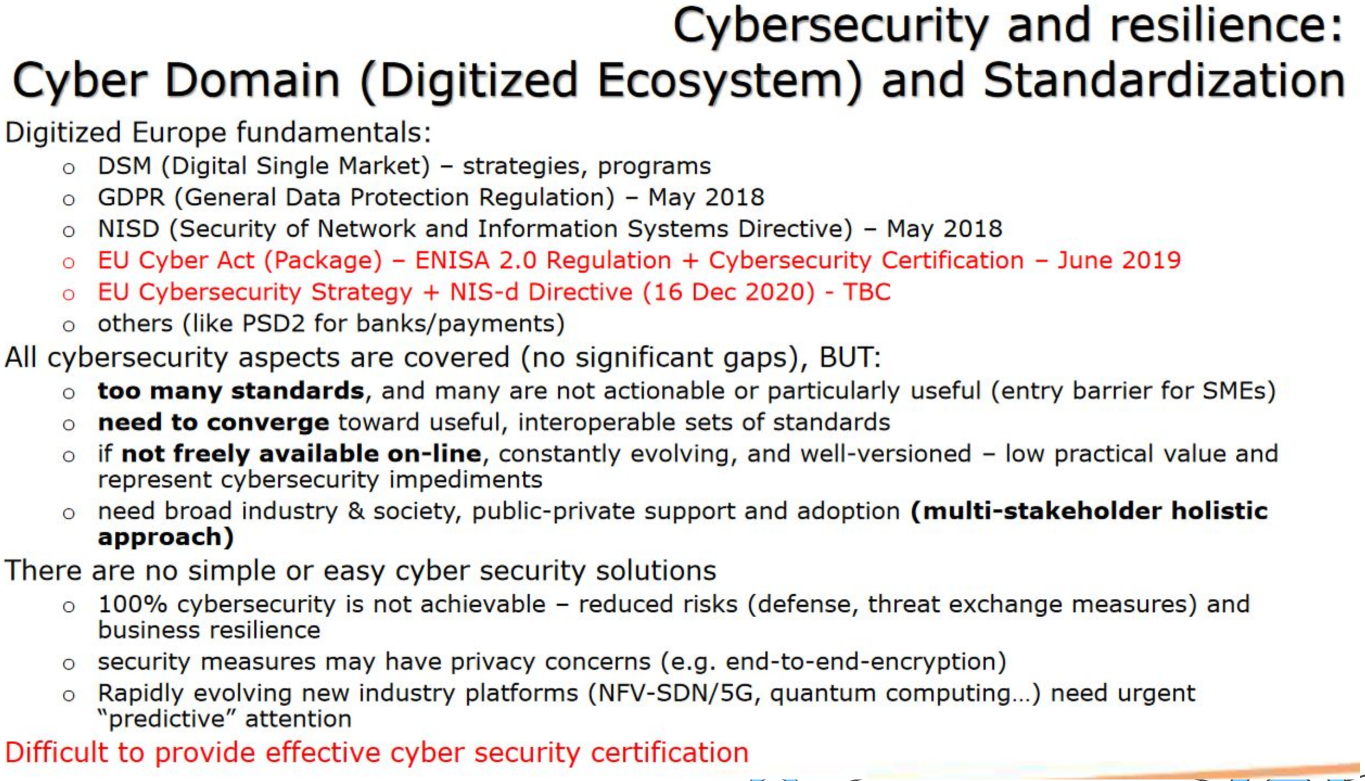
Organizations must get better at “surviving” in uncertainty

Knowledge and awareness of risk issues must be pervasive throughout the organizations

Traditional tools, techniques, and methods may not work in this environment

Existing organizational structures and governance model may not be agile enough to adapt

CERT-RMM накратко



Cybersecurity and resilience: Cyber Domain (Digitized Ecosystem) and Standardization

Digitized Europe fundamentals:

- DSM (Digital Single Market) – strategies, programs
- GDPR (General Data Protection Regulation) – May 2018
- NISD (Security of Network and Information Systems Directive) – May 2018
- EU Cyber Act (Package) – ENISA 2.0 Regulation + Cybersecurity Certification – June 2019
- EU Cybersecurity Strategy + NIS-d Directive (16 Dec 2020) - TBC
- others (like PSD2 for banks/payments)

All cybersecurity aspects are covered (no significant gaps), BUT:

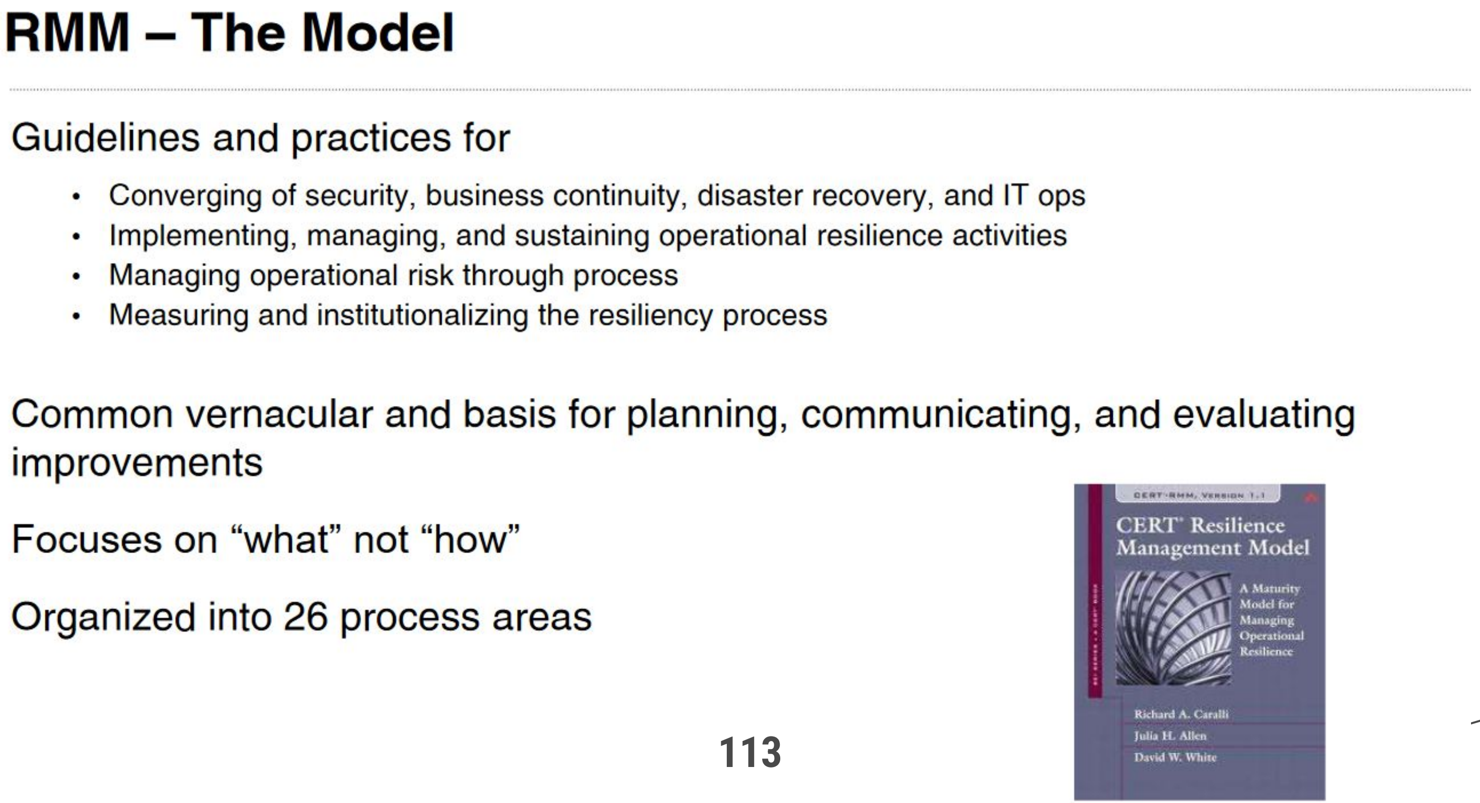
- **too many standards**, and many are not actionable or particularly useful (entry barrier for SMEs)
- **need to converge** toward useful, interoperable sets of standards
- if **not freely available on-line**, constantly evolving, and well-versioned – low practical value and represent cybersecurity impediments
- need broad industry & society, public-private support and adoption **(multi-stakeholder holistic approach)**

There are no simple or easy cyber security solutions

- 100% cybersecurity is not achievable – reduced risks (defense, threat exchange measures) and business resilience
- security measures may have privacy concerns (e.g. end-to-end-encryption)
- Rapidly evolving new industry platforms (NFV-SDN/5G, quantum computing…) need urgent "predictive" attention

Difficult to provide effective cyber security certification

CERT-RMM накратко



RMM – The Model

Guidelines and practices for

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

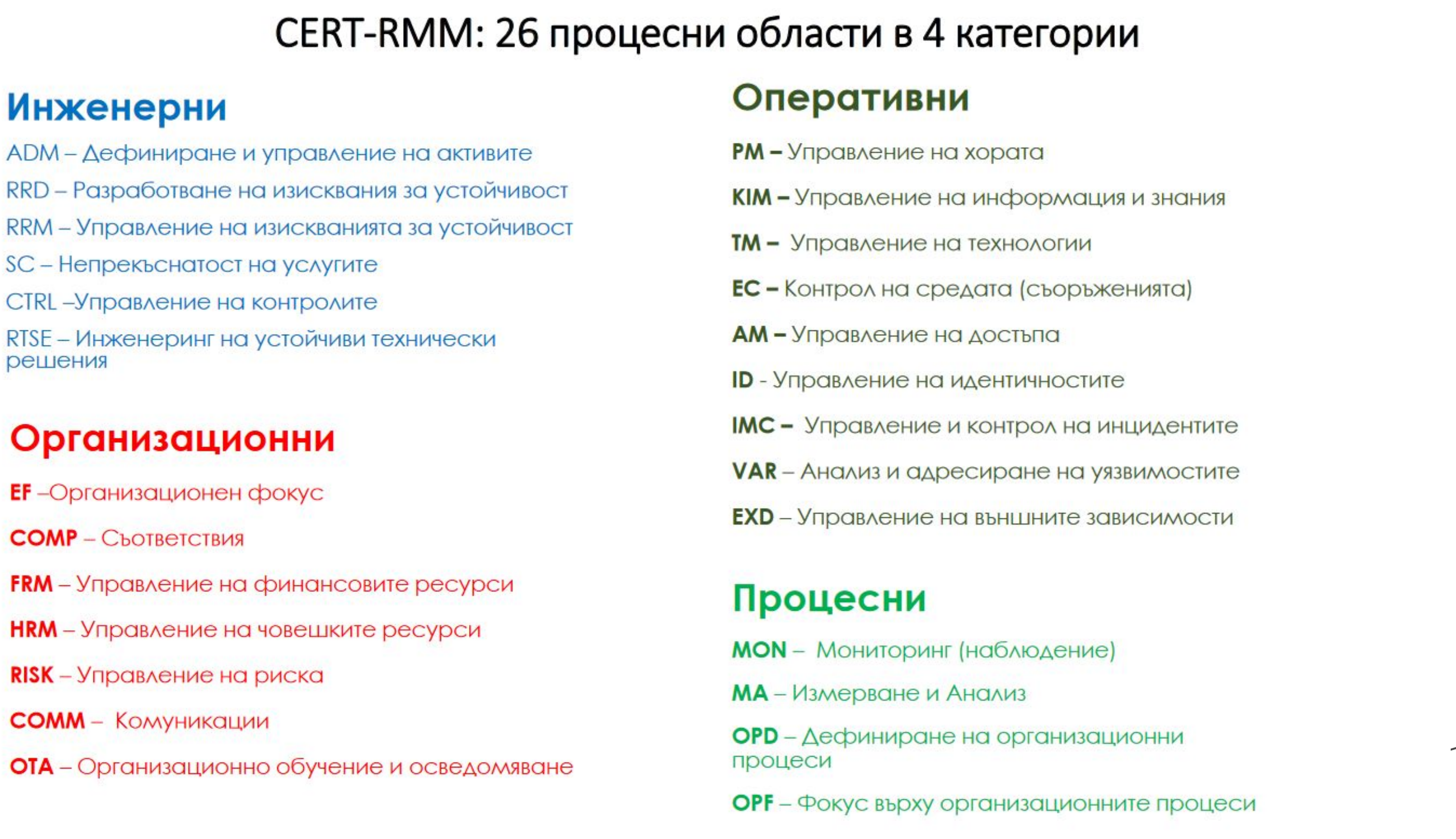
Common vernacular and basis for planning, communicating, and evaluating improvements

Focuses on “what” not “how”

Organized into 26 process areas

CERT-RMM, VERSION 1.1
CERT Resilience Management Model
A Maturity Model for Managing Operational Resilience
Richard A. Caralli
Julia H. Allen
David W. White

CERT-RMM накратко



CERT-RMM: 26 процесни области в 4 категории

Инженерни

ADM – Дефиниране и управление на активите
RRD – Разработване на изисквания за устойчивост
RRM – Управление на изискванията за устойчивост
SC – Непрекъснатост на услугите
CTRL –Управление на контролите
RTSE – Инженеринг на устойчиви технически решения

Организационни

EF –Организационен фокус
COMP – Съответствия
FRM – Управление на финансовите ресурси
HRM – Управление на човешките ресурси
RISK – Управление на риска
COMM – Комуникации
OTA – Организационно обучение и осведомяване

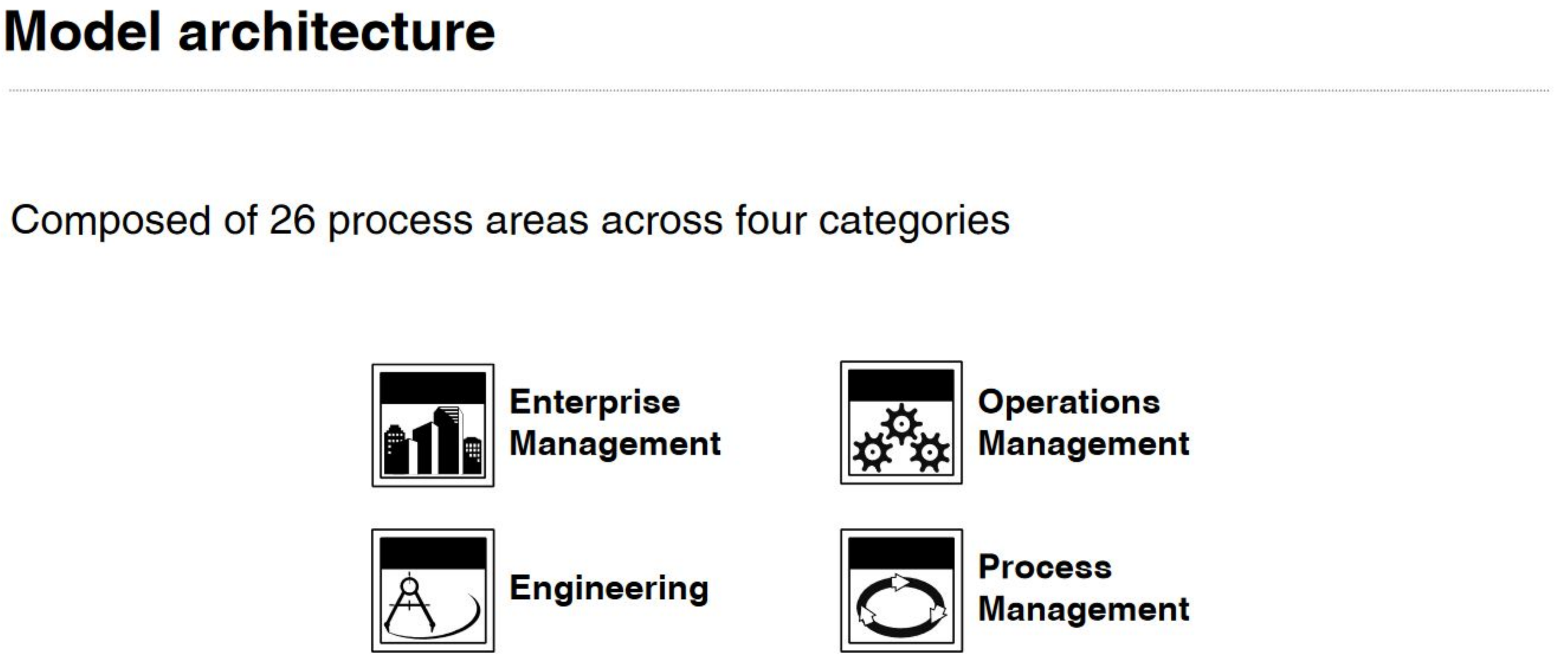
Оперативни

PM – Управление на хората
KIM – Управление на информация и знания
TM – Управление на технологии
EC – Контрол на средата (съоръженията)
AM – Управление на достъпа
ID - Управление на идентичностите
IMC – Управление и контрол на инцидентите
VAR – Анализ и адресиране на уязвимостите
EXD – Управление на външните зависимости

Процесни

MON – Мониторинг (наблюдение)
MA – Измерване и Анализ
OPD – Дефиниране на организационни процеси
OPF – Фокус върху организационните процеси

CERT-RMM накратко



Model architecture

Composed of 26 process areas across four categories

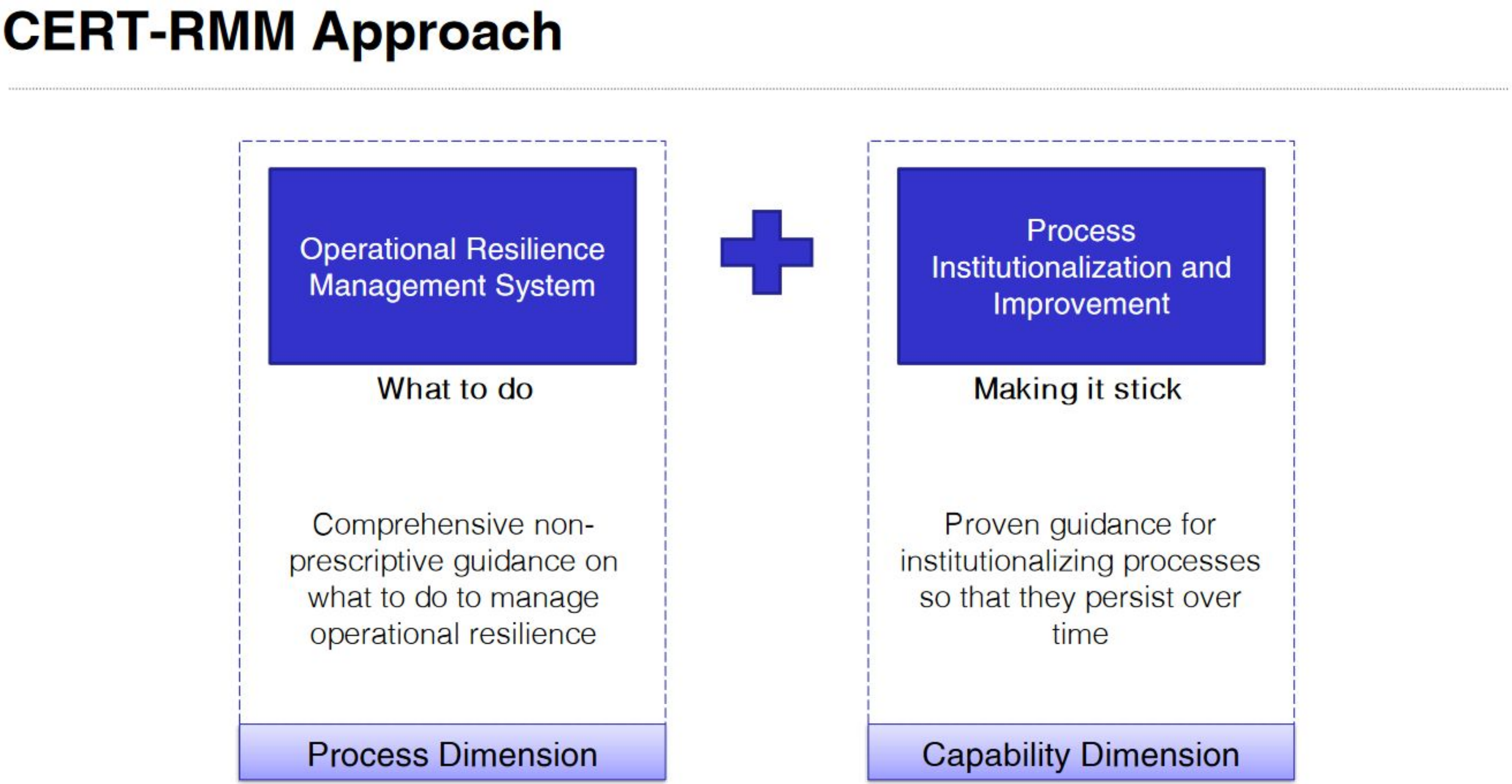
Enterprise Management

Operations Management

Engineering

Process Management

CERT-RMM накратко



CERT-RMM Approach

Operational Resilience Management System

What to do

Comprehensive non-prescriptive guidance on what to do to manage operational resilience

Process Dimension

+

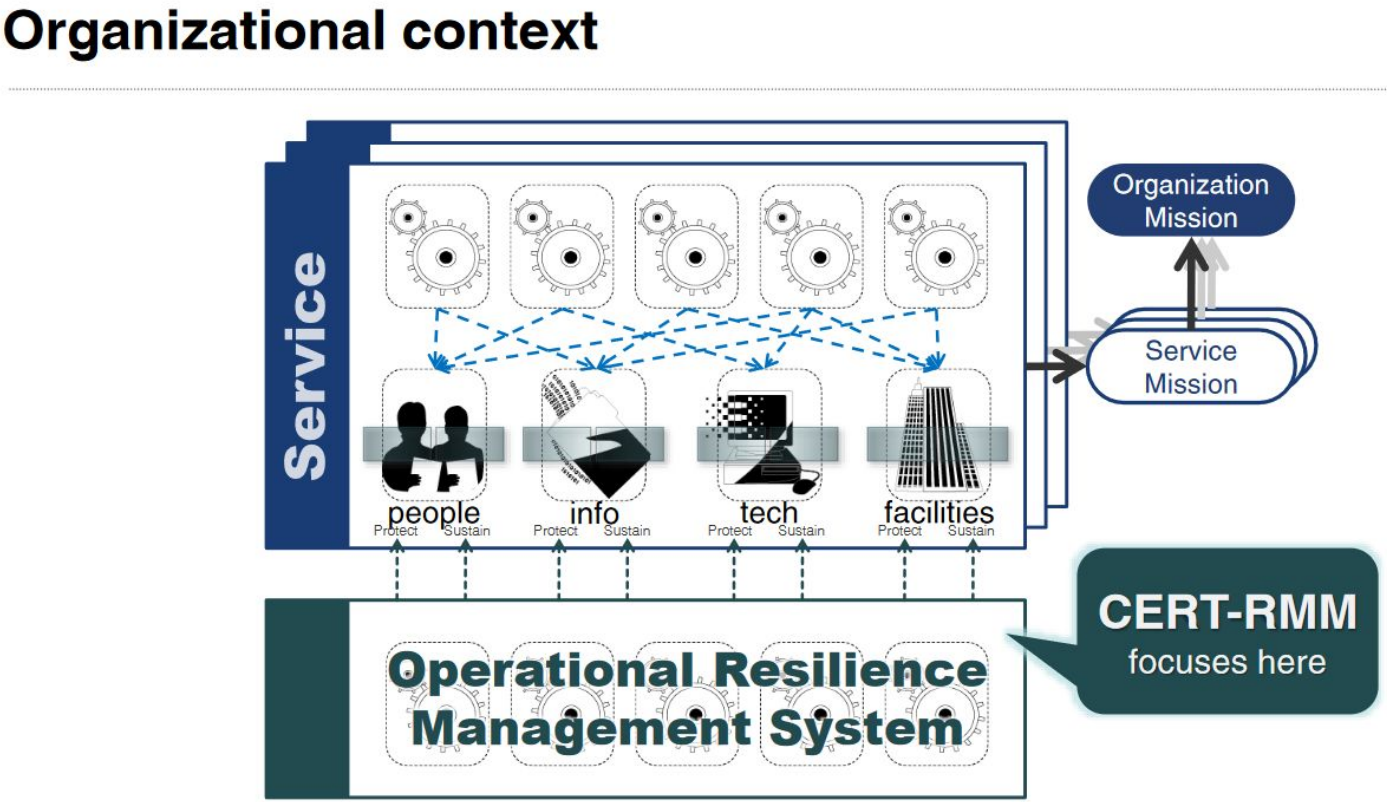
Process Institutionalization and Improvement

