Software Engineering Institute

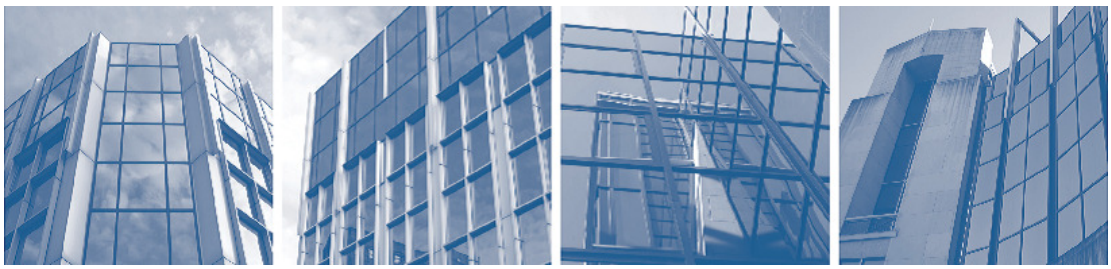
CERT® Resiliency Engineering Framework (REF) Outline

Preview version, v0.95R

Resiliency Engineering Framework Team
Resiliency Engineering and Management

November 2008

CERT Program



Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

CERT Resiliency Engineering Framework Outline

The purpose of this document is to provide a brief overview of the CERT Resiliency Engineering Framework (REF) by providing only the purpose statements, goals, and specific practices for each of the capability areas. The common goals and common practices are also provided at the end of the document, but are not reflected in the outline for each capability area.

For additional information and background on REF, the reader is referred to the Web at http://www.cert.org/resiliency_engineering. At that Web site, the full draft version of the framework is available, which includes detailed introductory material as well as explanatory material and subpractices for each of the capability areas.

ASSET DEFINITION AND MANAGEMENT

Engineering

Purpose

The purpose of Asset Definition and Management is to identify, document, and manage organizational assets during their lifecycle to ensure sustained productivity to support organizational services.

Concepts

Identify and establish asset types:

- People
- Information
- Technology
- Facilities

Asset owners

Asset custodians

Asset containers

Manage changes to assets

ADM-1 ESTABLISH ORGANIZATIONAL ASSETS

Organizational assets (people, information, technology, and facilities) are identified and the authority and responsibility for these assets is established.

ADM-1.1 Inventory Assets
Organizational assets are identified and inventoried.

ADM-1.2 Establish a Common Understanding
A common and consistent definition of assets is established and communicated.

ADM-1.3 Establish Ownership and Custodianship
The ownership and custodianship of assets is established.

ADM-2 ESTABLISH RELATIONSHIP BETWEEN ASSETS AND SERVICES

The relationship between assets and the services they support is established and examined.

ADM-2.1 Associate Assets with Services
Assets are associated with the service or services they support.

ADM-2.2 Analyze Asset-Service Dependencies
Instances where assets support more than one organizational service are identified and analyzed.

ADM-3 MANAGE ASSETS

The life cycle of assets is managed.

ADM-3.1 Identify Change Criteria
The criteria that would indicate changes in an asset or its association with a service are identified and established.

ADM-3.2 Maintain Changes to Assets and Inventory
Changes to assets are managed as conditions dictate.

ACCESS MANAGEMENT

Operations

Purpose

The purpose of Access Management is to ensure that access granted to organizational assets is commensurate with the asset's business and resiliency requirements.

Concepts

Control user environment

Access rights and privileges

Manage change to users and access rights

Connection to Identity Management

AM-1 MANAGE AND CONTROL ACCESS

Access granted to organizational assets is managed and controlled.

AM-1.1 Enable Access

Appropriate access to organizational assets is informed by resiliency requirements and owner approval.

AM-1.2 Manage Changes to Access Privileges

Manage changes to access privileges as assets, roles, and resiliency requirements change.

AM-1.3 Periodically Review and Maintain Access Privileges

Periodic review is performed to identify excessive or inappropriate levels of access privileges.

AM-1.4 Correct Inconsistencies

Excessive or inappropriate levels of access privileges are corrected.