Making it stick

Proven guidance for institutionalizing processes so that they persist over time

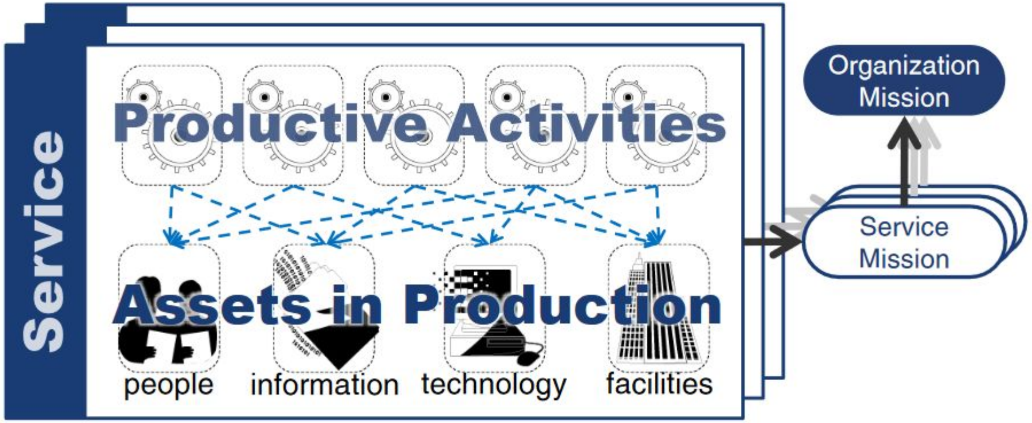
Capability Dimension

CERT-RMM накратко



CERT-RMM накратко

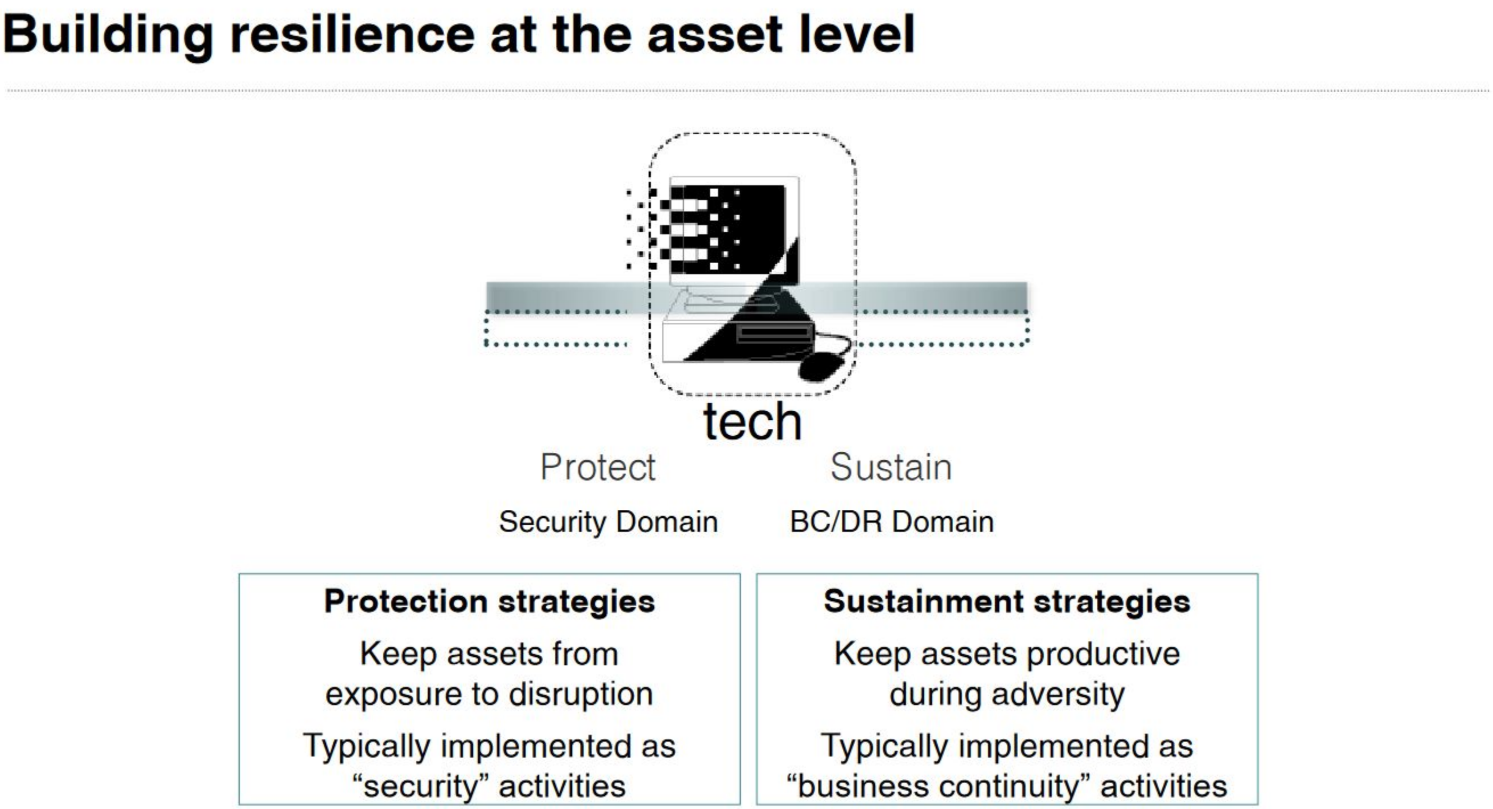
Organizational context



Four asset types:

- **People** – the human capital of the organization
- **Information** – data, records, knowledge in physical or digital form
- **Technology** – software, systems, hardware, network
- **Facilities** – offices, data centers, labs – the physical places

CERT-RMM накратко



Building resilience at the asset level

tech

Protect

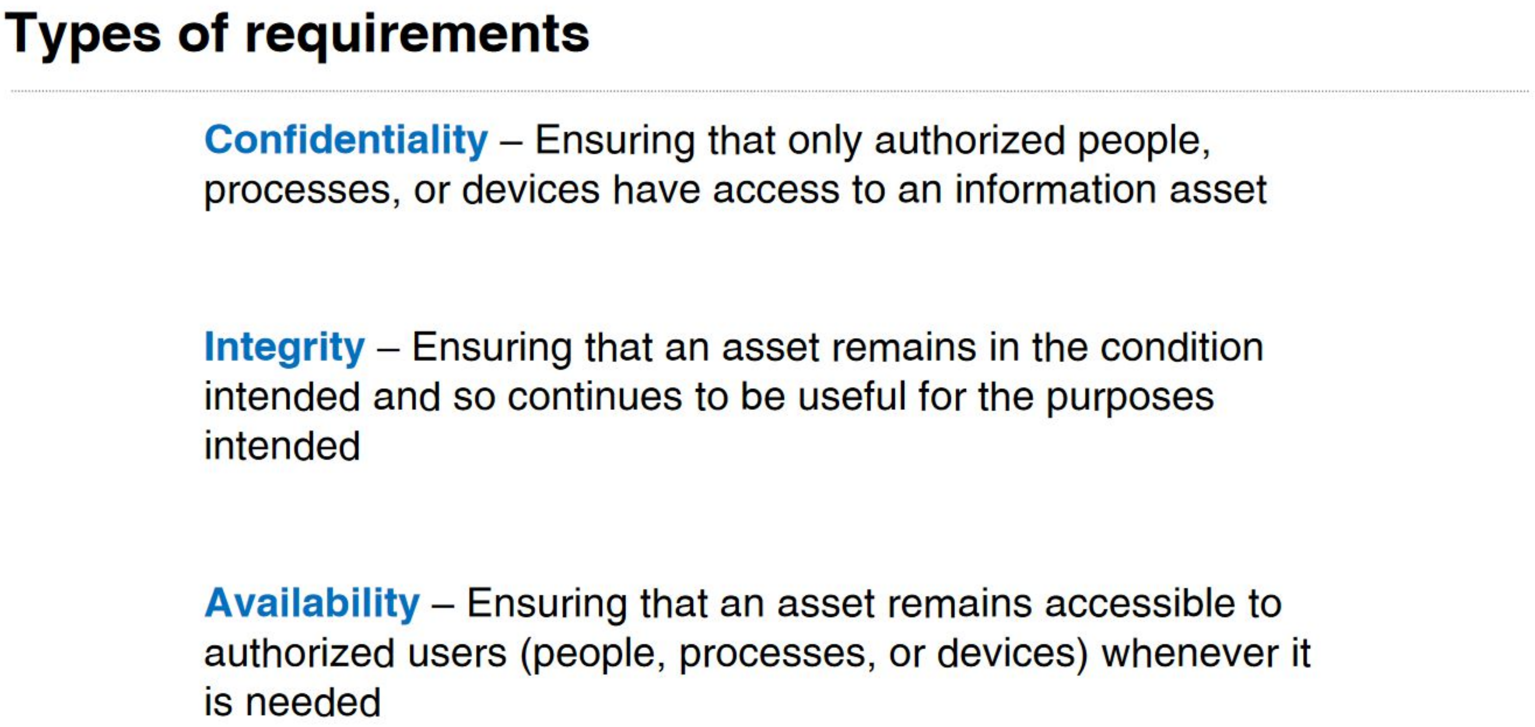
Sustain

Security Domain

BC/DR Domain

Protection strategies	**Sustainment strategies**
Keep assets from exposure to disruption	Keep assets productive during adversity
Typically implemented as “security” activities	Typically implemented as “business continuity” activities

CERT-RMM накратко

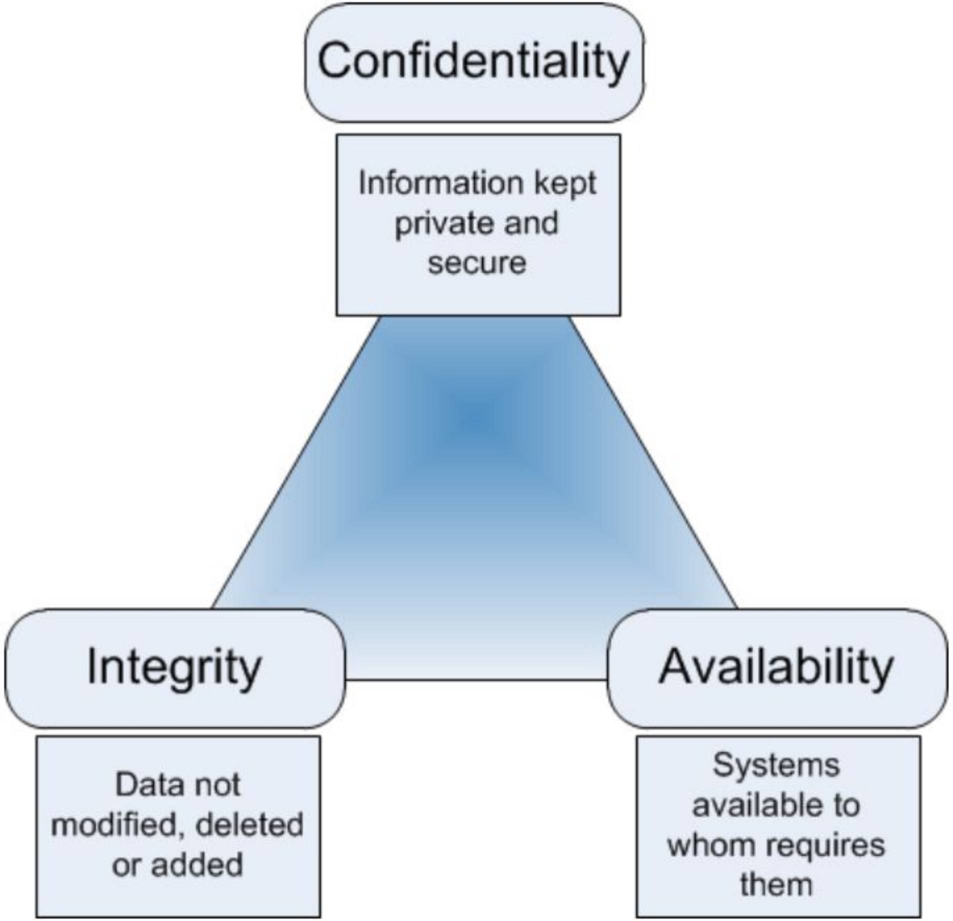


Types of requirements

Confidentiality – Ensuring that only authorized people, processes, or devices have access to an information asset

Integrity – Ensuring that an asset remains in the condition intended and so continues to be useful for the purposes intended

Availability – Ensuring that an asset remains accessible to authorized users (people, processes, or devices) whenever it is needed



Confidentiality

Information kept private and secure

Integrity

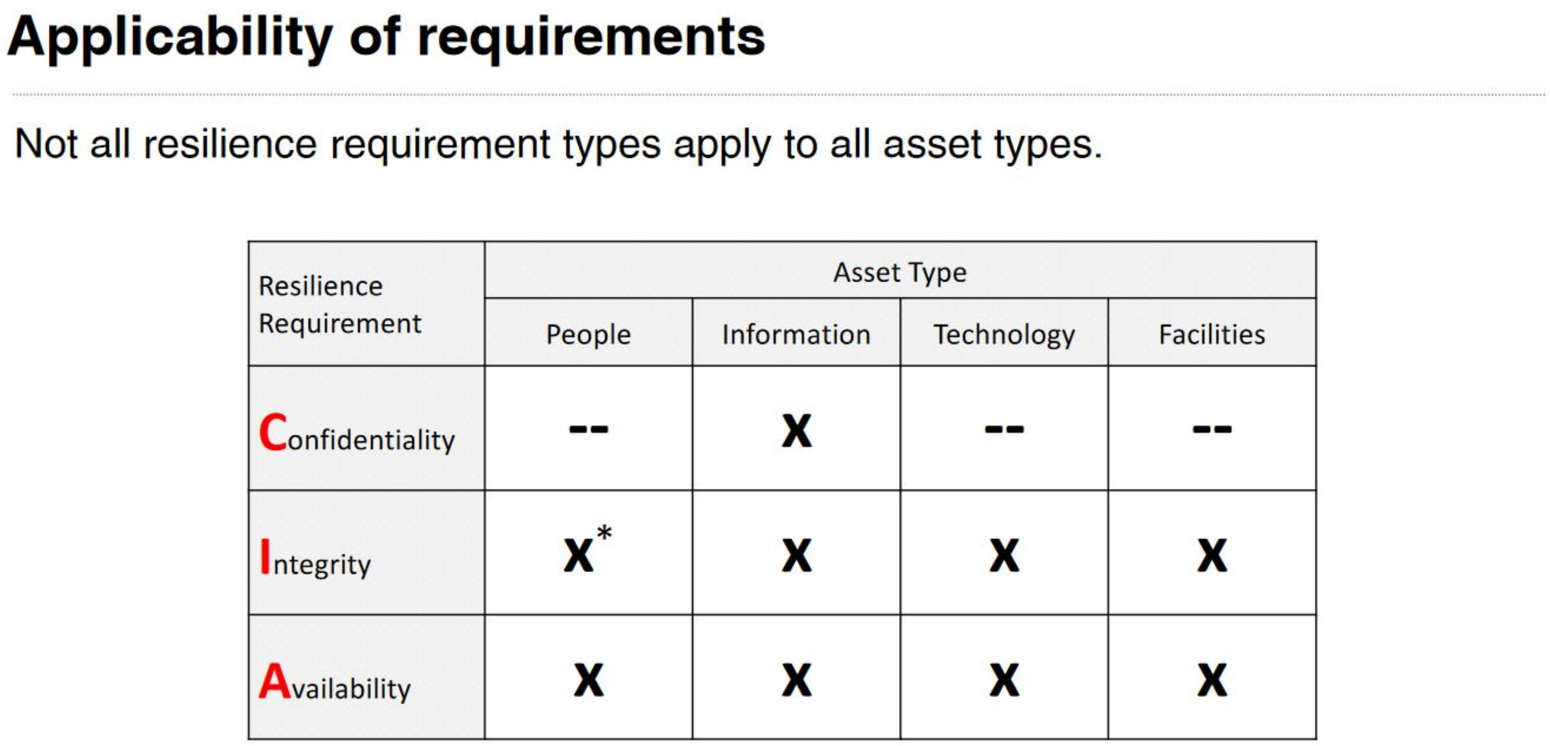
Data not modified, deleted or added

Availability

Systems available to whom requires them

Source: http://geraintw.blogspot.sg/2012/09/cia-infosec.html

CERT-RMM накратко



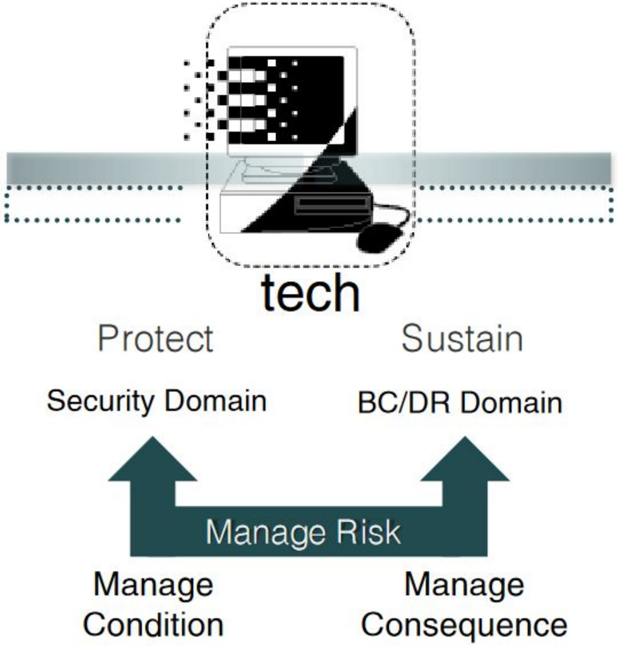
Applicability of requirements

Not all resilience requirement types apply to all asset types.

Resilience Requirement	Asset Type			
	People	Information	Technology	Facilities
Confidentiality	--	X	--	--
Integrity	X*	X	X	X
Availability	X	X	X	X

CERT-RMM накратко

Resilience strategy



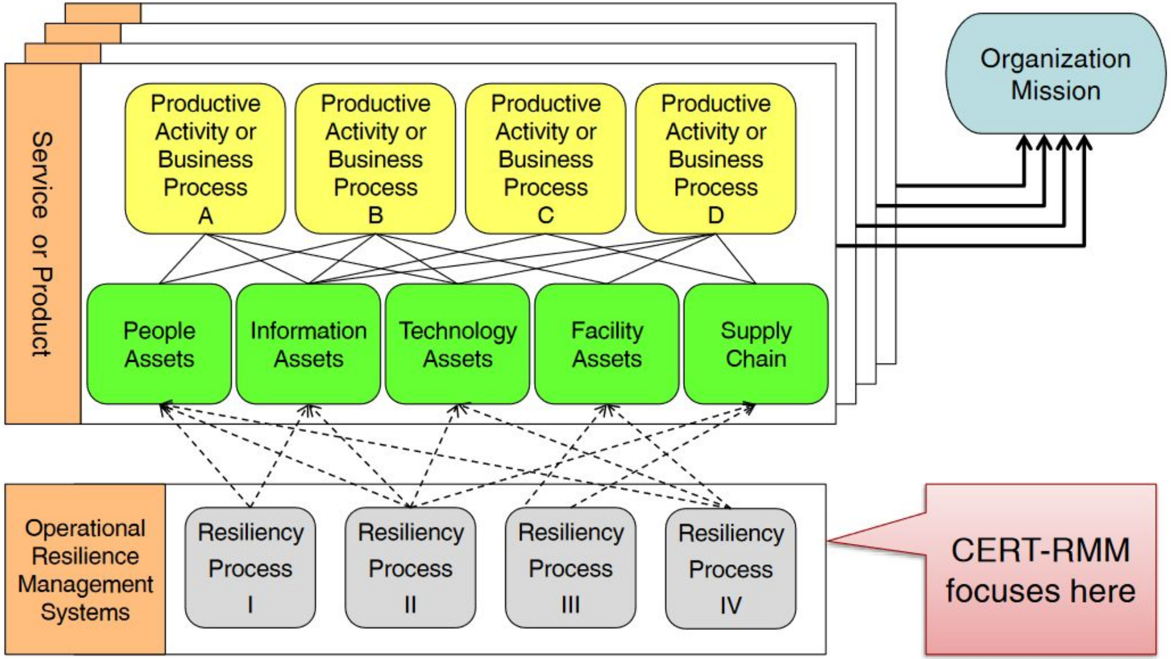
The optimal “mix” of protection and sustainment strategies

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

BC, security, & IT operations collaborating to manage risk

CERT-RMM накратко

Organizational Context for Resiliency Activities



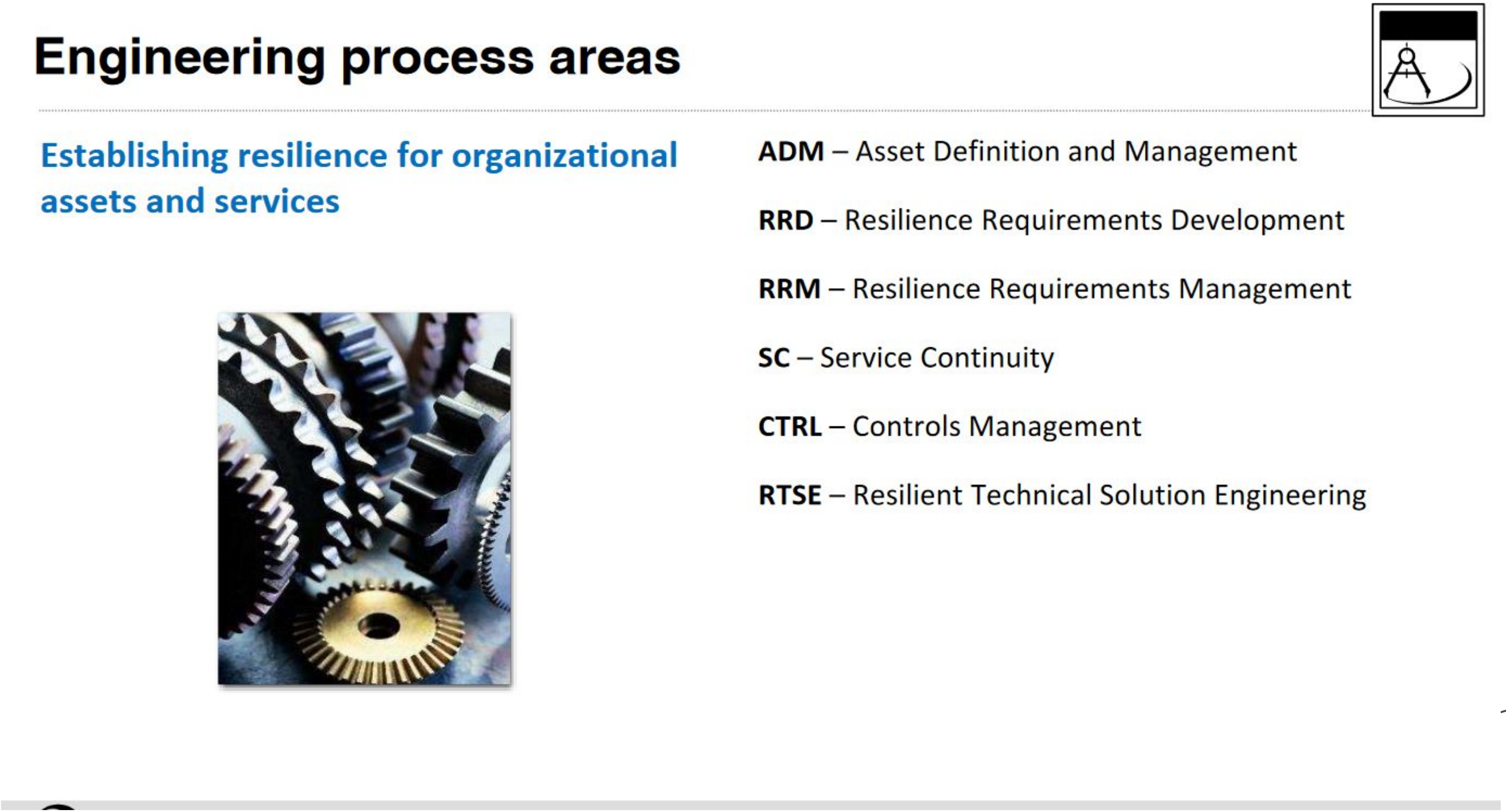
CERT-RMM накратко

Operations process areas

Managing the operational aspects of resilience

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

CERT-RMM накратко



Engineering process areas

Establishing resilience for organizational assets and services

ADM – Asset Definition and Management

RRD – Resilience Requirements Development

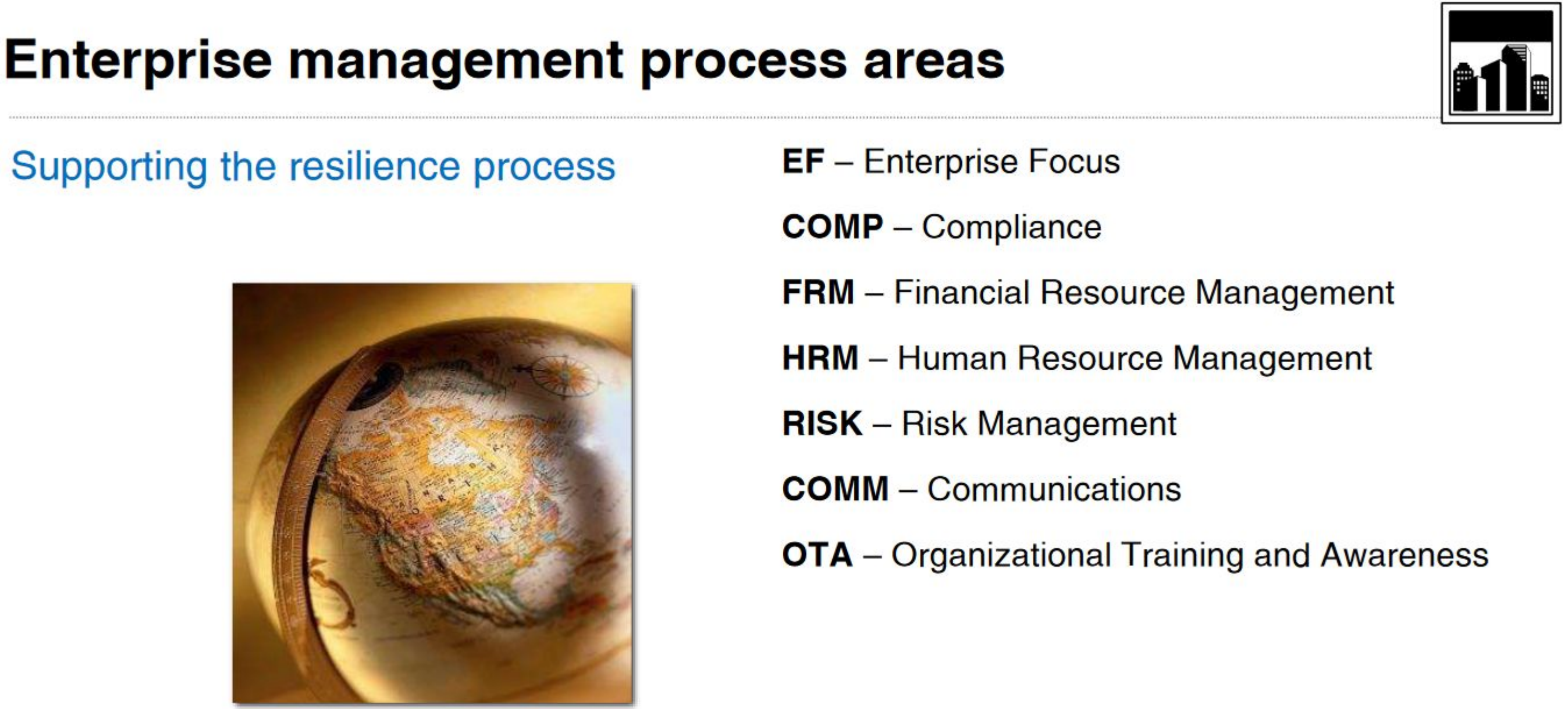
RRM – Resilience Requirements Management

SC – Service Continuity

CTRL – Controls Management

RTSE – Resilient Technical Solution Engineering

CERT-RMM накратко



Enterprise management process areas

Supporting the resilience process

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

CERT-RMM накратко

Process management process areas

Defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving processes

MON – Monitoring

MA – Measurement and Analysis

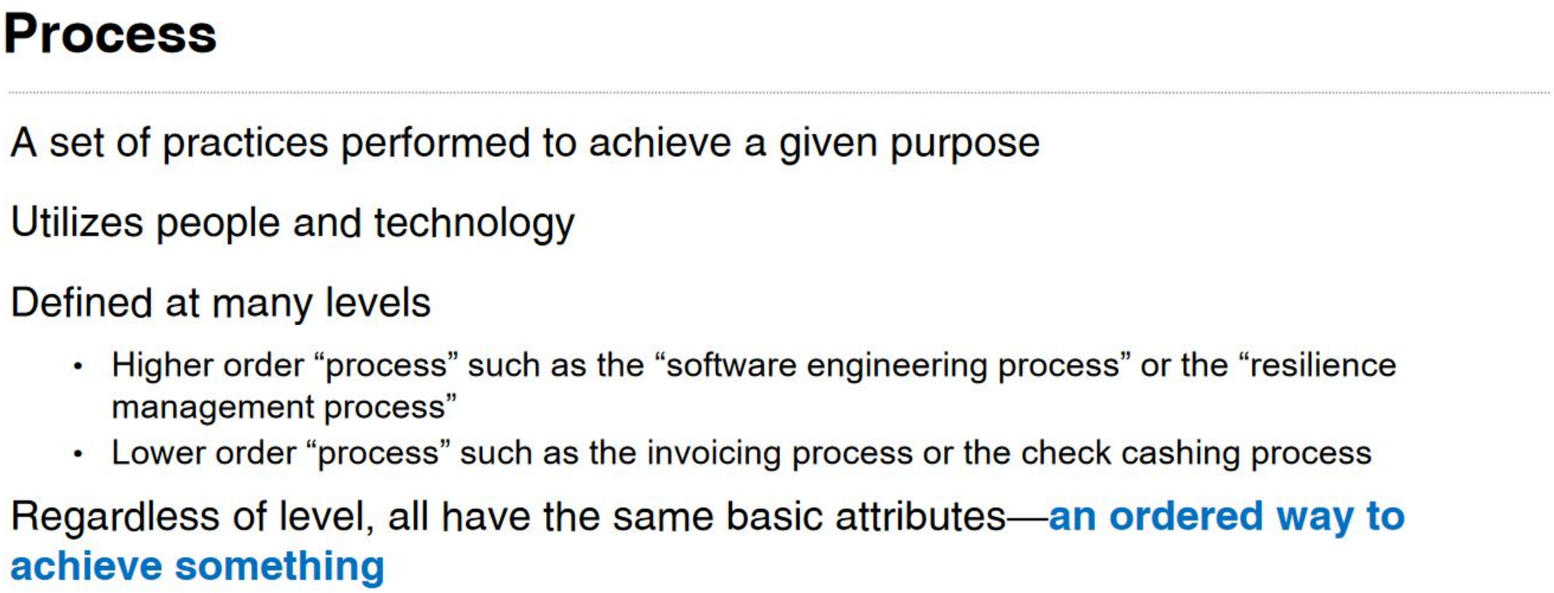
OPD – Organizational Process Definition

OPF – Organizational Process Focus

CERT-RMM накратко

Process institutionalization in CERT-RMM

CERT-RMM накратко



Process

A set of practices performed to achieve a given purpose

Utilizes people and technology

Defined at many levels

- Higher order “process” such as the “software engineering process” or the “resilience management process”
- Lower order “process” such as the invoicing process or the check cashing process

Regardless of level, all have the same basic attributes—**an ordered way to achieve something**

CERT-RMM накратко

CERT-RMM is not a prescriptive model; that is, there is no guidance provided to adopt the model in any sequential or prescriptive path.

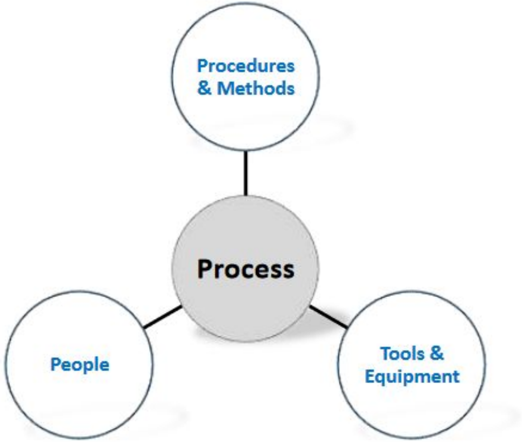
Process improvement is unique to each organization, thus CERT-RMM provides the basic structure to allow organizations to chart their own specific improvement path using the model as the basis.

CERT-RMM накратко

The value of process

Organizational improvement requires a focus on three critical dimensions: people, procedures and methods, and tools and equipment.

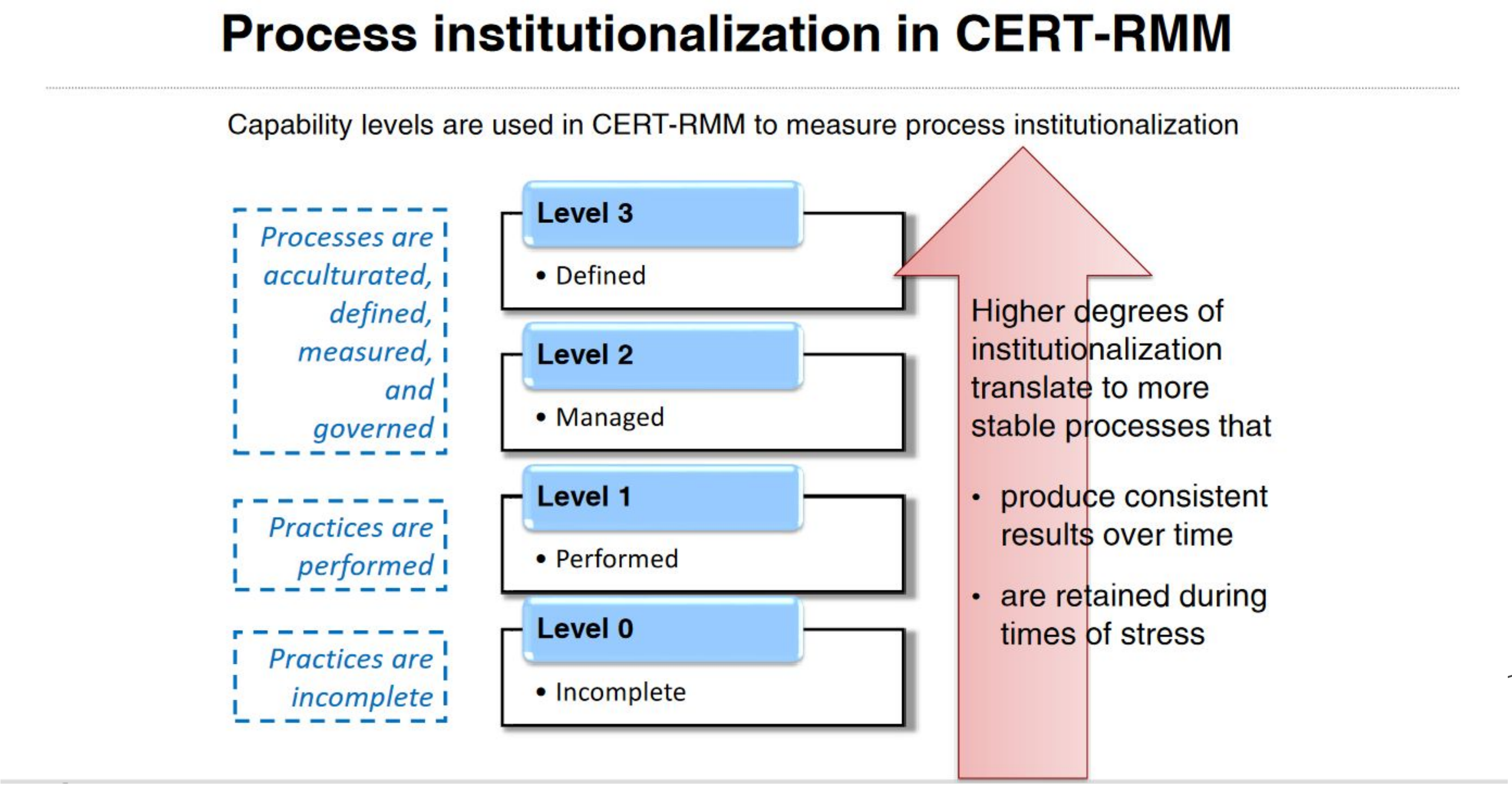
Process is what unifies these critical dimensions toward organizational objectives.



The quality of a system or product is highly influenced by the quality of the process used to acquire, develop, and maintain it. *

*Source: CMMI® for Development, Version 1.2, CMU/SEI-2006-TR-008, Software Engineering Institute, Carnegie Mellon University, August 2006

CERT-RMM накратко



Process institutionalization in CERT-RMM

Capability levels are used in CERT-RMM to measure process institutionalization

Processes are acculturated, defined, measured, and governed

Level 3
- Defined

Level 2
- Managed

Practices are performed

Level 1
- Performed

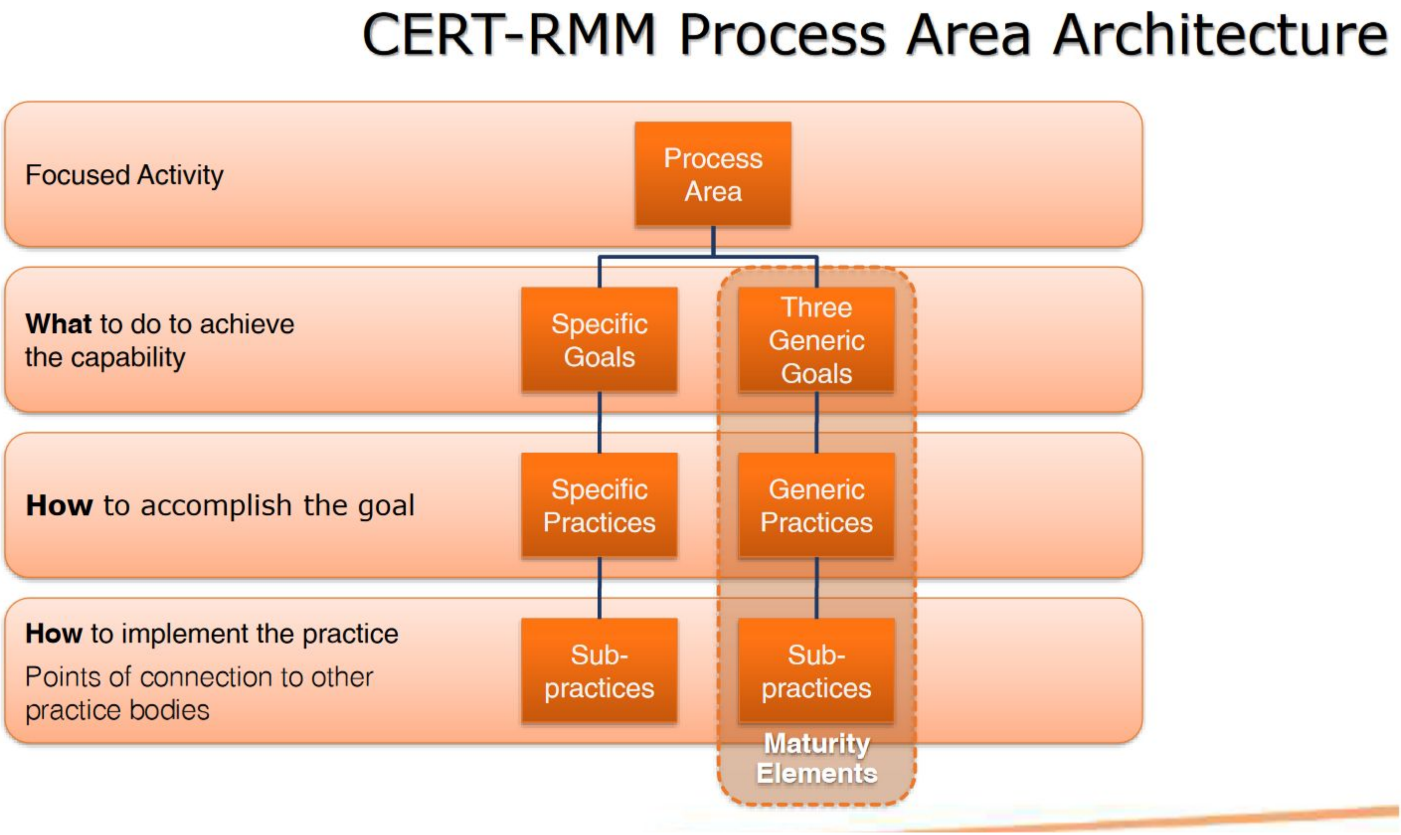
Practices are incomplete

Level 0
- Incomplete

Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

CERT-RMM накратко



CERT-RMM Process Area Architecture

Focused Activity

Process Area

What to do to achieve the capability

Specific Goals

Three Generic Goals

How to accomplish the goal

Specific Practices

Generic Practices

How to implement the practice

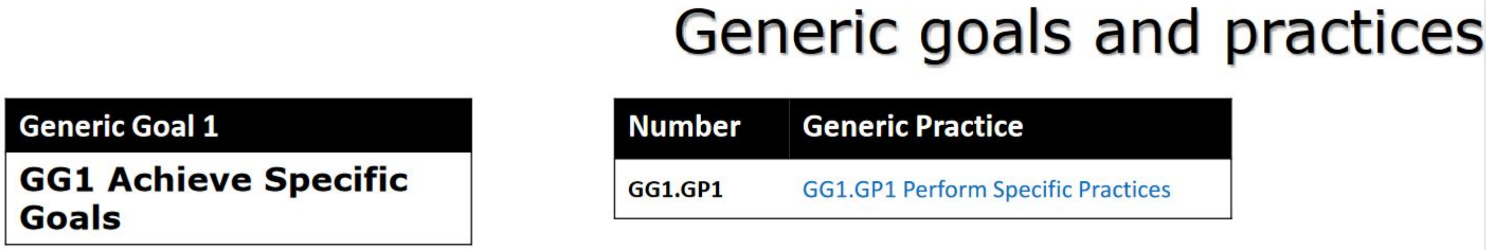
Points of connection to other practice bodies