COMMUNICATIONS

Enterprise

Purpose

The purpose of Communications is to develop, deploy, and manage internal and external communications to support resiliency activities and processes.

Concepts

Communications "stakeholders"

Communications methods, channels, and supporting infrastructure

Assess communications effectiveness

Improved future communications due to learning from events managed

COMM-1 ESTABLISH STANDARDS AND GUIDELINES FOR COMMUNICATIONS

The guidelines and standards for resiliency communications are established.

COMM-1.1 Identify Relevant Stakeholders
Internal and external stakeholders to whom the organization must communicate relative to resiliency activities are identified.

COMM-1.2 Identify Communications Requirements
The types and extent of communications needed by the organization to support stakeholders are identified.

COMM-1.3 Establish Communications Guidelines and Standards
The enterprise guidelines and standards for satisfying communications needs are established and maintained.

COMM-2 PREPARE FOR COMMUNICATIONS MANAGEMENT

The organizational process for developing, deploying, and managing resiliency communications is established.

COMM-2.1 Establish a Resiliency Communications Plan
Planning for the communications process is performed.

COMM-2.2 Establish a Resiliency Communications Program
A program for executing the communications management plan is established and maintained.

COMM-2.3 Identify and Assign Plan Personnel
Staff are assigned authority and accountability for carrying out the communications plan and program.

COMM-3 DELIVER RESILIENCY COMMUNICATIONS

The activities necessary to deliver communications for resiliency activities on an operational and event-driven basis are established.

COMM-3.1 Identify Communications Methods and Channels
Communications methods and channels relative to stakeholder and organizational needs are identified and established.

COMM-3.2 Establish and Maintain Communications Infrastructure
An infrastructure appropriate to meet the organization's resiliency communication needs is established and managed.

COMM-4 IMPROVE COMMUNICATIONS

Resiliency communications are reviewed to identify and implement improvements in the communications process.

COMM-4.1 Assess Communications Effectiveness

The effectiveness of communications plans and programs are assessed and corrective actions are identified.

COMM-4.2 Improve Communications

Lessons learned in managing communications are utilized to improve communications plans and programs.

COMPLIANCE

Enterprise

Purpose

The purpose of Compliance Management is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, and legislation related to managing operational resiliency.

Concepts

Compliance obligations for the organization come from many sources:

- Federal, state, and local government
- Foreign government and trade associations
- Industry associations and groups
- External codes of practice
- Internal policies, procedures, and guidelines
- Quality and process improvement certifications
- Agreements with suppliers, partners, and vendors

Improving the organizational capabilities in compliance management allows the organization to collect data once, comply many times. Documentation and analysis of all compliance obligations allows the organization to identify duplicate and conflicting requirements as well as obligations that do not have a cost/benefit to the organization to meet.

COMP-1 PREPARE FOR COMPLIANCE MANAGEMENT

The organizational environment and processes for identifying, satisfying, and monitoring compliance obligations are established.

COMP-1.1 Establish a Compliance Plan
A strategic plan for managing compliance to resiliency-related obligations is established.

COMP-1.2 Establish a Compliance Program
A program is established to carry out the activities and practices of the compliance plan.

COMP-1.3 Establish Resiliency Compliance Guidelines and Standards
The guidelines and standards for satisfying compliance obligations are established and communicated.

COMP-2 ESTABLISH COMPLIANCE OBLIGATIONS

The organization's compliance obligations are identified, documented, and communicated.

COMP-2.1 Identify Compliance Obligations
Compliance obligations are identified and documented.

COMP 2.2 Analyze Obligations
Compliance obligations are analyzed and organized to facilitate satisfaction.

COMP 2.3 Establish Ownership for Meeting Obligations
The responsibility for satisfying compliance obligations is established.

COMP-3 SATISFY COMPLIANCE OBLIGATIONS

The organization's compliance obligations are satisfied.

COMP-3.1 Collect and Validate Compliance Data

Data required to satisfy compliance obligations is collected and validated.

COMP-3.2 Satisfy Compliance Obligations

Compliance obligations are satisfied through compliance activities.