Sub-practices

Sub-practices

Maturity Elements

CERT-RMM накратко

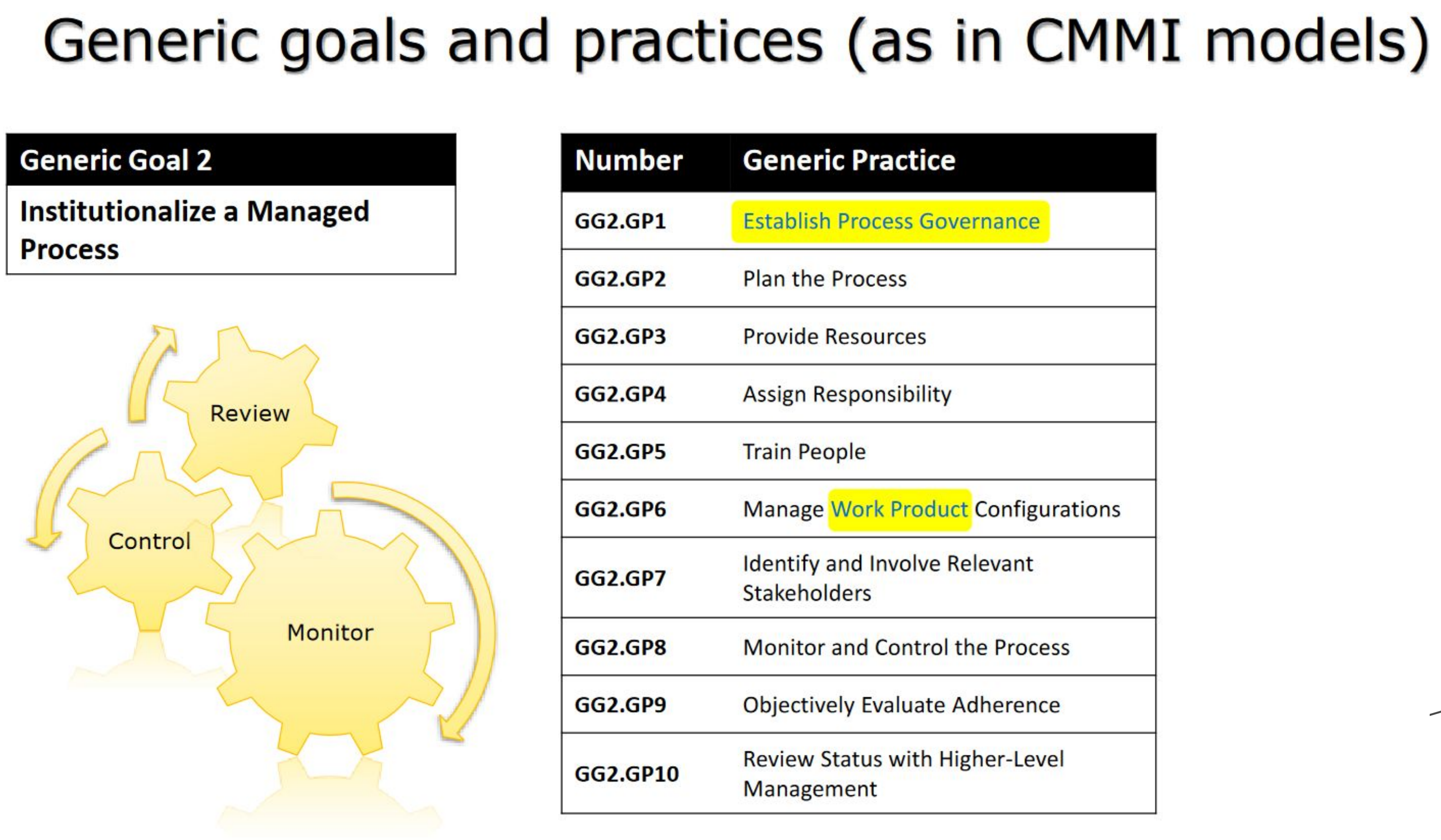


Generic goals and practices

Generic Goal 1
GG1 Achieve Specific Goals

Number	Generic Practice
GG1.GP1	GG1.GP1 Perform Specific Practices

CERT-RMM накратко



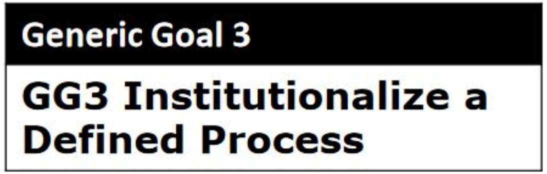
Generic goals and practices (as in CMMI models)

Generic Goal 2
Institutionalize a Managed Process

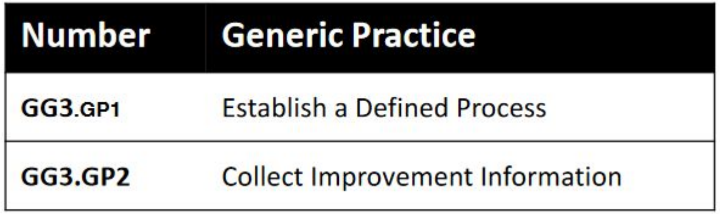
Review
Control
Monitor

Number	Generic Practice
GG2.GP1	Establish Process Governance
GG2.GP2	Plan the Process
GG2.GP3	Provide Resources
GG2.GP4	Assign Responsibility
GG2.GP5	Train People
GG2.GP6	Manage Work Product Configurations
GG2.GP7	Identify and Involve Relevant Stakeholders
GG2.GP8	Monitor and Control the Process
GG2.GP9	Objectively Evaluate Adherence
GG2.GP10	Review Status with Higher-Level Management

CERT-RMM накратко



Generic Goal 3
GG3 Institutionalize a Defined Process



Number	Generic Practice
GG3.GP1	Establish a Defined Process
GG3.GP2	Collect Improvement Information

CERT-RMM накратко

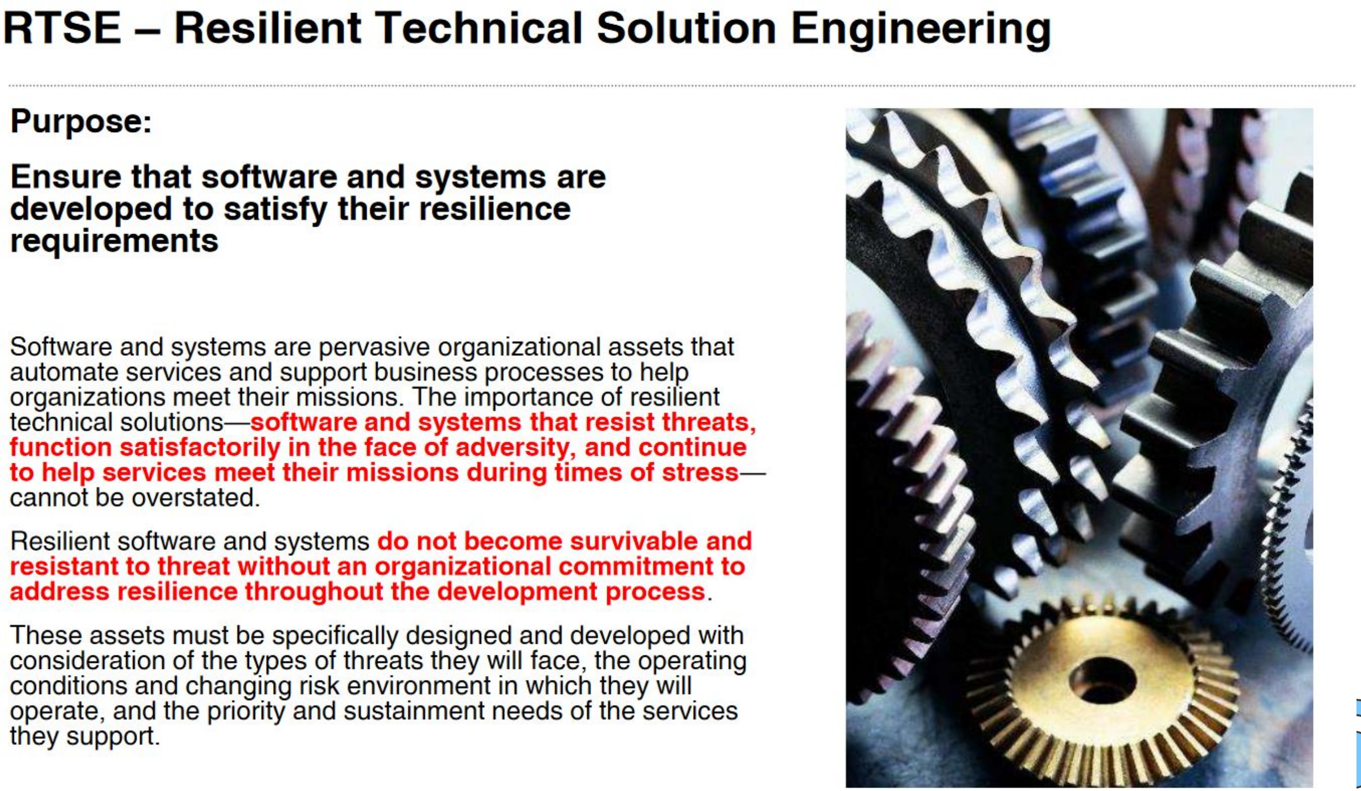
DO NOT FORGET!!!

Process ≠ Bureaucracy

Process = (Organized) Work

CERT-RMM накратко

CERT-RMM накратко



RTSE – Resilient Technical Solution Engineering

Purpose:

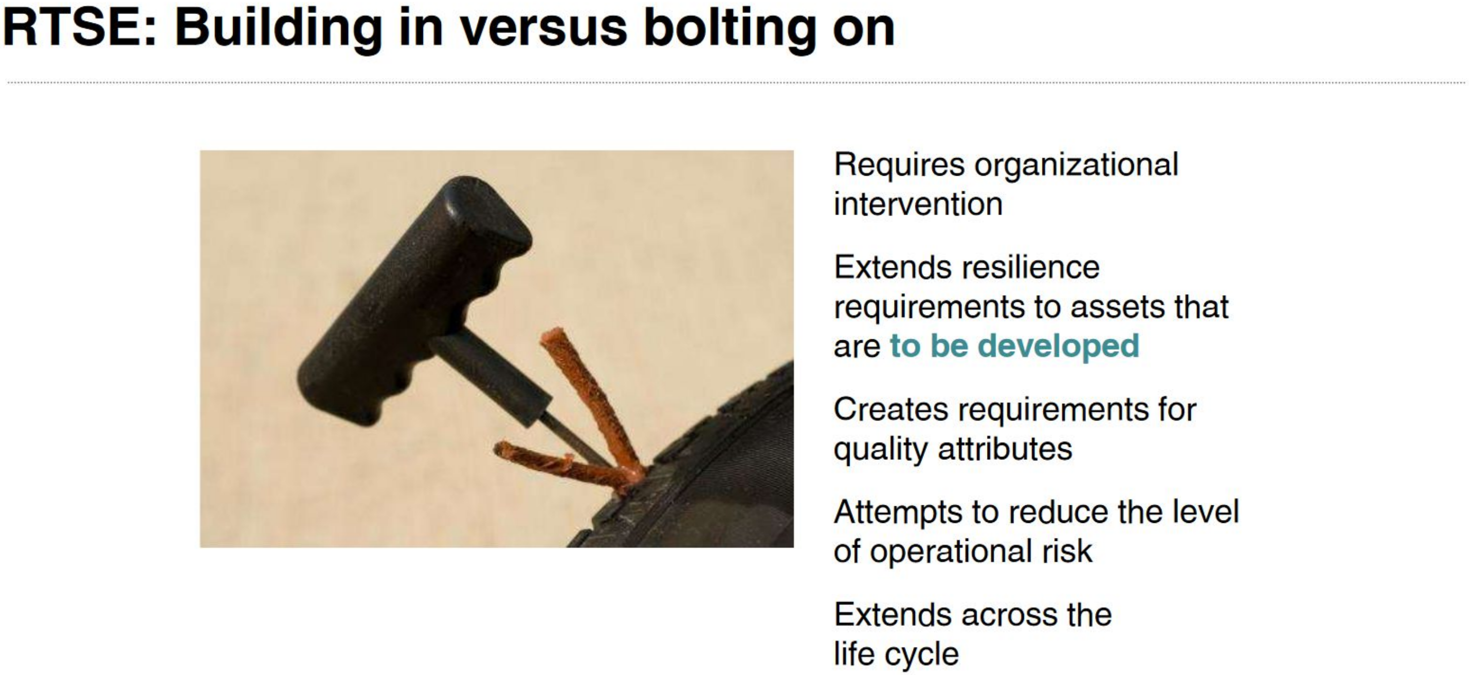
Ensure that software and systems are developed to satisfy their resilience requirements

Software and systems are pervasive organizational assets that automate services and support business processes to help organizations meet their missions. The importance of resilient technical solutions—**software and systems that resist threats, function satisfactorily in the face of adversity, and continue to help services meet their missions during times of stress**—cannot be overstated.

Resilient software and systems **do not become survivable and resistant to threat without an organizational commitment to address resilience throughout the development process**.

These assets must be specifically designed and developed with consideration of the types of threats they will face, the operating conditions and changing risk environment in which they will operate, and the priority and sustainment needs of the services they support.

CERT-RMM накратко



RTSE: Building in versus bolting on

Requires organizational intervention

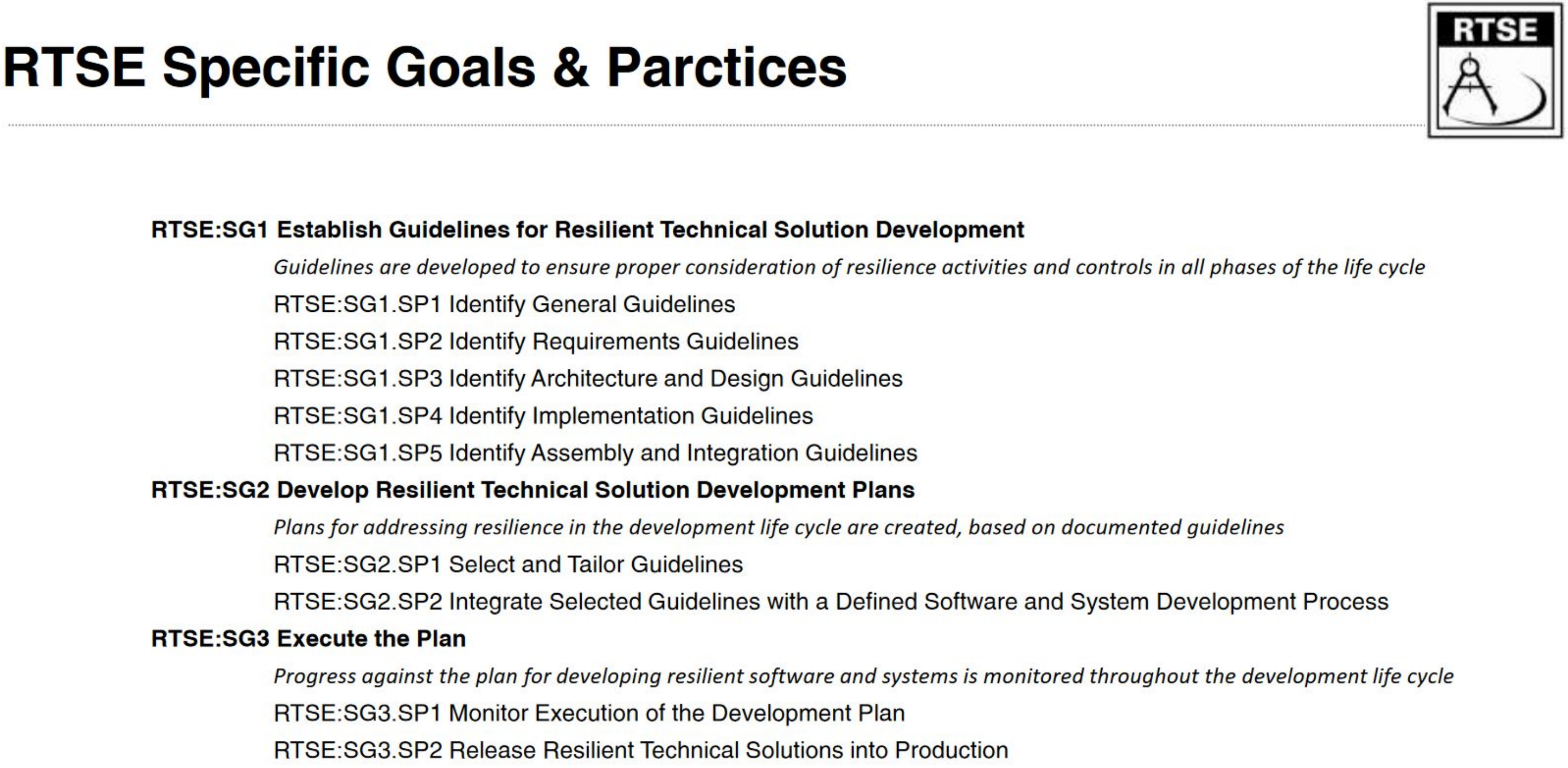
Extends resilience requirements to assets that are **to be developed**

Creates requirements for quality attributes

Attempts to reduce the level of operational risk

Extends across the life cycle

CERT-RMM накратко



RTSE Specific Goals & Parctices

RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development

Guidelines are developed to ensure proper consideration of resilience activities and controls in all phases of the life cycle

- RTSE:SG1.SP1 Identify General Guidelines
- RTSE:SG1.SP2 Identify Requirements Guidelines
- RTSE:SG1.SP3 Identify Architecture and Design Guidelines
- RTSE:SG1.SP4 Identify Implementation Guidelines
- RTSE:SG1.SP5 Identify Assembly and Integration Guidelines

RTSE:SG2 Develop Resilient Technical Solution Development Plans

Plans for addressing resilience in the development life cycle are created, based on documented guidelines

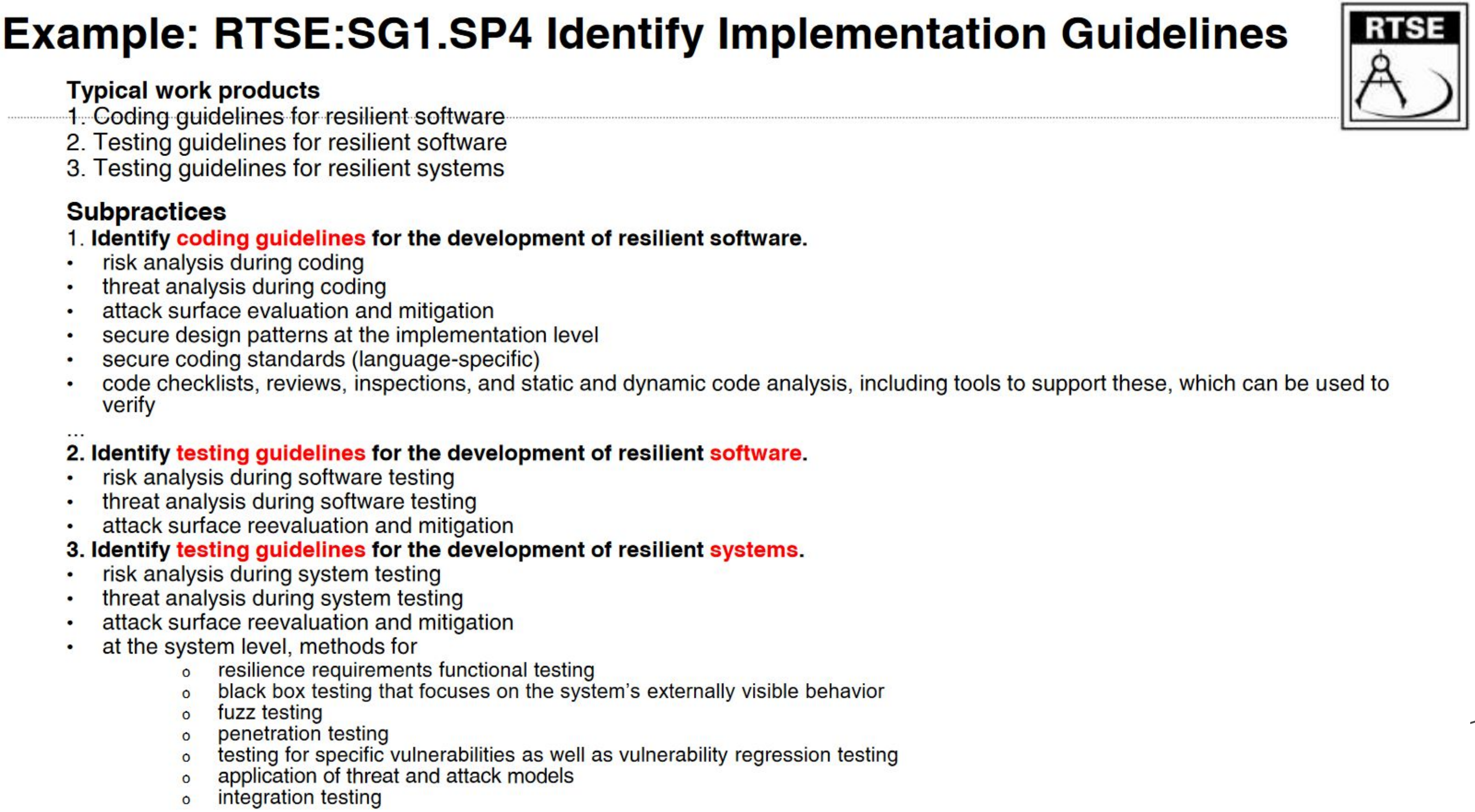
- RTSE:SG2.SP1 Select and Tailor Guidelines
- RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process

RTSE:SG3 Execute the Plan

Progress against the plan for developing resilient software and systems is monitored throughout the development life cycle

- RTSE:SG3.SP1 Monitor Execution of the Development Plan
- RTSE:SG3.SP2 Release Resilient Technical Solutions into Production

CERT-RMM накратко



Example: RTSE:SG1.SP4 Identify Implementation Guidelines

RTSE

Typical work products

1. Coding guidelines for resilient software
2. Testing guidelines for resilient software
3. Testing guidelines for resilient systems

Subpractices

1. **Identify coding guidelines for the development of resilient software.**

- risk analysis during coding
- threat analysis during coding
- attack surface evaluation and mitigation
- secure design patterns at the implementation level
- secure coding standards (language-specific)
- code checklists, reviews, inspections, and static and dynamic code analysis, including tools to support these, which can be used to verify

...