COMP-3.3 Remediate Areas of Non-Compliance

Remediation of areas of non-compliance is performed to ensure satisfaction of compliance obligations.

COMP-4 MONITOR COMPLIANCE ACTIVITIES

The organization's satisfaction of compliance obligations is monitored and adjusted as necessary.

COMP-4.1 Evaluate Compliance Activities

Satisfaction of the organization's compliance obligations is independently monitored and improved.

ENVIRONMENTAL CONTROL

Operations

Purpose

The purpose of Environmental Control is to establish and manage an appropriate level of physical, environmental, and geographical controls to support the resilient operations of services in organizational facilities.

Concepts

Assess risks to facility assets

Control operational and geographical environment

Manage public/private partner dependencies

Retire or vacate facility

EC-1 ESTABLISH AND PRIORITIZE FACILITY ASSETS

Facility assets are prioritized to ensure resiliency of key services that they support.

EC-1.1 Prioritize Facility Assets
Facility assets are prioritized relative to their importance in supporting the delivery of key services.

EC-1.2 Establish Resiliency-Focused Facility Assets
Facility assets that specifically support the organization's service continuity plans are identified and established.

EC-2 PROTECT FACILITY ASSETS

Administrative, technical, and physical controls for information assets are identified, implemented, monitored, and managed.

EC-2.1 Assign Resiliency Requirements to Facility Assets
Resiliency requirements that have been defined are assigned to facility assets.

EC-2.2 Establish and implement Controls
Administrative, technical, and physical controls that are required to meet the established resiliency requirements are identified and implemented

EC-3 MANAGE FACILITY ASSET RISK

Operational and environmental risks to facility assets are identified and managed.

EC-3.1 Identify and Assess Facility Asset Risk
Risks to facility assets are periodically identified and assessed.

EC-3.2 Mitigate Facility Risks
Risk mitigation strategies for facility assets are developed and implemented.

EC-4 CONTROL OPERATIONAL ENVIRONMENT

The operational environment of the facility is controlled to ensure its availability.

EC-4.1 Perform Facility Sustainability Planning
The availability of key facilities is ensured through sustainability planning.

EC-4.2 Maintain Environmental Conditions
Environmental conditions of the facility asset are maintained.

EC-4.3 Manage Dependencies on Public Services
Dependencies on public services for the facility asset are identified and managed.

EC-4.4 Manage Dependencies on Public Infrastructure
Dependencies on public infrastructure for the facility asset are identified and managed.

EC-4.5 Plan for Facility Retirement
The retirement of a facility is planned for to minimize operational impact.

ENTERPRISE FOCUS

Enterprise

Purpose

The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the resiliency engineering process.

Concepts

Strategic drivers

Critical success factors

Integrating resiliency and risk awareness into the culture

Senior management sponsorship of resiliency

Developing an overall strategy for resiliency that supports the organization's operational risk management strategy

Oversight and governance of the resiliency plan and program

EF-1 ESTABLISH STRATEGIC OBJECTIVES

The strategic objectives of the organization are established as the foundation for the resiliency engineering process.

EF-1.1 Establish Strategic Objectives
Strategic objectives are identified and established as the basis for resiliency activities.

EF-1.2 Establish Critical Success Factors
The critical success factors of the organization are identified and established.

EF-1.3 Establish Organizational Services
The key services that support the accomplishment of strategic objectives are established.

EF-2 STRATEGIC RESILIENCY PLANNING

Strategic planning for the resiliency engineering process is performed.

EF-2.1 Establish a Strategic Resiliency Plan
A strategic plan for managing operational resiliency is established as the basis for the resiliency engineering process.

EF-2.2 Establish a Resiliency Engineering Program
A program is established to carry out the activities and practices of the strategic resiliency plan.

EF-3 ESTABLISH SPONSORSHIP

Visible executive sponsorship for the resiliency engineering process is established.

EF-3.1 Commit Funding for Resiliency Engineering
A commitment to funding resiliency activities is established at the executive level.

EF-3.2 Promote a Resiliency-Aware Culture
A resiliency-aware culture is promoted through goal setting and achievement.

EF-3.3 Sponsor Resiliency Standards and Policies
The development, implementation, enforcement, and management of resiliency

EF-4 PROVIDE RESILIENCY OVERSIGHT

Governance over the resiliency engineering process is established and performed.

EF-4.1 Establish Resiliency as a Governance Focus Area

Governance activities are extended to the resiliency engineering process and accomplishment of the process goals.

EF-4.2 Perform Resiliency Oversight

Oversight is performed over the resiliency engineering process for adherence to established procedures, policies, standards, guidelines, and regulations.

EF-4.3 Establish Corrective Actions

Corrective actions are identified to address performance issues.

EXTERNAL DEPENDENCIES

Operations

Purpose

The purpose of External Dependencies is to ensure that appropriate resiliency measures are in place to protect and sustain services and assets that are dependent on the actions of external parties.

Concepts

Resiliency value chain

Supplier resiliency

EXD-1 IDENTIFY EXTERNAL DEPENDENCIES

External parties that access, provide, or manage critical services or assets are identified and characterized, and updated as needed.

EXD-1.1 Identify and Characterize External Dependencies
Establish and maintain a characterized list of external parties on which the organization depends for critical services or assets.

EXD-2 MANAGE RISKS DUE TO EXTERNAL DEPENDENCIES

Risks due to external dependencies are identified and managed.

EXD-2.1 Identify And Assess Risks Due To External Dependencies
Risks associated with critical external parties are periodically identified and assessed.

EXD-2.2 Mitigate Risks Due To External Dependencies
Risk mitigation strategies for external dependencies are developed and implemented.

EXD-3 ESTABLISH FORMAL RELATIONSHIPS

The organization's essential activities for managing and sustaining operational resiliency are funded.

EXD-3.1 Establish Enterprise Requirements For External Dependencies
Enterprise requirements that apply to all critical external parties are established and maintained.

EXD-3.2 Establish Resiliency Requirements For External Dependencies
Resiliency requirements for each critical external party are established and maintained.

EXD-3.3 Evaluate And Select External Parties
External parties are selected based on an evaluation of their ability to meet the specified requirements.

EXD-3.4 Formalize Relationships
Establish and maintain formal agreements with external parties.

EXD-4 MANAGE EXTERNAL PARTY PERFORMANCE

The performance of critical external parties is monitored and corrective actions are taken as necessary.

EXD-4.1 Continuously Monitor External Party Performance
The performance of critical external parties is monitored against the requirements.

EXD-4.2 Correct External Party Performance
Corrective actions are implemented to support external party performance as necessary.

FINANCIAL RESOURCE MANAGEMENT

Enterprise

Purpose

The purpose of Financial Resource Management is to request, receive, manage, and apply financial resources to support resiliency objectives and requirements.

Concepts

Resiliency budgets and accounting

Report the true cost of resiliency (COR) & controls

Return on resiliency investment (RORI)

FRM-1 ESTABLISH FINANCIAL COMMITMENT

A commitment to funding resiliency activities is established.

FRM-1.1 Commit Funding for Resiliency Engineering
A commitment to funding resiliency activities is established at the executive level.

FRM-1.2 Establish Structure to Support Financial Management
The structure that supports the assignment and management of financial resources to resiliency activities is established.

FRM-2 PERFORM FINANCIAL PLANNING

Planning for funding resiliency management activities is performed.

FRM-2.1 Define Funding Needs
The financial obligations for managing the resiliency engineering process are established.

FRM-2.2 Establish Resiliency Budgets
Capital and expense budgets for resiliency management are established.

FRM-2.3 Resolve Funding Gaps
Identify and resolve gaps in funding for resiliency management and mitigate associated risks.

FRM-3 FUND RESILIENCY ACTIVITIES

The organization's essential activities for managing and sustaining operational resiliency are funded.

FRM-3.1 Fund Resiliency Activities
Access to funds for resiliency management activities is provided.

FRM-4 ACCOUNT FOR RESILIENCY ACTIVITIES

Accounting for the financial commitment to resiliency activities is performed and used for process improvement.