2. **Identify testing guidelines for the development of resilient software.**

- risk analysis during software testing
- threat analysis during software testing
- attack surface reevaluation and mitigation

3. **Identify testing guidelines for the development of resilient systems.**

- risk analysis during system testing
- threat analysis during system testing
- attack surface reevaluation and mitigation
- at the system level, methods for
    - resilience requirements functional testing
    - black box testing that focuses on the system’s externally visible behavior
    - fuzz testing
    - penetration testing
    - testing for specific vulnerabilities as well as vulnerability regression testing
    - application of threat and attack models
    - integration testing

CERT-RMM накратко

Incident Management and Control (IMC)

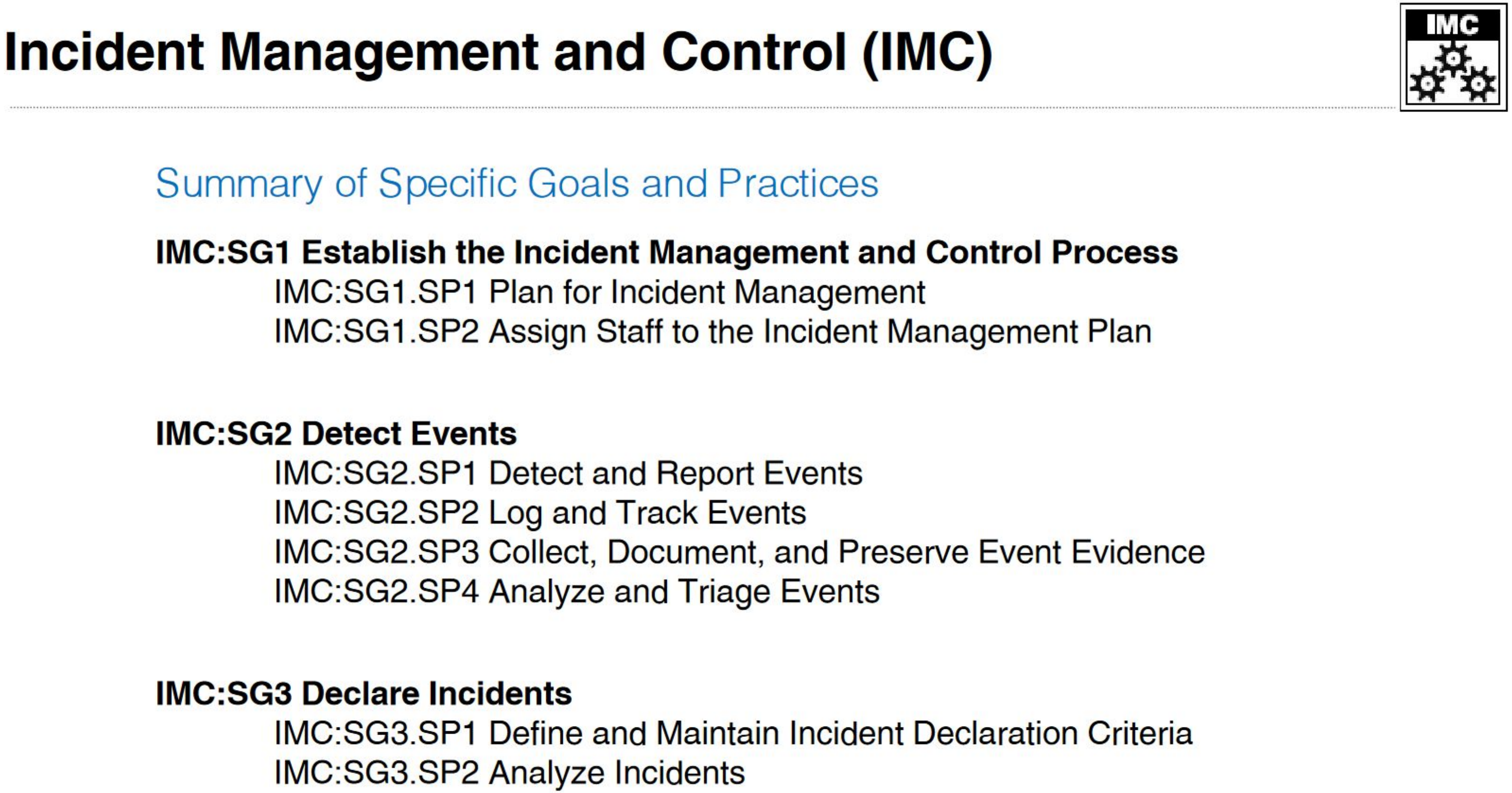
IMC

Event

Incident

Crisis

CERT-RMM накратко



Incident Management and Control (IMC)

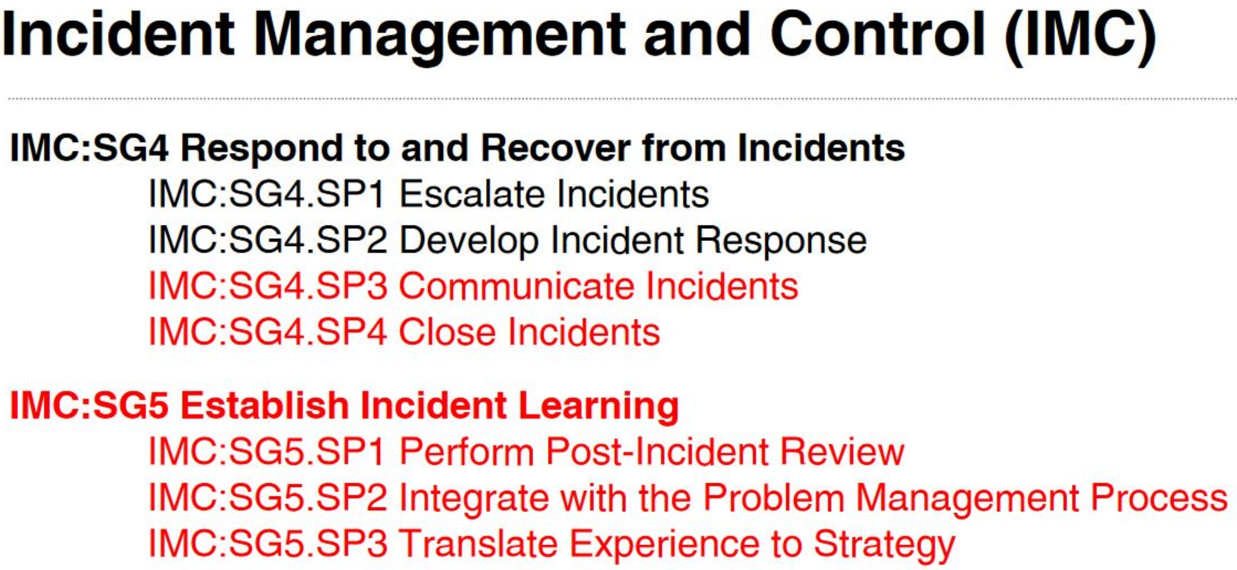
Summary of Specific Goals and Practices

IMC:SG1 Establish the Incident Management and Control Process
- IMC:SG1.SP1 Plan for Incident Management
- IMC:SG1.SP2 Assign Staff to the Incident Management Plan

IMC:SG2 Detect Events
- IMC:SG2.SP1 Detect and Report Events
- IMC:SG2.SP2 Log and Track Events
- IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence
- IMC:SG2.SP4 Analyze and Triage Events

IMC:SG3 Declare Incidents
- IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria
- IMC:SG3.SP2 Analyze Incidents

CERT-RMM накратко

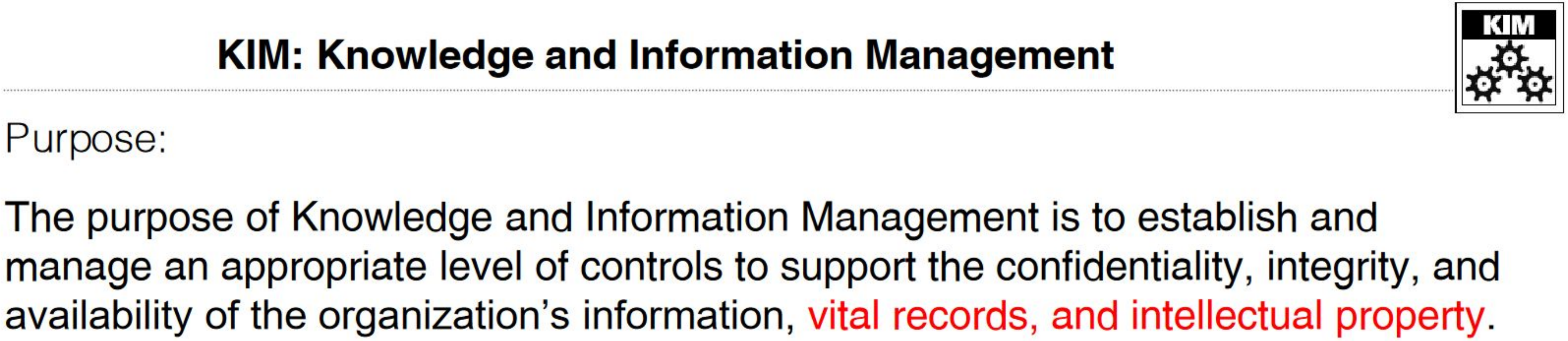


Incident Management and Control (IMC)

IMC:SG4 Respond to and Recover from Incidents
- IMC:SG4.SP1 Escalate Incidents
- IMC:SG4.SP2 Develop Incident Response
- IMC:SG4.SP3 Communicate Incidents
- IMC:SG4.SP4 Close Incidents

IMC:SG5 Establish Incident Learning
- IMC:SG5.SP1 Perform Post-Incident Review
- IMC:SG5.SP2 Integrate with the Problem Management Process
- IMC:SG5.SP3 Translate Experience to Strategy

CERT-RMM накратко

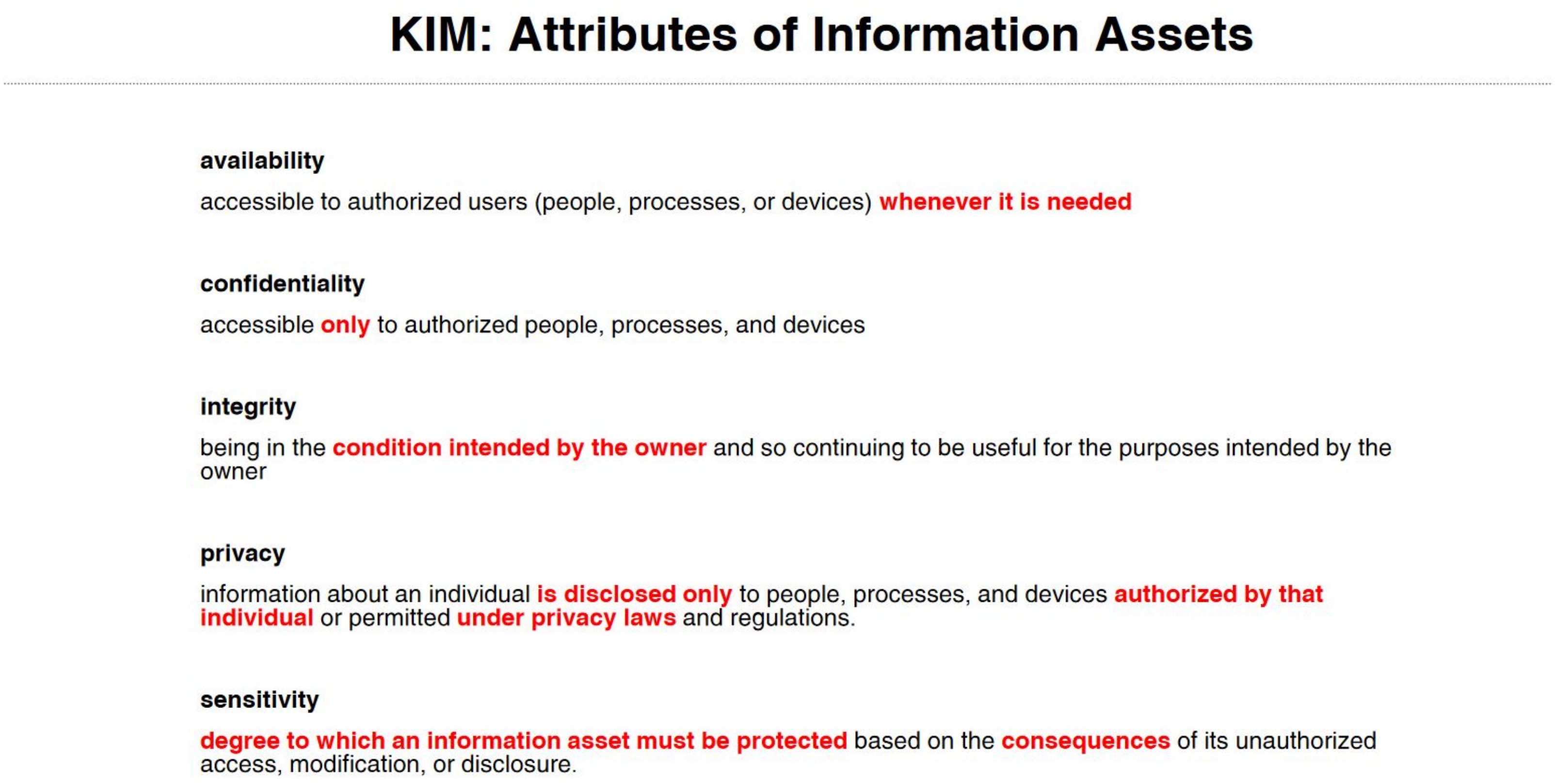


KIM: Knowledge and Information Management

Purpose:

The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization’s information, vital records, and intellectual property.

CERT-RMM накратко



KIM: Attributes of Information Assets

availability

accessible to authorized users (people, processes, or devices) **whenever it is needed**

confidentiality

accessible **only** to authorized people, processes, and devices

integrity

being in the **condition intended by the owner** and so continuing to be useful for the purposes intended by the owner

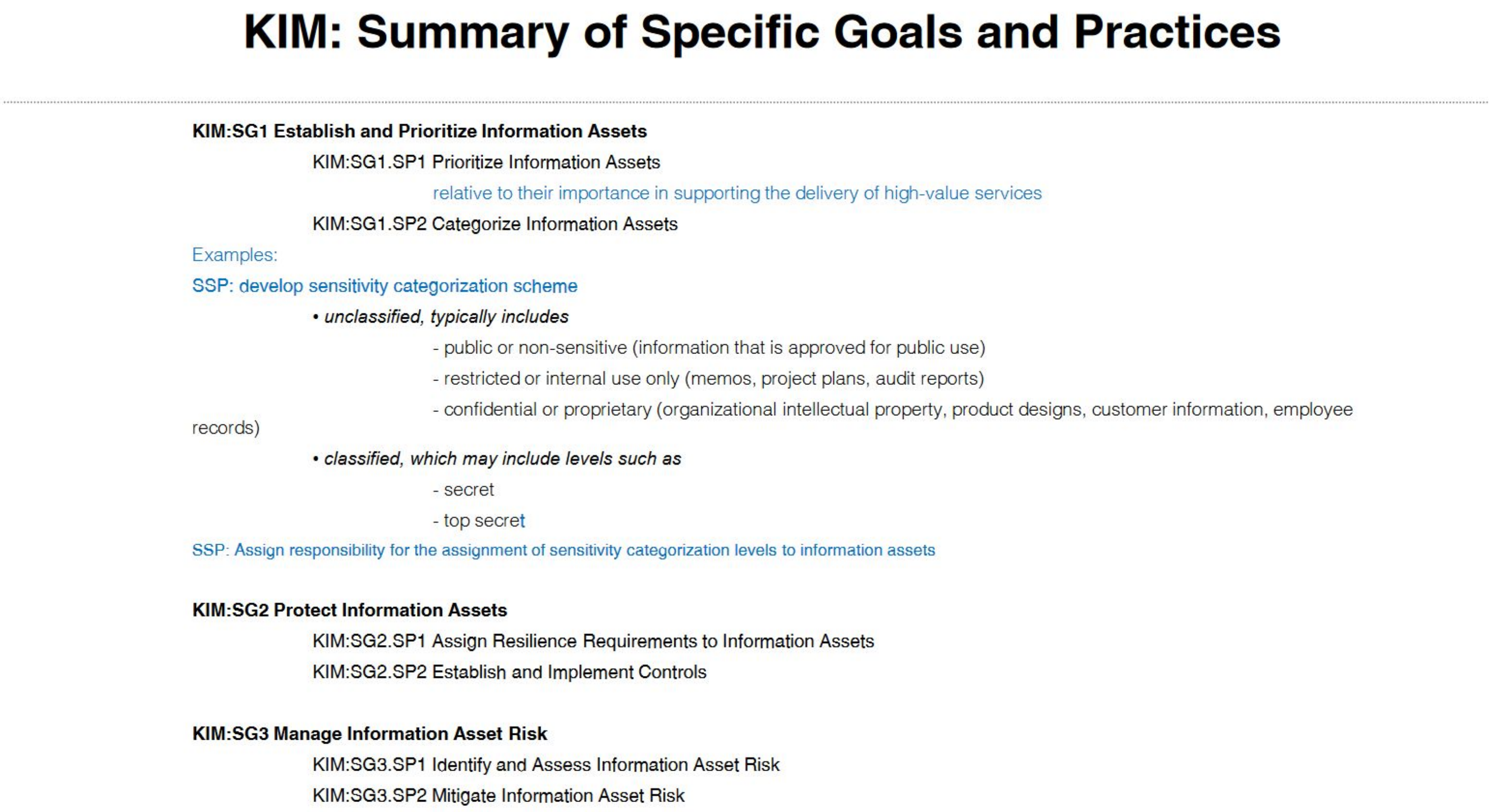
privacy

information about an individual **is disclosed only** to people, processes, and devices **authorized by that individual** or permitted **under privacy laws** and regulations.

sensitivity

degree to which an information asset must be protected based on the **consequences** of its unauthorized access, modification, or disclosure.

CERT-RMM накратко



KIM: Summary of Specific Goals and Practices

KIM:SG1 Establish and Prioritize Information Assets

- KIM:SG1.SP1 Prioritize Information Assets
  - relative to their importance in supporting the delivery of high-value services
- KIM:SG1.SP2 Categorize Information Assets

Examples:

SSP: develop sensitivity categorization scheme

- *unclassified, typically includes*
  - public or non-sensitive (information that is approved for public use)
  - restricted or internal use only (memos, project plans, audit reports)
  - confidential or proprietary (organizational intellectual property, product designs, customer information, employee records)
- *classified, which may include levels such as*
  - secret
  - top secret

SSP: Assign responsibility for the assignment of sensitivity categorization levels to information assets

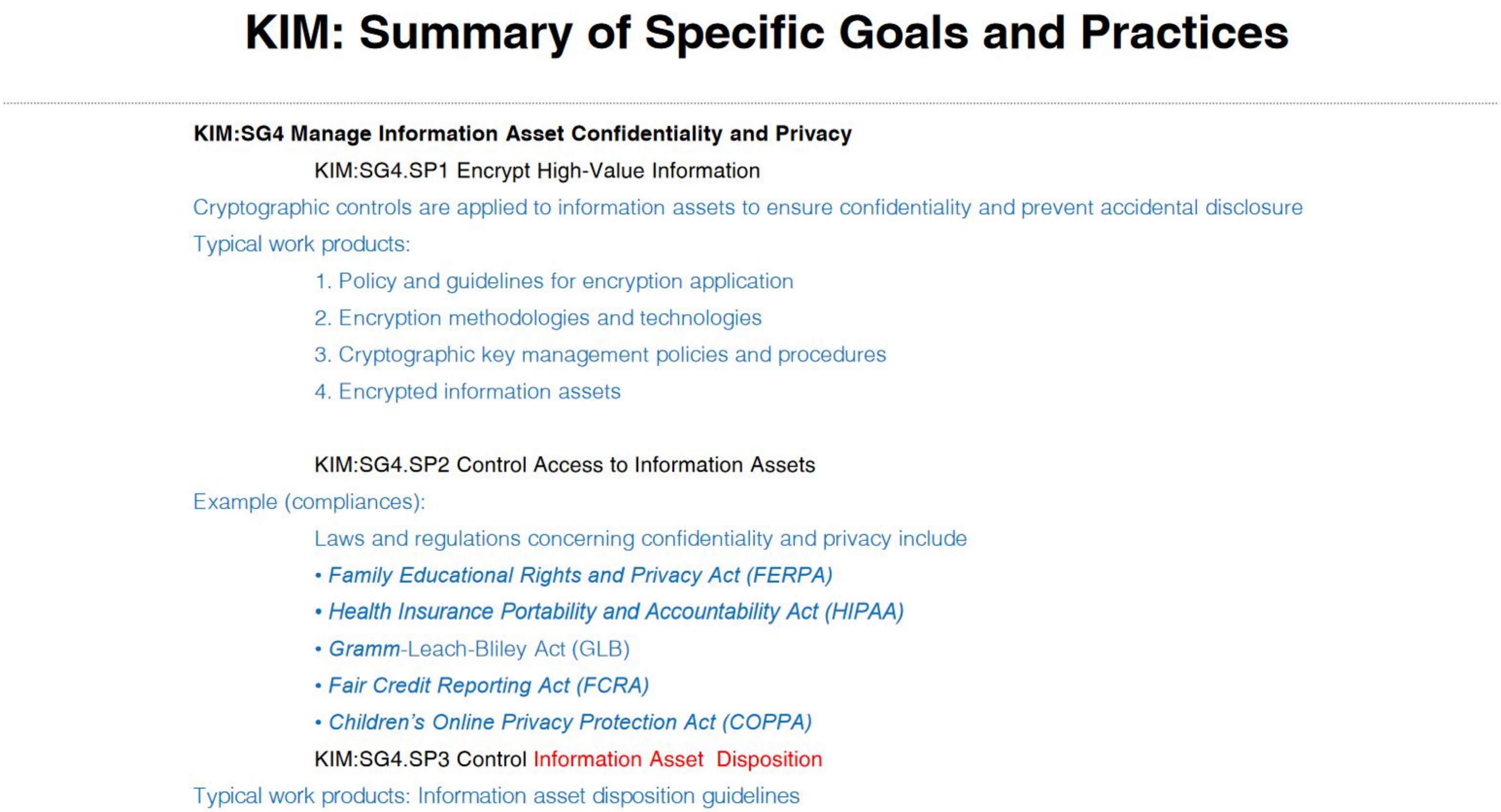
KIM:SG2 Protect Information Assets

- KIM:SG2.SP1 Assign Resilience Requirements to Information Assets
- KIM:SG2.SP2 Establish and Implement Controls

KIM:SG3 Manage Information Asset Risk

- KIM:SG3.SP1 Identify and Assess Information Asset Risk
- KIM:SG3.SP2 Mitigate Information Asset Risk

CERT-RMM накратко



KIM: Summary of Specific Goals and Practices

KIM:SG4 Manage Information Asset Confidentiality and Privacy

KIM:SG4.SP1 Encrypt High-Value Information

Cryptographic controls are applied to information assets to ensure confidentiality and prevent accidental disclosure

Typical work products:

1. Policy and guidelines for encryption application
2. Encryption methodologies and technologies
3. Cryptographic key management policies and procedures
4. Encrypted information assets

KIM:SG4.SP2 Control Access to Information Assets

Example (compliances):

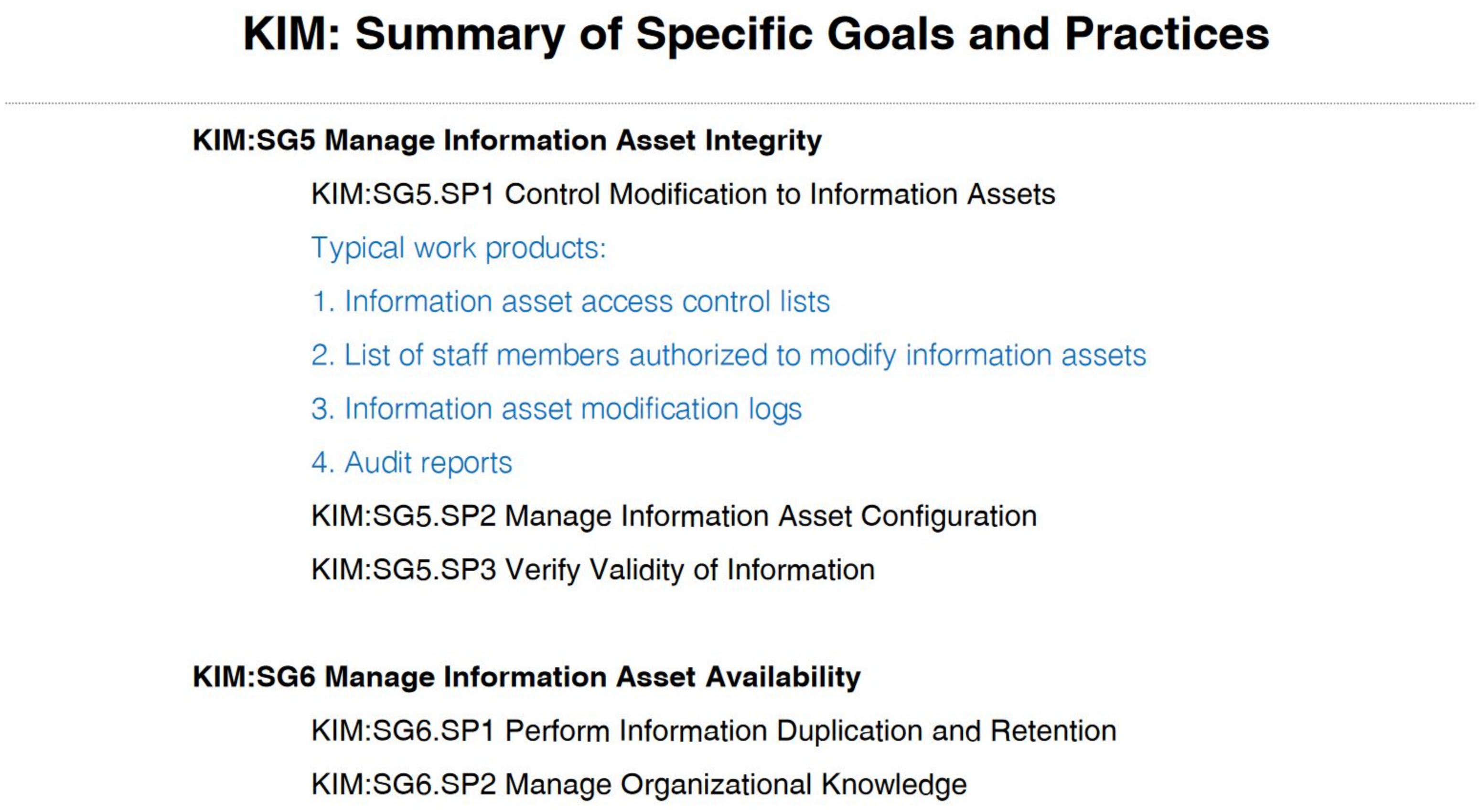
Laws and regulations concerning confidentiality and privacy include