FRM-4.1 Track and Document Costs
The costs associated with resiliency management are tracked and documented.

FRM-4.2 Perform Cost and Performance Analysis
Cost and performance analysis for funded resiliency management activities is performed.

FRM-5 OPTIMIZE RESILIENCY EXPENDITURES AND INVESTMENTS

The return to the organization for investment in resiliency activities is measured and assessed.

FRM-5.1 Optimize Resiliency Expenditures

Optimize the expenditures related to implementing and managing protection and sustainability strategies against the benefits derived from these actions.

FRM-5.2 Determine Return on Resiliency Investments

Calculate a return on resiliency investments where possible.

FRM-5.3 Identify Cost Recovery Opportunities

Opportunities for the organization to recover costs and investments in resiliency management activities are identified.

HUMAN RESOURCES MANAGEMENT

Enterprise

Purpose

The purpose of Human Resources Management is to manage the employment life cycle and performance of staff in a manner that contributes to the organization's ability to manage operational resiliency.

Concepts

Baseline competencies and skills inventory

Determine suitability of candidates for resiliency positions

Resiliency as a job responsibility

Disciplinary process for policy violation

Voluntary and involuntary separation including exit interviews, executed confidentiality agreements, sustainability of roles

HRM-1 ESTABLISH RESOURCE NEEDS

The resource needs to staff the activities and tasks of the organization's resiliency program and plan are identified and satisfied.

HRM-1.1 Establish Baseline Competencies
The staffing and skill needs relative to the resiliency engineering process are established.

HRM-1.2 Inventory Skills and Identify Gaps
The current skill set for resiliency engineering is inventoried and gaps in necessary skills are identified.

HRM-1.3 Address Skill Deficiencies
Gaps in skills necessary to meet resiliency engineering needs are addressed.

HRM-2 MANAGE STAFF ACQUISITION

The acquisition of staff to meet operational needs is performed with consideration of the organization's resiliency objectives.

HRM-2.1 Verify Suitability of Candidate Personnel
Candidate personnel are evaluated for suitability against position requirements and risks.

HRM-2.2 Establish Terms and Conditions of Employment
Employment agreements appropriate for the position and role are developed and executed.

HRM-3 MANAGE STAFF PERFORMANCE

The performance of staff to support the organization's resiliency program is managed.

HRM-3.1 Establish Resiliency as a Job Responsibility
Resiliency obligations for staff are communicated, agreed to, and documented as conditions of employment.

HRM-3.2 Establish Resiliency Performance Goals and Objectives
Goals and objectives for supporting the organization's resiliency program are established as part of the performance management process.

HRM-3.3 Measure and Assess Performance
Performance against goals and objectives is measured, achievements are acknowledged, and corrective actions are identified and communicated.

HRM-3.4 Establish Disciplinary Process

A disciplinary process is established for personnel who violate resiliency policies.

HRM-4 MANAGE CHANGES TO EMPLOYMENT STATUS

Changes in the employment status of personnel in the organization are managed.

HRM-4.1 Manage Impact of Position Changes

Administrative controls are established to sustain functions, obligations, and critical roles upon position changes or terminations.

HRM-4.2 Manage Access to Assets

Access to and possession of organizational assets relative to position changes is managed.

HRM-4.3 Manage Involuntary Terminations

Administrative controls and procedures are established to manage the effects of involuntary terminations.

IDENTITY MANAGEMENT

Operations

Purpose

The purpose of Identity Management is to create, maintain, and deactivate identities and associated attributes that are provided access to organizational assets.

Concepts

Identify life cycle – typically people but can be systems, devices, or other processes

Establish identities

Profile the objects or users by roles, responsibilities, level of trusted access

Connect to Access Management

ID-1 ESTABLISH IDENTITIES

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

ID-1.1 Create Identities
Persons, objects, and entities that require access to organizational assets are registered and profiled.

ID-1.2 Establish Identity Repository
The identity community is established and documented.

ID-1.3 Assign Roles to Identities
Organizational roles are established and associated with identities.

ID-2 MANAGE IDENTITIES

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

ID-2.1 Monitor and Manage Identity Changes
Changes to identities are monitored for and managed.

ID-2.2 Periodically Review and Maintain Identities
Periodic review is performed to identify identities that are invalid.

ID-2.3 Correct Inconsistencies
Inconsistencies between the identity community and the persons, objects, and entities they represent are corrected.

ID-2.4 Deprovision Identities
Deprovision identities where need has expired or has been eliminated.

INCIDENT MANAGEMENT AND CONTROL

Operations

Purpose

The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and to determine an appropriate organizational response.

Concepts

Events, incidents, and crises

Incident life-cycle

- event detection
- analysis
- response

IMC-1 ESTABLISH INCIDENT MANAGEMENT AND CONTROL PROCESS

The organizational process for identifying, analyzing, responding to, and learning from incidents is established.

IMC-1.1 Plan for Incident Management
Planning is performed for developing and implementing the organization's incident management and control processes.

IMC-1.2 Resource Incident Management Plan
Resources are identified and assigned to the incident management plan.

IMC-2 DETECT EVENTS

Establish and maintain a process for detecting and reporting events.

IMC-2.1 Detect and Report Events
Events are detected and reported.

IMC-2.2 Log and Track Events
Events are logged and tracked from inception to disposition.

IMC-2.3 Collect, Document, and Preserve Event Evidence
The process for collecting, documenting, and preserving event evidence is established and managed.

IMC-2.4 Define and Maintain Incident Validation Criteria
Criteria for declaring incidents is defined and maintained.

IMC-3 ANALYZE EVENTS

Events are analyzed to support incident declaration and response planning.

IMC-3.1 Triage Events
Events are triaged to support incident analysis and response.

IMC-3.2 Analyze Events
Analyze events to understand underlying causes and to support the development of an appropriate incident response.

IMC-4 RESPOND TO AND RECOVER FROM INCIDENTS

The process for responding to and recovering from incidents is established.

IMC-4.1 Escalate Incidents

Incidents are escalated to the appropriate stakeholders for input and resolution.

IMC-4.2 Develop Incident Response

A response to an incident is developed and implemented to prevent or limit organizational impact.

IMC-4.3 Communicate Incidents

A plan for the communication of incidents to relevant stakeholders and a process for managing on-going incident communications is established.

IMC-4.4 Close Incidents

Incidents are closed after relevant actions have been taken by the organization.

IMC-5 ESTABLISH INCIDENT LEARNING

Lessons learned from identifying, analyzing, and responding to incidents are translated into actions to improve service and asset protection and sustainability.

IMC-5.1 Perform Post-Incident Review

Post-incident review is performed to determine underlying causes.

IMC-5.2 Integrate with Problem Management Process

A link between incident handling and the organization's problem management process is established.

IMC-5.3 Translate Experience to Strategy

The lessons learned from incident management are analyzed and translated into service and asset protection and continuity strategies.

KNOWLEDGE AND INFORMATION MANAGEMENT

Operations

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.

Concepts

Identify risks to information assets

Classify information assets

Apply security controls to meet security requirements

Information asset disposition guidelines

Knowledge management

Information retention and duplication

KIM-1 ESTABLISH AND PRIORITIZE INFORMATION ASSETS

Information assets are prioritized to ensure resiliency of key services in which they are used.

KIM-1.1 Prioritize Information Assets
Information assets are prioritized relative to their importance in supporting the delivery of key services.

KIM-1.2 Categorize and Classify Information Assets
Information assets that support key services are categorized and classified as to their organizational sensitivity.

KIM-2 PROTECT INFORMATION ASSETS

Administrative, technical, and physical controls for information assets are identified, implemented, monitored, and managed.

KIM-2.1 Assign Resiliency Requirements to Information Assets
Resiliency requirements that have been defined are assigned to information assets.

KIM-2.2 Establish and Implement Controls
Administrative, technical, and physical controls that are required to meet the established resiliency requirements are identified and implemented.

KIM-3 MANAGE INFORMATION ASSET RISK

Operational risks to information assets are identified and managed.