- *Family Educational Rights and Privacy Act (FERPA)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Gramm*-Leach-Bliley Act (GLB)
- *Fair Credit Reporting Act (FCRA)*
- *Children's Online Privacy Protection Act (COPPA)*

KIM:SG4.SP3 Control Information Asset Disposition

Typical work products: Information asset disposition guidelines

CERT-RMM накратко



KIM: Summary of Specific Goals and Practices

KIM:SG5 Manage Information Asset Integrity

KIM:SG5.SP1 Control Modification to Information Assets

Typical work products:

1. Information asset access control lists
2. List of staff members authorized to modify information assets
3. Information asset modification logs
4. Audit reports

KIM:SG5.SP2 Manage Information Asset Configuration

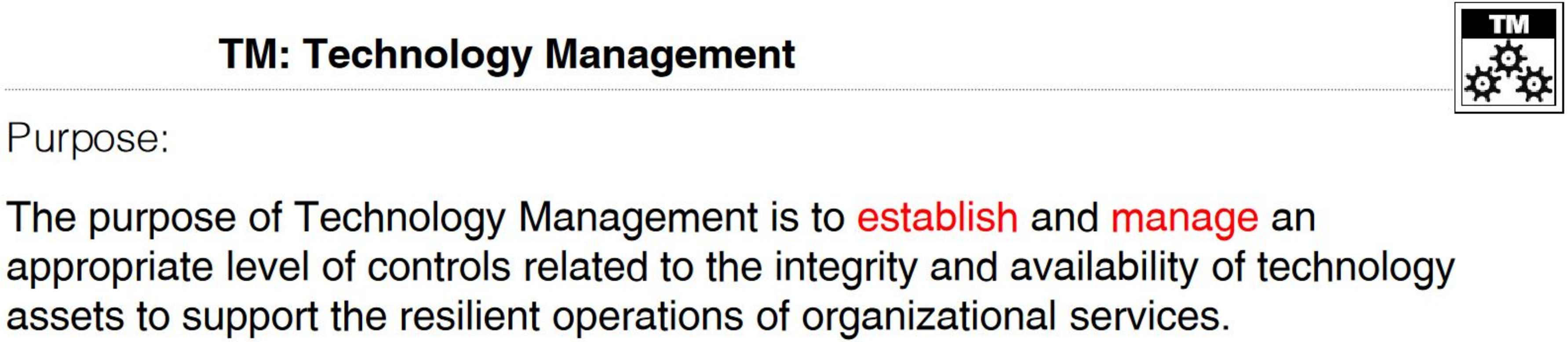
KIM:SG5.SP3 Verify Validity of Information

KIM:SG6 Manage Information Asset Availability

KIM:SG6.SP1 Perform Information Duplication and Retention

KIM:SG6.SP2 Manage Organizational Knowledge

CERT-RMM накратко



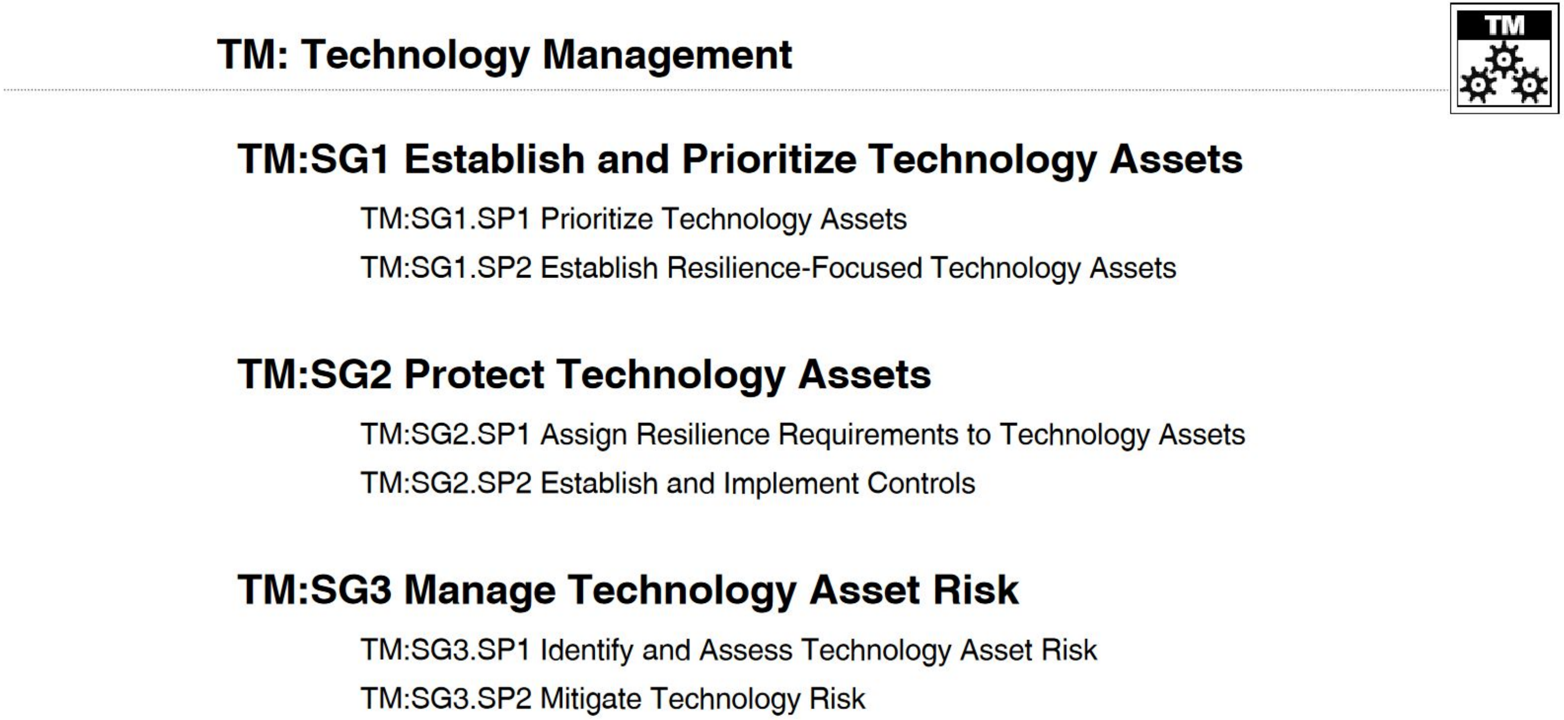
TM: Technology Management

TM

Purpose:

The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

CERT-RMM накратко



TM: Technology Management

TM:SG1 Establish and Prioritize Technology Assets

TM:SG1.SP1 Prioritize Technology Assets

TM:SG1.SP2 Establish Resilience-Focused Technology Assets

TM:SG2 Protect Technology Assets

TM:SG2.SP1 Assign Resilience Requirements to Technology Assets

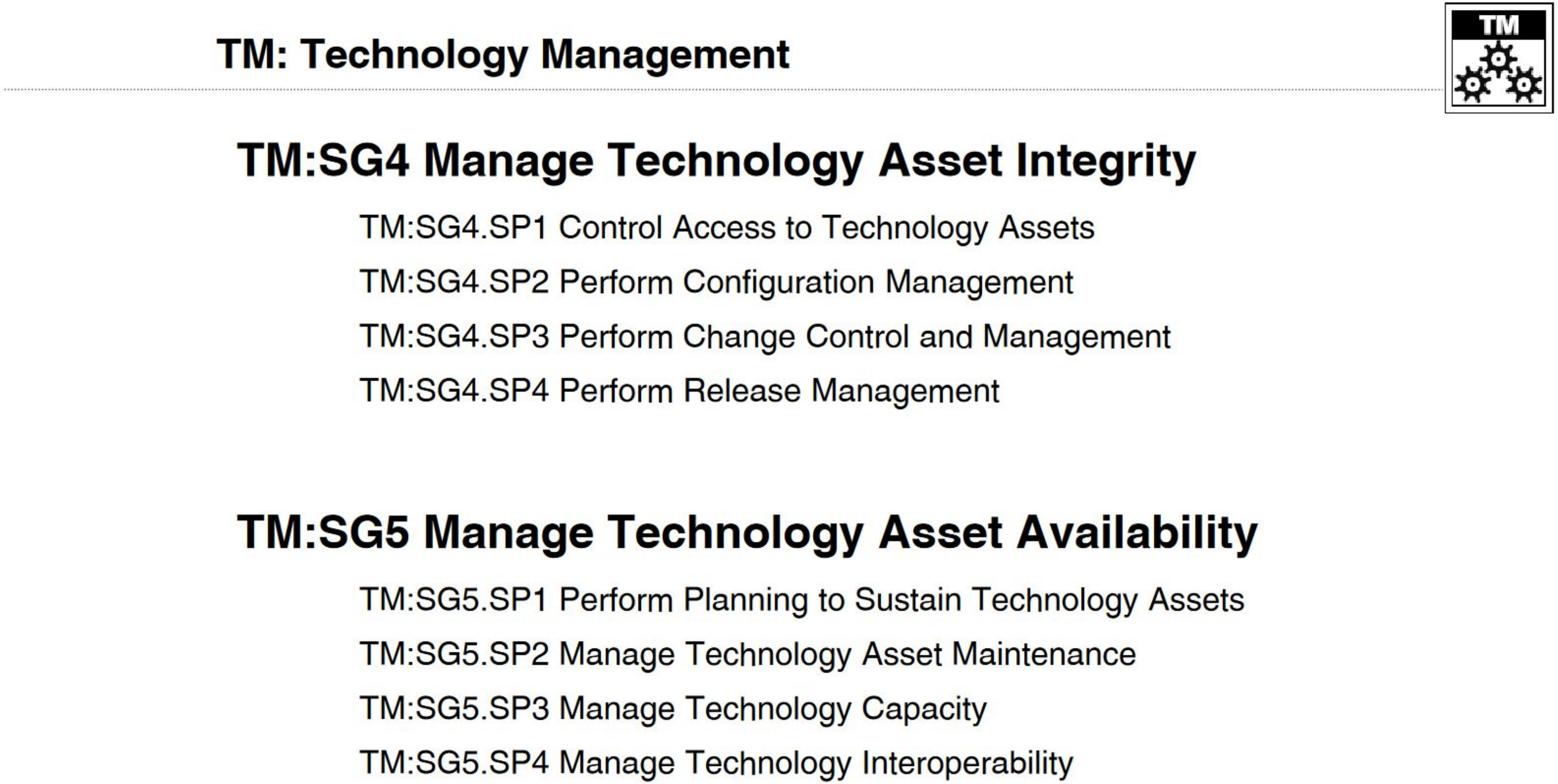
TM:SG2.SP2 Establish and Implement Controls

TM:SG3 Manage Technology Asset Risk

TM:SG3.SP1 Identify and Assess Technology Asset Risk

TM:SG3.SP2 Mitigate Technology Risk

CERT-RMM накратко



TM: Technology Management

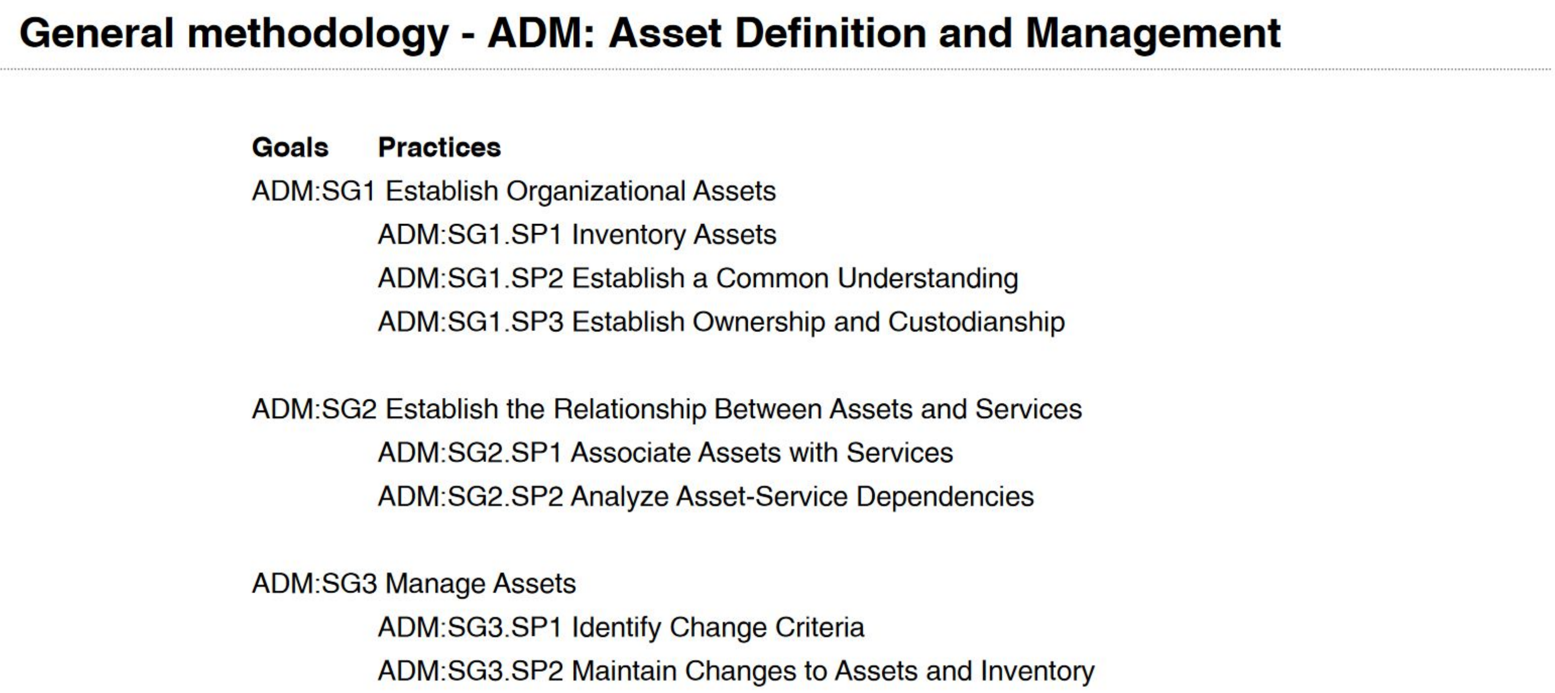
TM:SG4 Manage Technology Asset Integrity

TM:SG4.SP1 Control Access to Technology Assets
TM:SG4.SP2 Perform Configuration Management
TM:SG4.SP3 Perform Change Control and Management
TM:SG4.SP4 Perform Release Management

TM:SG5 Manage Technology Asset Availability

TM:SG5.SP1 Perform Planning to Sustain Technology Assets
TM:SG5.SP2 Manage Technology Asset Maintenance
TM:SG5.SP3 Manage Technology Capacity
TM:SG5.SP4 Manage Technology Interoperability

CERT-RMM накратко



General methodology - ADM: Asset Definition and Management

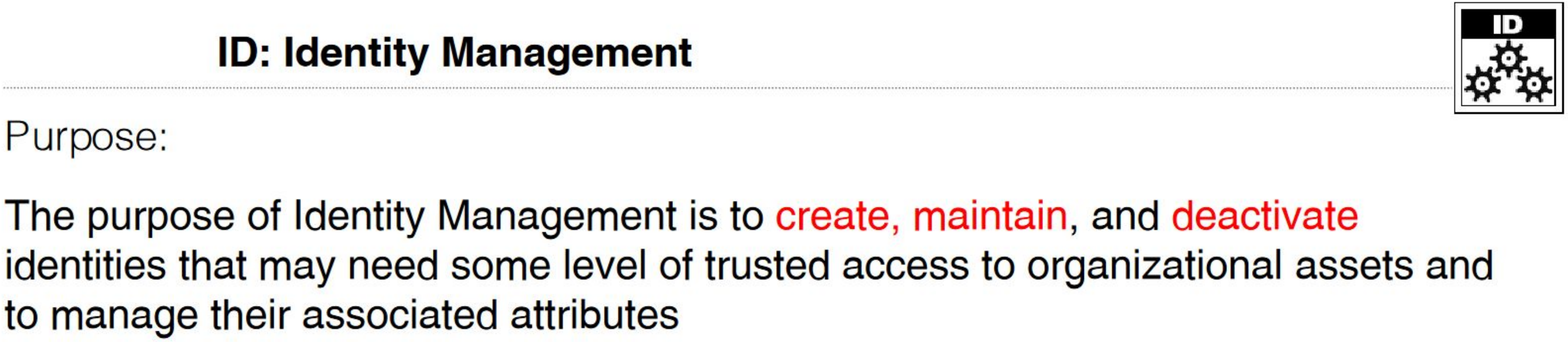
Goals **Practices**

- ADM:SG1 Establish Organizational Assets
    - ADM:SG1.SP1 Inventory Assets
    - ADM:SG1.SP2 Establish a Common Understanding
    - ADM:SG1.SP3 Establish Ownership and Custodianship

- ADM:SG2 Establish the Relationship Between Assets and Services
    - ADM:SG2.SP1 Associate Assets with Services
    - ADM:SG2.SP2 Analyze Asset-Service Dependencies

- ADM:SG3 Manage Assets
    - ADM:SG3.SP1 Identify Change Criteria
    - ADM:SG3.SP2 Maintain Changes to Assets and Inventory

CERT-RMM накратко

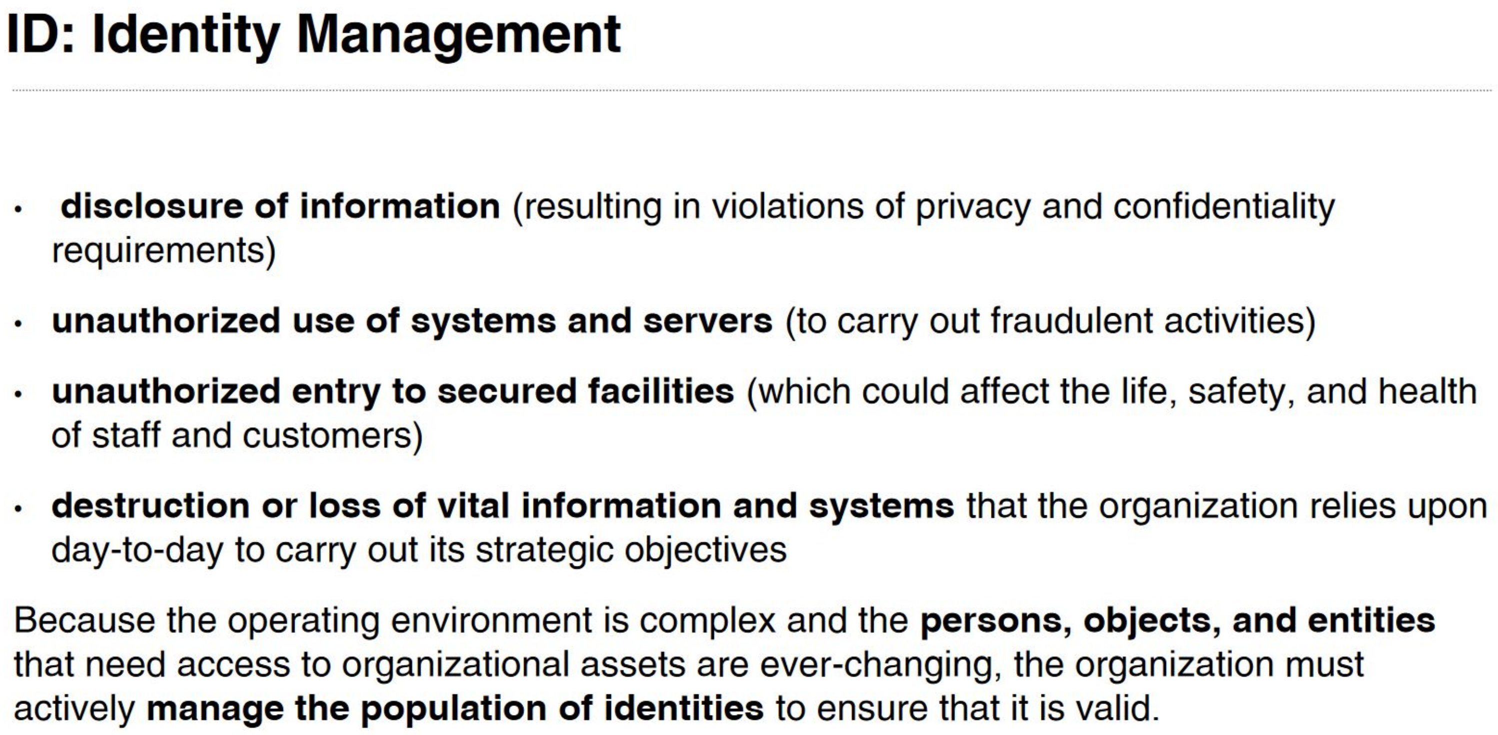


ID: Identity Management

Purpose:

The purpose of Identity Management is to create, maintain, and deactivate identities that may need some level of trusted access to organizational assets and to manage their associated attributes