KIM-3.1 Identify and Assess Information Asset Risk
Risks to information assets are periodically identified and assessed.

KIM-3.2 Mitigate Information Asset Risk
Risk mitigation strategies for information assets are developed and implemented.

KIM-4 MANAGE INFORMATION ASSET CONFIDENTIALITY AND PRIVACY

The confidentiality and privacy considerations of information assets are managed.

KIM-4.1 Encrypt Critical Information
Cryptographic controls are applied to information assets to ensure confidentiality and prevent accidental disclosure.

KIM-4.2 Control Access to Information Assets
Access controls are developed and implemented to limit access to information assets.

KIM-4.3 Control Information Asset Disposition
The means for disposing of information assets is controlled.

KIM-5 MANAGE INFORMATION ASSET INTEGRITY

The availability of information assets to support key services is managed.

KIM-5.1 Control Modification to Information Assets
The modification of information assets is controlled.

KIM-5.2 Manage Information Asset Configuration
Information asset baselines are created and changes are managed.

KIM-5.3 Verify Validity of Information
Controls are implemented to sustain the validity and reliability of information assets.

KIM-6 MANAGE INFORMATION ASSET AVAILABILITY

The availability of information assets to support key services is managed.

KIM-6.1 Perform Information Duplication and Retention
Key information assets are backed-up and retained to support services when needed.

KIM-6.2 Manage Organizational Knowledge
The organizational and intellectual knowledge of staff is identified and documented.

MEASUREMENT AND ANALYSIS

Process Management

Purpose

The purpose of Measurement and Analysis is to develop and sustain a measurement capability that is used to support management information needs for managing the resiliency engineering process.

Concepts

Objectives for measurement

Collect, store, analyze, and report data

MA-1 ALIGN MEASUREMENT AND ANALYSIS ACTIVITIES

Measurement objectives and activities are aligned with identified information needs and objectives.

MA-1.1 Establish Measurement Objectives
Measurement objectives are established and maintained based on information needs and objectives.

MA-1.2 Specify Measures
The measures necessary to meet measurement objectives are established.

MA-1.3 Specify Data Collection and Storage Procedures
The techniques for collecting and storing measurement data are specified.

MA-1.4 Specify Analysis Procedures
The techniques for analysis and reporting are specified.

MA-2 PROVIDE MEASUREMENT RESULTS

Measurement results, which address identified information needs and objectives, are provided.

MA-2.1 Collect Measurement Data
Measurement data is collected consistent with measurement objectives.

MA-2.2 Analyze Measurement Data
Measurement data are analyzed against measurement objectives.

MA-2.3 Store Data and Results
Measurement data, analysis, and results are stored.

MA-2.4 Communicate Results
The results of measurement and analysis activities are communicated to relevant stakeholders.

MONITORING

Process Management

Purpose

The purpose of Monitoring is to collect, record, and distribute information about the resiliency engineering process to the organization on a timely basis.

Concepts

Stakeholders of monitoring process

Monitoring requirements (compliance)

Monitoring infrastructure

MON-1 ESTABLISH AND MAINTAIN A MONITORING PROGRAM

Establish and maintain a program for identifying, recording, collecting, and reporting important resiliency information.

MON-1.1 Establish Monitoring Program
Establish and maintain the program for identifying, collecting, and disseminating monitoring information.

MON-1.2 Identify Stakeholders
The organizational and external entities that rely upon information collected from the monitoring process are identified.

MON-1.3 Establish Monitoring Requirements
The requirements for monitoring resiliency engineering processes are established.

MON-1.4 Analyze and Prioritize Monitoring Requirements
Monitoring requirements are analyzed and prioritized to ensure they can be satisfied.

MON-2 PERFORM MONITORING

The monitoring process is performed throughout the enterprise.

MON-2.1 Establish and Maintain Monitoring Infrastructure
A monitoring infrastructure commensurate with meeting monitoring requirements is established and maintained.

MON-2.2 Establish Collection Standards and Parameters
The standards and parameters for collecting information and managing data are established.

MON-2.3 Collect and Record Information
Information relevant to the resiliency engineering process is collected and recorded.