CERT-RMM накратко

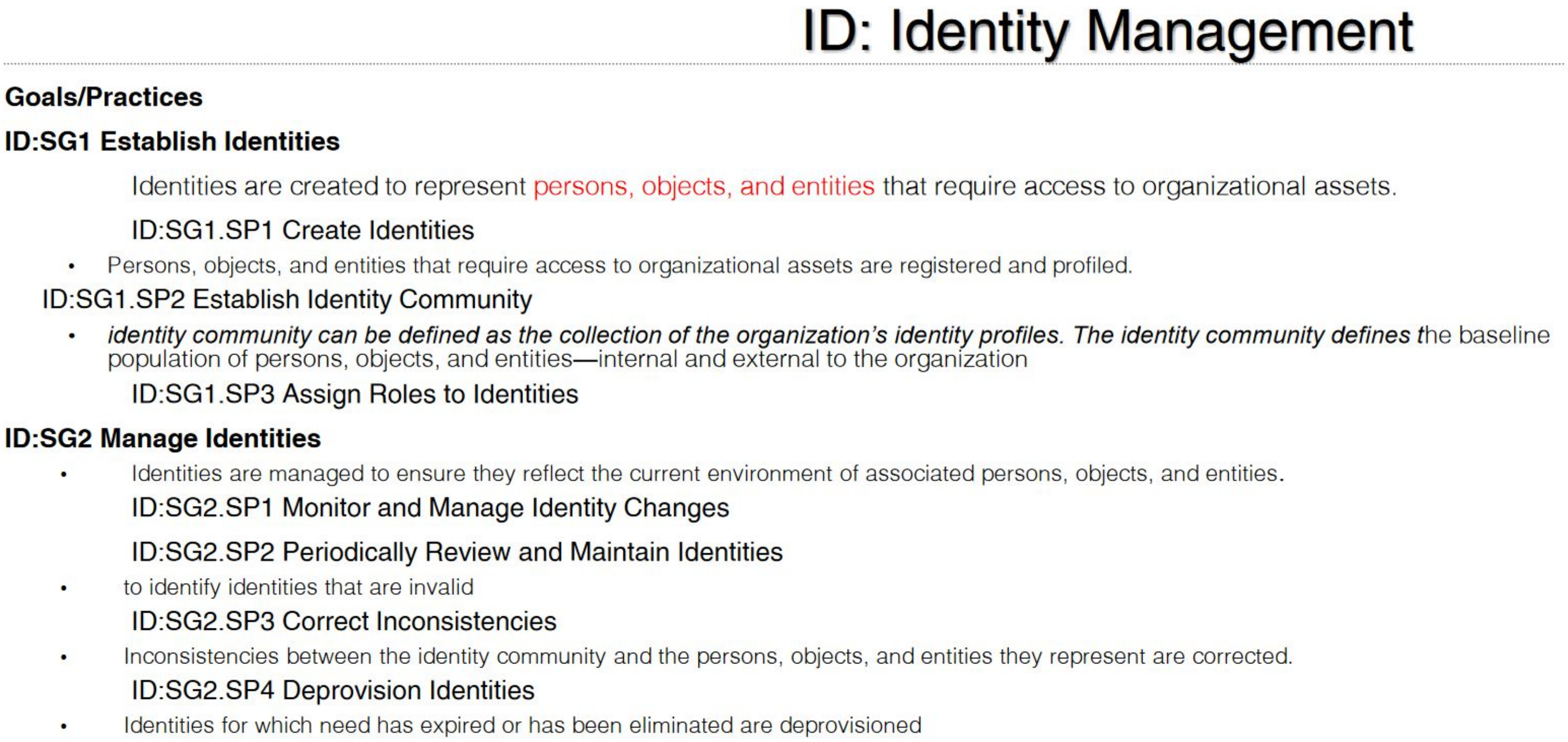


ID: Identity Management

- **disclosure of information** (resulting in violations of privacy and confidentiality requirements)
- **unauthorized use of systems and servers** (to carry out fraudulent activities)
- **unauthorized entry to secured facilities** (which could affect the life, safety, and health of staff and customers)
- **destruction or loss of vital information and systems** that the organization relies upon day-to-day to carry out its strategic objectives

Because the operating environment is complex and the **persons, objects, and entities** that need access to organizational assets are ever-changing, the organization must actively **manage the population of identities** to ensure that it is valid.

CERT-RMM накратко



ID: Identity Management

Goals/Practices

ID:SG1 Establish Identities

Identities are created to represent persons, objects, and entities that require access to organizational assets.

ID:SG1.SP1 Create Identities

- Persons, objects, and entities that require access to organizational assets are registered and profiled.

ID:SG1.SP2 Establish Identity Community

- *identity community can be defined as the collection of the organization's identity profiles. The identity community defines t*he baseline population of persons, objects, and entities—internal and external to the organization

ID:SG1.SP3 Assign Roles to Identities

ID:SG2 Manage Identities

- Identities are managed to ensure they reflect the current environment of associated persons, objects, and entities.

ID:SG2.SP1 Monitor and Manage Identity Changes

ID:SG2.SP2 Periodically Review and Maintain Identities

- to identify identities that are invalid

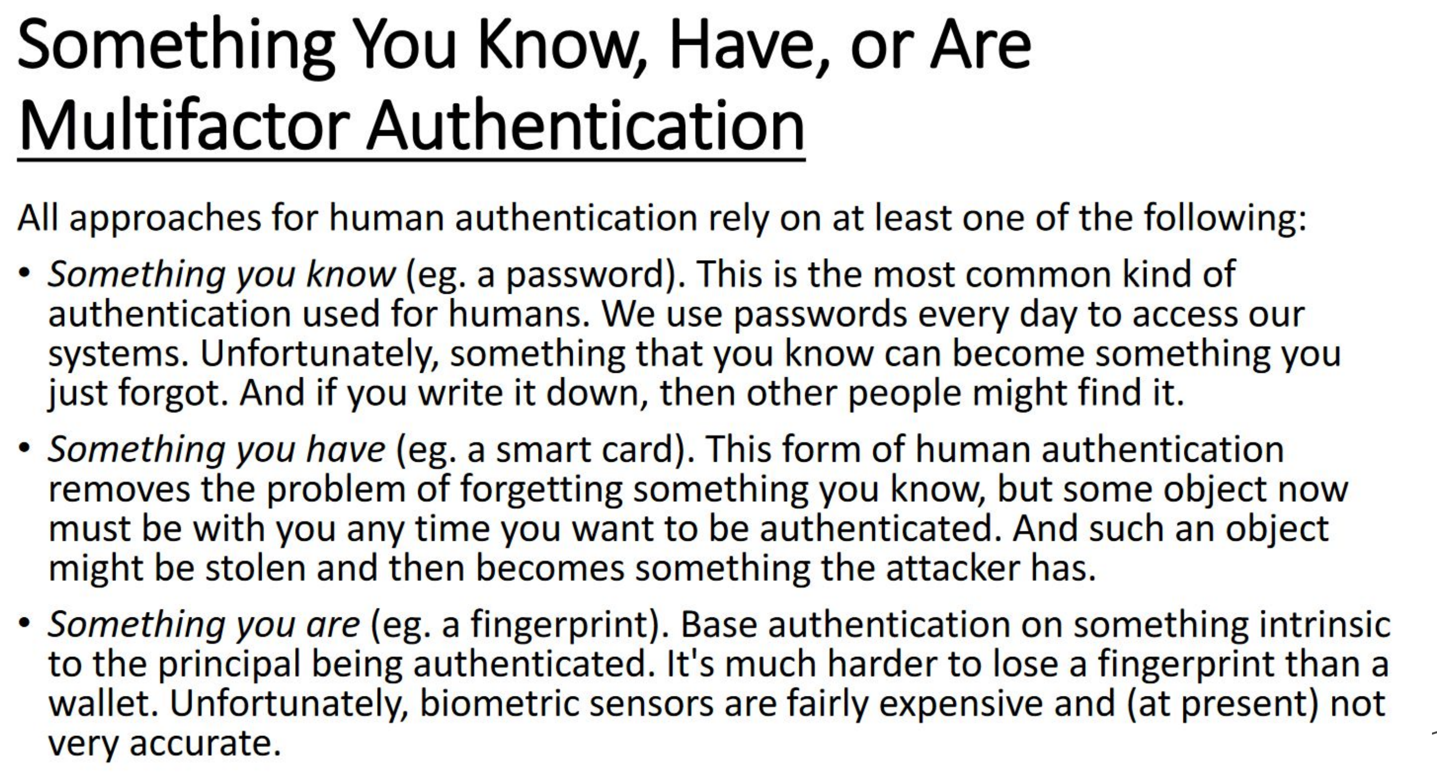
ID:SG2.SP3 Correct Inconsistencies

- Inconsistencies between the identity community and the persons, objects, and entities they represent are corrected.

ID:SG2.SP4 Deprovision Identities

- Identities for which need has expired or has been eliminated are deprovisioned

CERT-RMM накратко



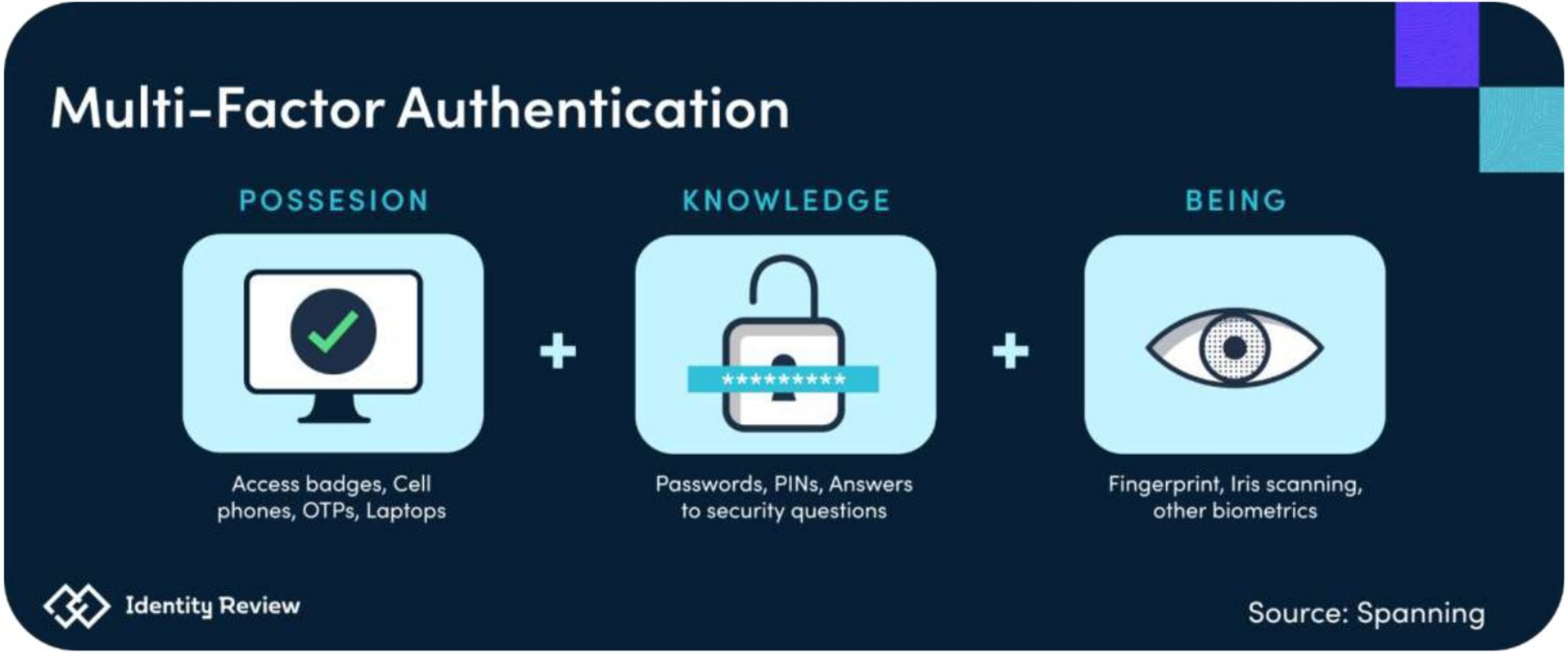
Something You Know, Have, or Are

Multifactor Authentication

All approaches for human authentication rely on at least one of the following:

- *Something you know* (eg. a password). This is the most common kind of authentication used for humans. We use passwords every day to access our systems. Unfortunately, something that you know can become something you just forgot. And if you write it down, then other people might find it.
- *Something you have* (eg. a smart card). This form of human authentication removes the problem of forgetting something you know, but some object now must be with you any time you want to be authenticated. And such an object might be stolen and then becomes something the attacker has.
- *Something you are* (eg. a fingerprint). Base authentication on something intrinsic to the principal being authenticated. It's much harder to lose a fingerprint than a wallet. Unfortunately, biometric sensors are fairly expensive and (at present) not very accurate.

CERT-RMM накратко



Multi-Factor Authentication

POSSESION

Access badges, Cell phones, OTPs, Laptops

+

KNOWLEDGE

Passwords, PINs, Answers to security questions

+

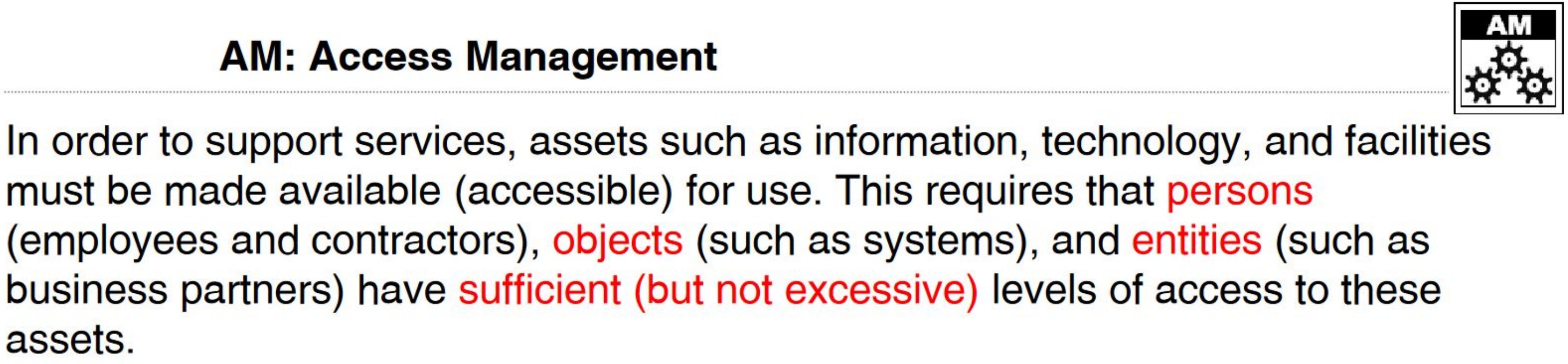
BEING

Fingerprint, Iris scanning, other biometrics

Identity Review

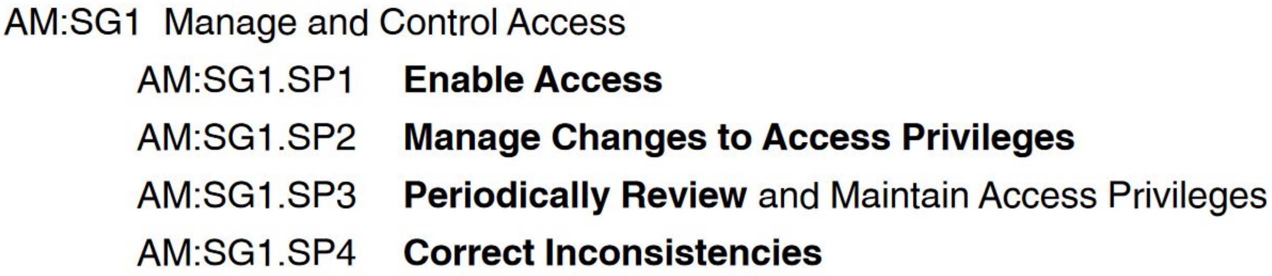
Source: Spanning

CERT-RMM накратко



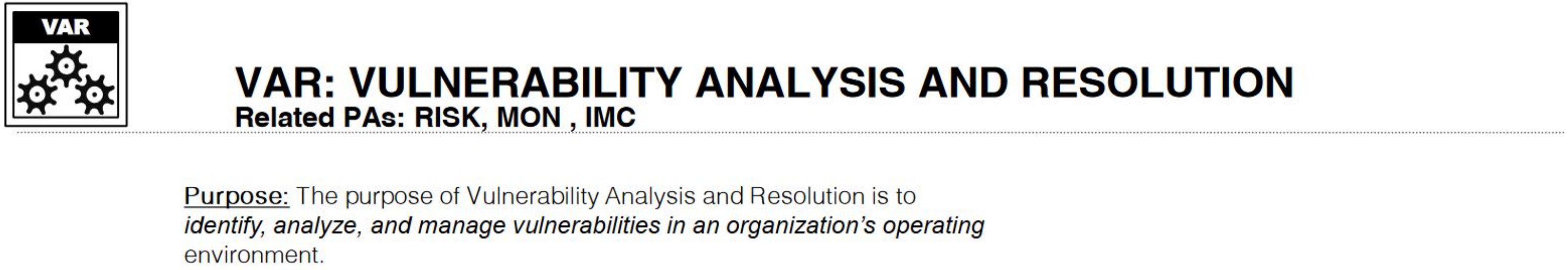
AM: Access Management

In order to support services, assets such as information, technology, and facilities must be made available (accessible) for use. This requires that persons (employees and contractors), objects (such as systems), and entities (such as business partners) have sufficient (but not excessive) levels of access to these assets.



AM:SG1 Manage and Control Access
  - AM:SG1.SP1 **Enable Access**
  - AM:SG1.SP2 **Manage Changes to Access Privileges**
  - AM:SG1.SP3 **Periodically Review** and Maintain Access Privileges
  - AM:SG1.SP4 **Correct Inconsistencies**

CERT-RMM накратко



VAR

VAR: VULNERABILITY ANALYSIS AND RESOLUTION

Related PAs: RISK, MON , IMC

Purpose: The purpose of Vulnerability Analysis and Resolution is to *identify, analyze, and manage vulnerabilities in an organization's operating* environment.

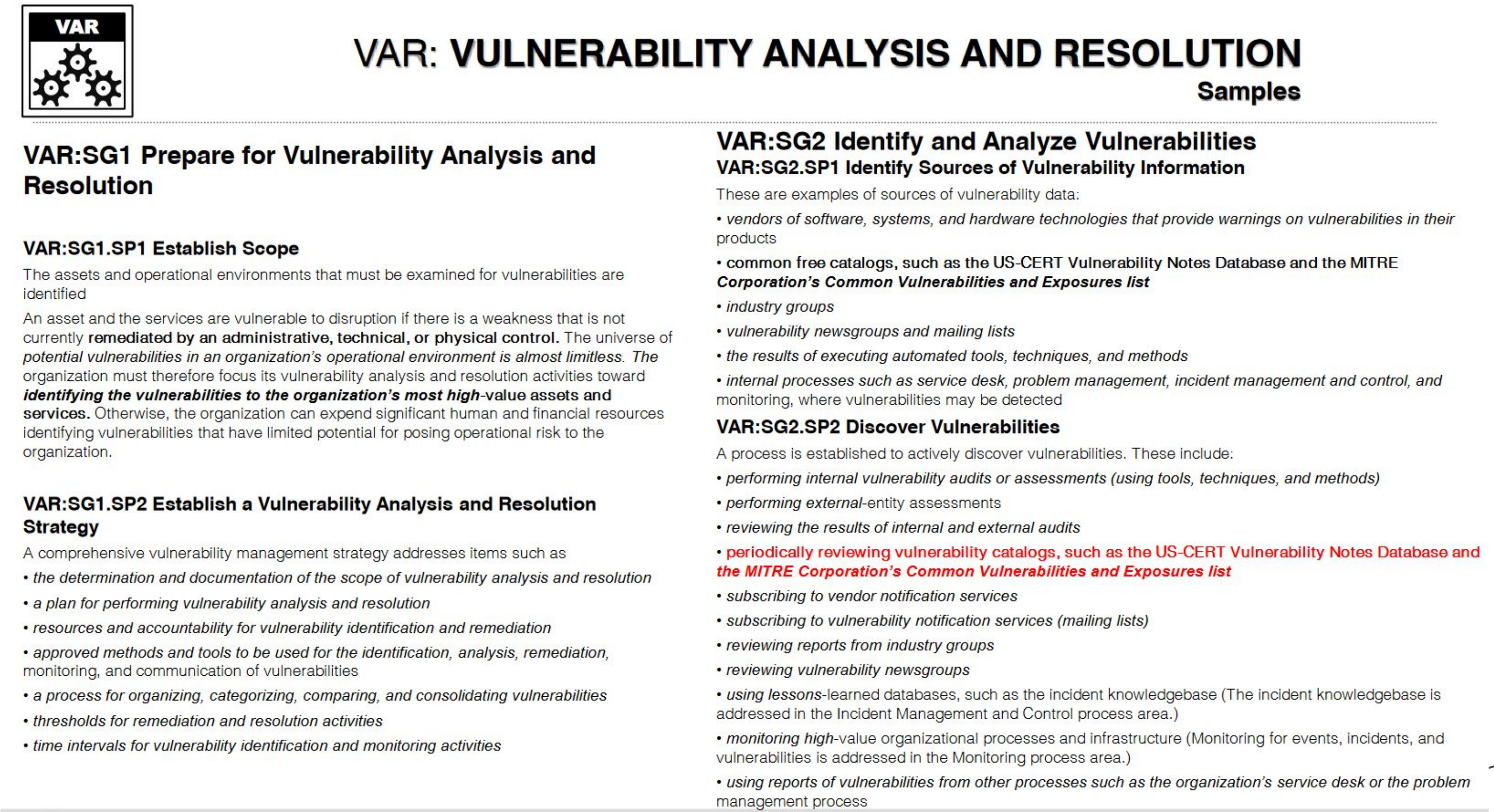
VAR:SG1 Prepare for Vulnerability Analysis and Resolution

VAR:SG2 Identify and Analyze Vulnerabilities

VAR:SG3 Manage Exposure to Vulnerabilities

VAR:SG4 Identify Root Causes

CERT-RMM накратко



VAR: VULNERABILITY ANALYSIS AND RESOLUTION

Samples

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

VAR:SG1.SP1 Establish Scope

The assets and operational environments that must be examined for vulnerabilities are identified

An asset and the services are vulnerable to disruption if there is a weakness that is not currently **remediated by an administrative, technical, or physical control.** The universe of *potential vulnerabilities in an organization's operational environment is almost limitless. The* organization must therefore focus its vulnerability analysis and resolution activities toward ***identifying the vulnerabilities to the organization's most high*-value assets and services.** Otherwise, the organization can expend significant human and financial resources identifying vulnerabilities that have limited potential for posing operational risk to the organization.

VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy

A comprehensive vulnerability management strategy addresses items such as

- *the determination and documentation of the scope of vulnerability analysis and resolution*
- *a plan for performing vulnerability analysis and resolution*
- *resources and accountability for vulnerability identification and remediation*
- *approved methods and tools to be used for the identification, analysis, remediation,* monitoring, and communication of vulnerabilities
- *a process for organizing, categorizing, comparing, and consolidating vulnerabilities*
- *thresholds for remediation and resolution activities*
- *time intervals for vulnerability identification and monitoring activities*

VAR:SG2 Identify and Analyze Vulnerabilities

VAR:SG2.SP1 Identify Sources of Vulnerability Information

These are examples of sources of vulnerability data:

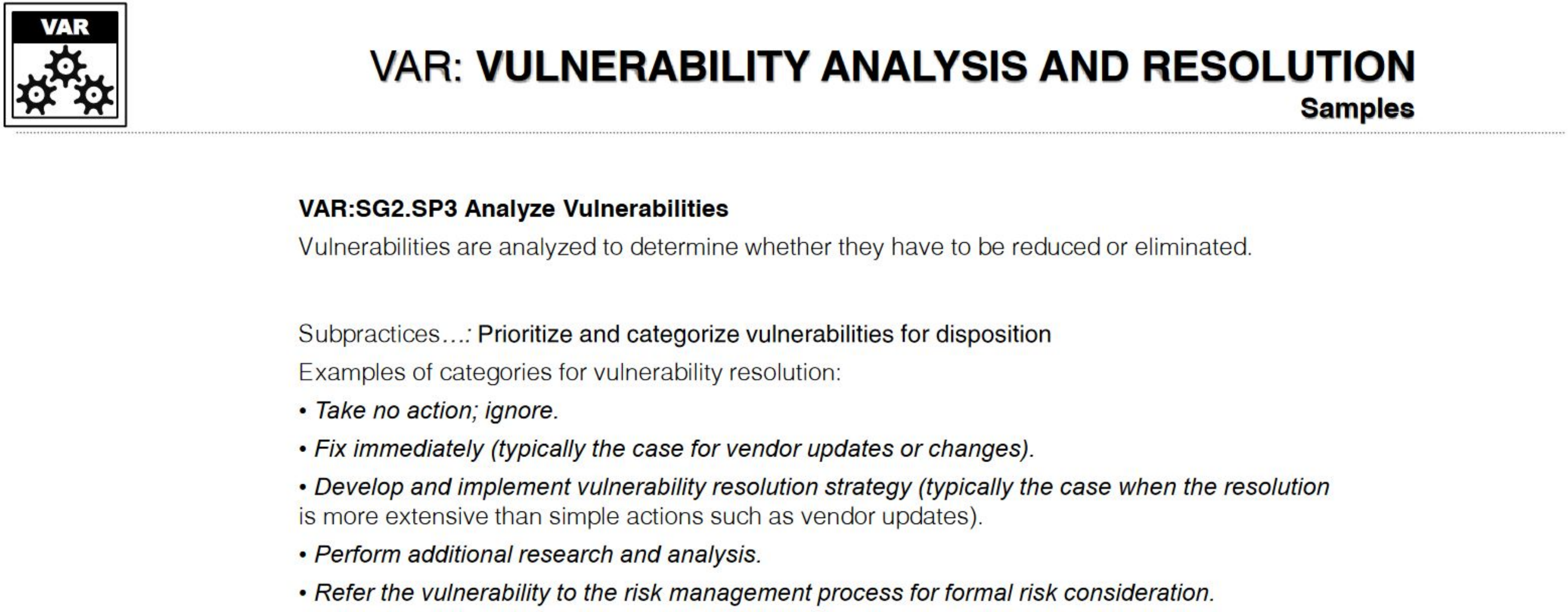
- *vendors of software, systems, and hardware technologies that provide warnings on vulnerabilities in their* products
- common free catalogs, such as the US-CERT Vulnerability Notes Database and the MITRE ***Corporation's Common Vulnerabilities and Exposures list***
- *industry groups*
- *vulnerability newsgroups and mailing lists*
- *the results of executing automated tools, techniques, and methods*
- *internal processes such as service desk, problem management, incident management and control, and* monitoring, where vulnerabilities may be detected

VAR:SG2.SP2 Discover Vulnerabilities

A process is established to actively discover vulnerabilities. These include:

- *performing internal vulnerability audits or assessments (using tools, techniques, and methods)*
- *performing external-*entity assessments
- *reviewing the results of internal and external audits*
- periodically reviewing vulnerability catalogs, such as the US-CERT Vulnerability Notes Database and ***the MITRE Corporation's Common Vulnerabilities and Exposures list***
- *subscribing to vendor notification services*
- *subscribing to vulnerability notification services (mailing lists)*
- *reviewing reports from industry groups*
- *reviewing vulnerability newsgroups*
- *using lessons-*learned databases, such as the incident knowledgebase (The incident knowledgebase is addressed in the Incident Management and Control process area.)
- *monitoring high-*value organizational processes and infrastructure (Monitoring for events, incidents, and vulnerabilities is addressed in the Monitoring process area.)
- *using reports of vulnerabilities from other processes such as the organization's service desk or the problem* management process

CERT-RMM накратко



VAR

VAR: **VULNERABILITY ANALYSIS AND RESOLUTION**

Samples

VAR:SG2.SP3 Analyze Vulnerabilities

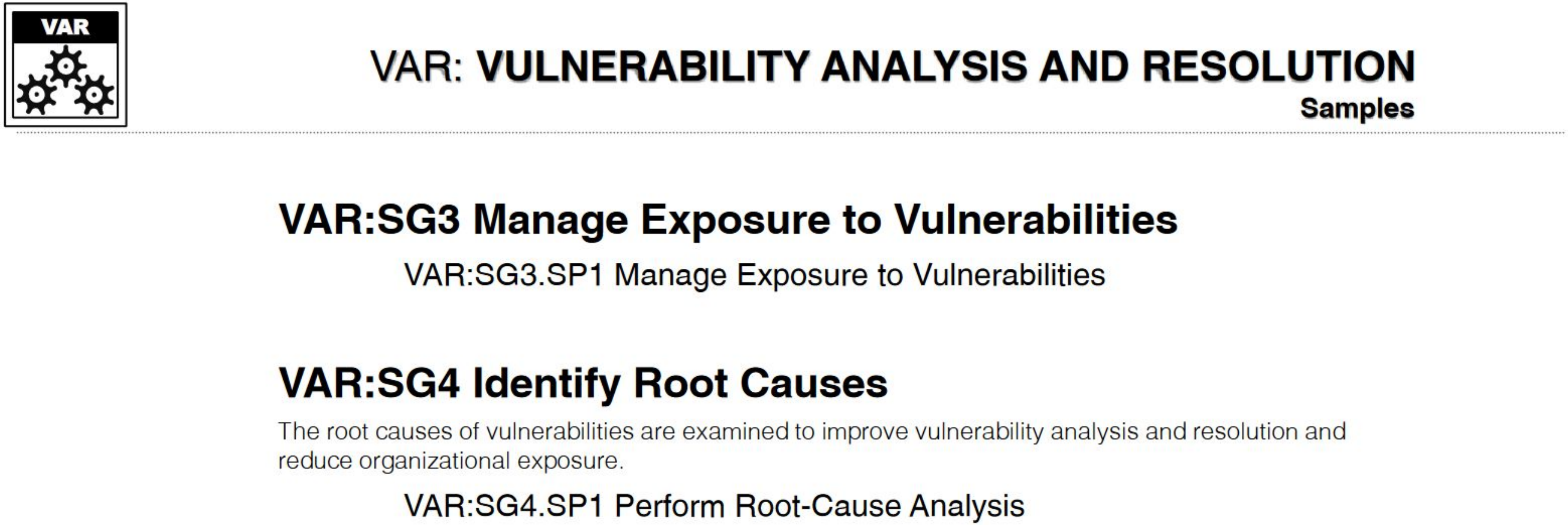
Vulnerabilities are analyzed to determine whether they have to be reduced or eliminated.

Subpractices…: Prioritize and categorize vulnerabilities for disposition

Examples of categories for vulnerability resolution:

- *Take no action; ignore.*
- *Fix immediately (typically the case for vendor updates or changes).*
- *Develop and implement vulnerability resolution strategy (typically the case when the resolution* is more extensive than simple actions such as vendor updates).
- *Perform additional research and analysis.*
- *Refer the vulnerability to the risk management process for formal risk consideration.*

CERT-RMM накратко



VAR: **VULNERABILITY ANALYSIS AND RESOLUTION**

Samples

VAR:SG3 Manage Exposure to Vulnerabilities

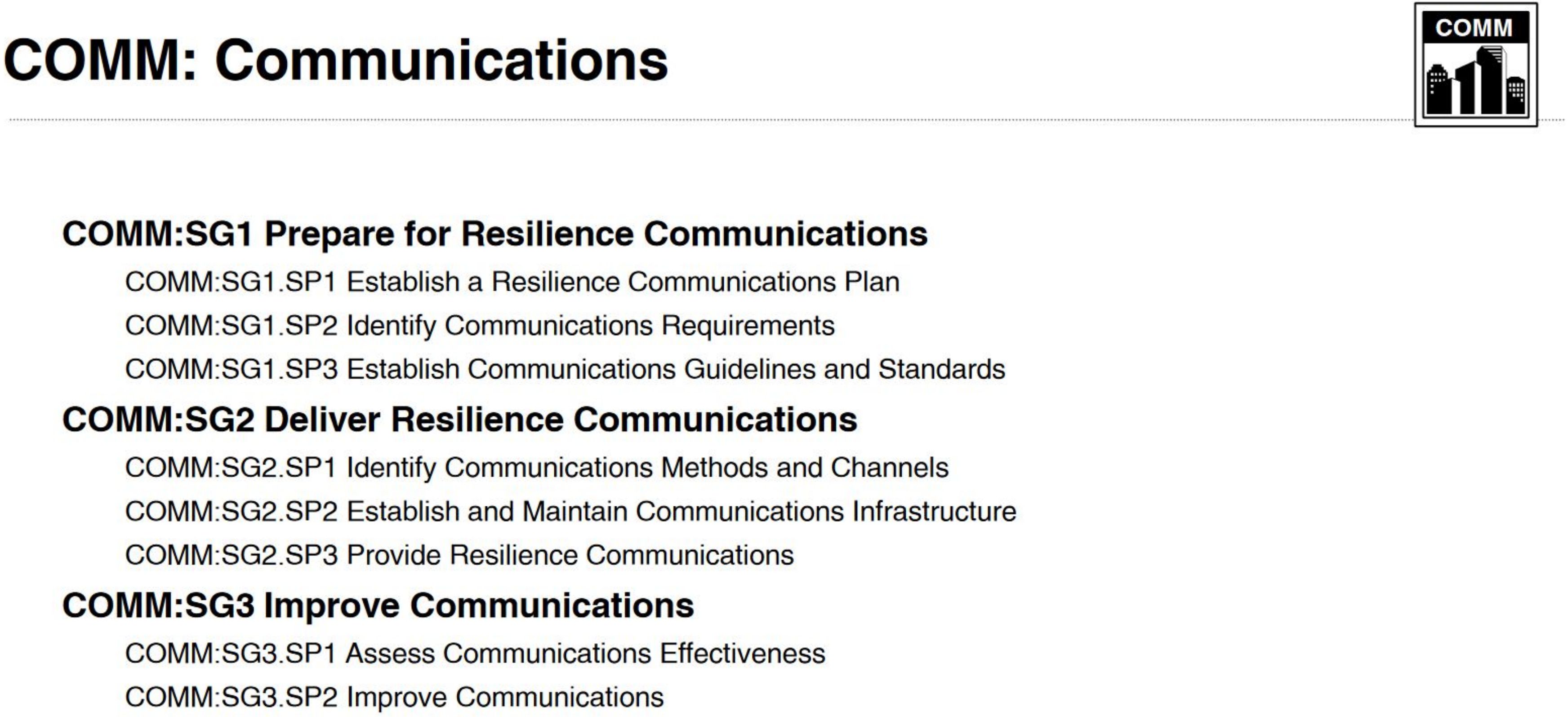
VAR:SG3.SP1 Manage Exposure to Vulnerabilities

VAR:SG4 Identify Root Causes

The root causes of vulnerabilities are examined to improve vulnerability analysis and resolution and reduce organizational exposure.

VAR:SG4.SP1 Perform Root-Cause Analysis

CERT-RMM накратко



COMM: Communications

COMM:SG1 Prepare for Resilience Communications

- COMM:SG1.SP1 Establish a Resilience Communications Plan
- COMM:SG1.SP2 Identify Communications Requirements
- COMM:SG1.SP3 Establish Communications Guidelines and Standards

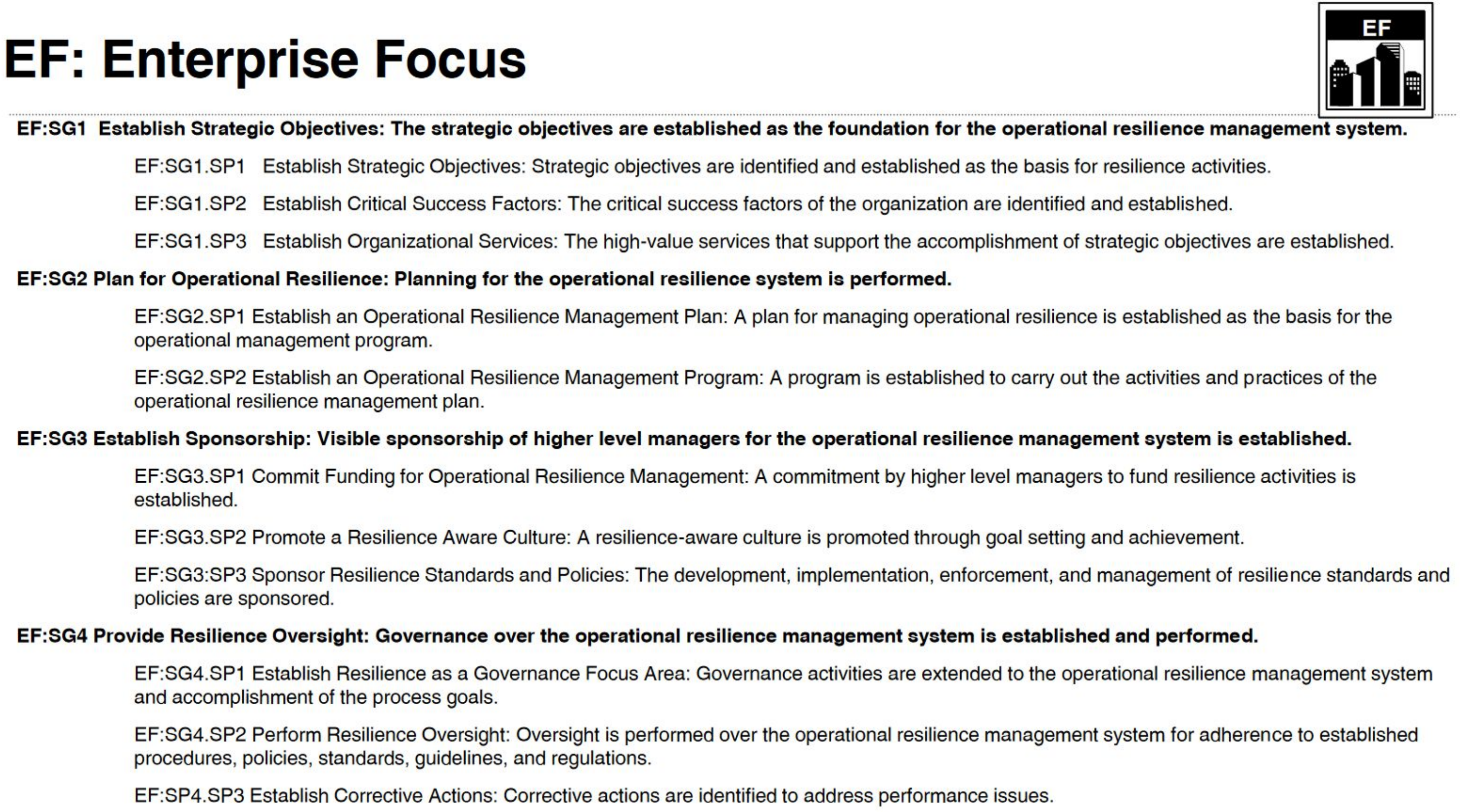
COMM:SG2 Deliver Resilience Communications

- COMM:SG2.SP1 Identify Communications Methods and Channels
- COMM:SG2.SP2 Establish and Maintain Communications Infrastructure
- COMM:SG2.SP3 Provide Resilience Communications

COMM:SG3 Improve Communications

- COMM:SG3.SP1 Assess Communications Effectiveness
- COMM:SG3.SP2 Improve Communications

CERT-RMM накратко



EF: Enterprise Focus

EF:SG1 Establish Strategic Objectives: The strategic objectives are established as the foundation for the operational resilience management system.

EF:SG1.SP1 Establish Strategic Objectives: Strategic objectives are identified and established as the basis for resilience activities.

EF:SG1.SP2 Establish Critical Success Factors: The critical success factors of the organization are identified and established.

EF:SG1.SP3 Establish Organizational Services: The high-value services that support the accomplishment of strategic objectives are established.

EF:SG2 Plan for Operational Resilience: Planning for the operational resilience system is performed.

EF:SG2.SP1 Establish an Operational Resilience Management Plan: A plan for managing operational resilience is established as the basis for the operational management program.

EF:SG2.SP2 Establish an Operational Resilience Management Program: A program is established to carry out the activities and practices of the operational resilience management plan.

EF:SG3 Establish Sponsorship: Visible sponsorship of higher level managers for the operational resilience management system is established.

EF:SG3.SP1 Commit Funding for Operational Resilience Management: A commitment by higher level managers to fund resilience activities is established.

EF:SG3.SP2 Promote a Resilience Aware Culture: A resilience-aware culture is promoted through goal setting and achievement.

EF:SG3:SP3 Sponsor Resilience Standards and Policies: The development, implementation, enforcement, and management of resilience standards and policies are sponsored.

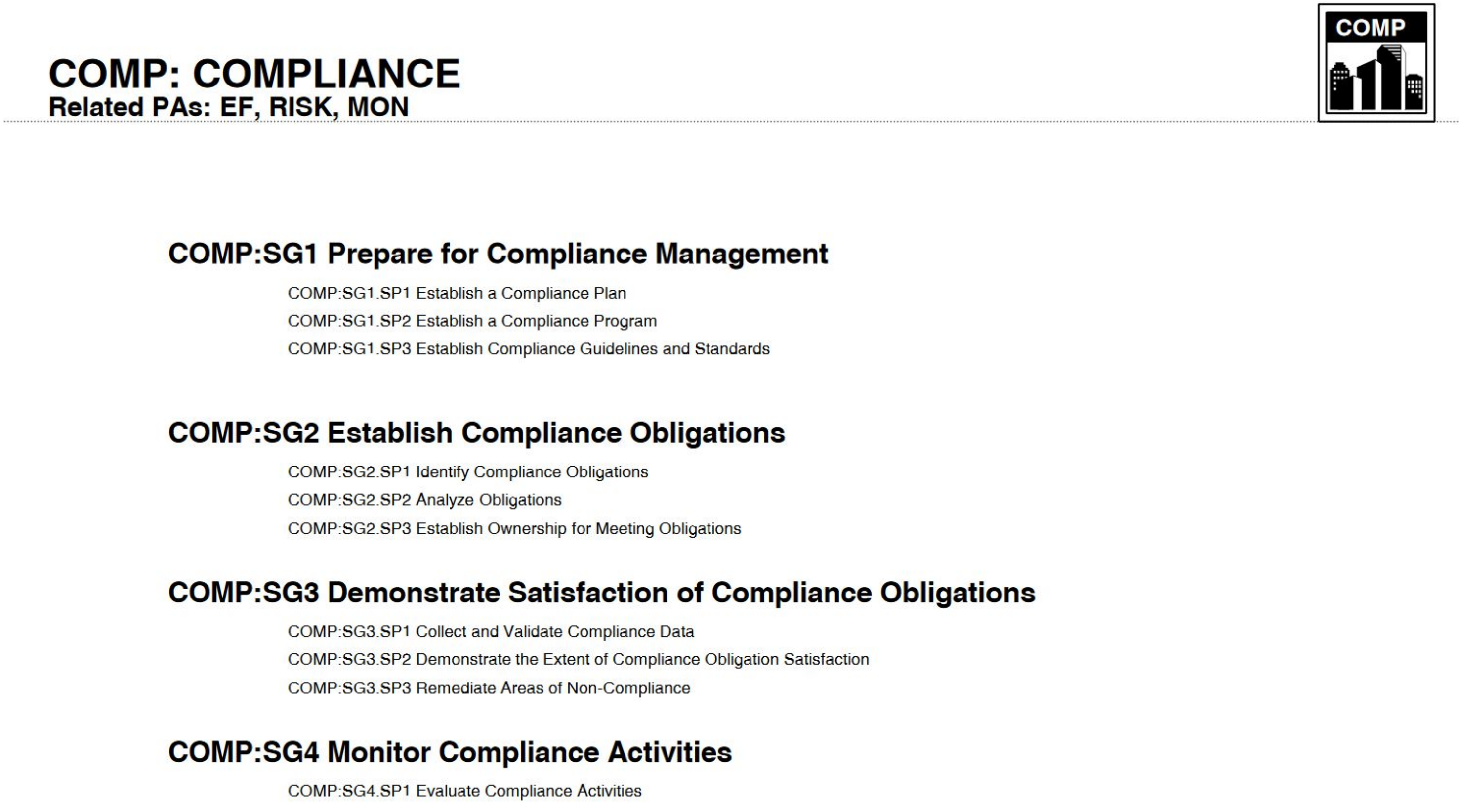
EF:SG4 Provide Resilience Oversight: Governance over the operational resilience management system is established and performed.

EF:SG4.SP1 Establish Resilience as a Governance Focus Area: Governance activities are extended to the operational resilience management system and accomplishment of the process goals.

EF:SG4.SP2 Perform Resilience Oversight: Oversight is performed over the operational resilience management system for adherence to established procedures, policies, standards, guidelines, and regulations.

EF:SP4.SP3 Establish Corrective Actions: Corrective actions are identified to address performance issues.

CERT-RMM накратко



COMP: COMPLIANCE

Related PAs: EF, RISK, MON

COMP

COMP:SG1 Prepare for Compliance Management

- COMP:SG1.SP1 Establish a Compliance Plan
- COMP:SG1.SP2 Establish a Compliance Program
- COMP:SG1.SP3 Establish Compliance Guidelines and Standards

COMP:SG2 Establish Compliance Obligations

- COMP:SG2.SP1 Identify Compliance Obligations
- COMP:SG2.SP2 Analyze Obligations
- COMP:SG2.SP3 Establish Ownership for Meeting Obligations

COMP:SG3 Demonstrate Satisfaction of Compliance Obligations

- COMP:SG3.SP1 Collect and Validate Compliance Data
- COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction
- COMP:SG3.SP3 Remediate Areas of Non-Compliance

COMP:SG4 Monitor Compliance Activities

- COMP:SG4.SP1 Evaluate Compliance Activities

Литература

- https://www.officesolutionsit.com.au/blog/cyber-security-policy-template
- https://resources.workable.com/cyber-security-policy
- https://purplesec.us/resources/cyber-security-policy-templates/
- https://www.sei.cmu.edu/about/divisions/cert/index.cfm
- https://cmu-sei.github.io/DevSecOps-Model/#Diagrams__4a8f7de3-a27e-4fc8-bcbc-4da182e93b48

Благодаря!

Въпроси?

mstoeva@uni-plovdiv.bg
http://edesign-bg.com