MON-2.4 Distribute Information
Collected and recorded information is disseminated to appropriate stakeholders.

ORGANIZATIONAL TRAINING AND AWARENESS

Enterprise

Purpose

The purpose of Organizational Training and Awareness is to promote awareness and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resiliency.

Concepts

Conduct awareness campaign

Train for resiliency skill development

Identify competencies for which tactical training is needed to support operational resiliency

"Inculcation" and "acculturation" of risk awareness

Assess effectiveness of training

OTA-1 ESTABLISH AWARENESS PROGRAM

An awareness program that supports the organization's resiliency program is established.

OTA-1.1 Establish Awareness Needs
The awareness needs of the organization are established and maintained.

OTA-1.2 Establish Awareness Training Plan
A plan for developing, implementing, and maintaining an awareness training program is established and maintained.

OTA-1.3 Establish Awareness Training Capability
A capability for consistent and repeatable delivery of awareness training is established and maintained.

OTA-2 CONDUCT AWARENESS ACTIVITIES

Awareness activities that support the organization's resiliency program are performed.

OTA-2.1 Perform Awareness Activities
Awareness activities are performed according to the awareness plan.

OTA-2.2 Establish Awareness Records
Records of awareness activities performed are established and maintained.

OTA-2.3 Assess Awareness Activity Effectiveness
The effectiveness of the awareness program is assessed and corrective actions are identified.

OTA-3 ESTABLISH RESILIENCY TRAINING CAPABILITY

Training capabilities that support the resiliency engineering process are established and maintained.

OTA-3.1 Establish Resiliency Training Needs
The training needs of the organization are established and maintained.

OTA-3.2 Establish Resiliency Training Plan
A plan for developing, implementing, and maintaining a resiliency training program is established and maintained.

OTA-3.3 Establish Resiliency Training Capability
A capability for delivering training to resiliency-focused personnel is established and maintained.

OTA-4 CONDUCT RESILIENCY TRAINING

Training necessary for staff to perform their roles effectively is provided.

OTA-4.1 Deliver Resiliency Training

Training is delivered according to the training plan.

OTA-4.2 Establish Resiliency Training Records

Records of delivered training are established and maintained.

OTA-4.3 Assess Resiliency Training Effectiveness

The effectiveness of the training program is assessed and corrective actions are identified.

PEOPLE MANAGEMENT

Operations

Purpose

The purpose of People Management is to establish and manage the contributions and availability of [the] people [asset] to support the resilient operation of organizational services.

Concepts

The role of people in supporting the operation of the business

Identify key personnel

Assess risks to the availability of people

Availability consideration of replacement people

Return-to-work considerations in the event of realized risk

PM-1 ESTABLISH KEY PERSONNEL

The key personnel of the organization are identified and prioritized.

PM-1.1 Identify Key Personnel
The key personnel from a resiliency perspective are identified and characterized.

PM-2 MANAGE RISKS ASSOCIATED WITH PERSONNEL AVAILABILITY

Operational risks related to the availability of personnel are identified and managed.

PM-2.1 Identify and Assess Personnel Risk
Risks to the availability of personnel are periodically identified and assessed.

PM-2.2 Mitigate Personnel Risk
Mitigation strategies for the risks related to the availability of personnel are developed and implemented.

PM-3 MANAGE THE AVAILABILITY OF PERSONNEL

The availability of personnel to support key services is managed.

PM-3.1 Establish Redundancy for Key Personnel
Redundancy for key personnel is established to ensure continuity of services.

PM-3.2 Perform Succession Planning
Key personnel roles and responsibilities are supported through succession planning.

PM-3.3 Prepare for Redeployment
Establish plans and prepare personnel for redeployment to other roles during a disruptive event or in the execution of a continuity of operations plan.

PM-3.4 Plan to Support Personnel During Disruptive Event
Plans are developed and implemented to ensure support is provided for personnel as they are deployed during a disruptive event.

PM-3.5 Plan for Return-to-Work Considerations
Plans are developed and implemented to address return-to-work issues for personnel after a disruptive event.

RISK MANAGEMENT

Enterprise

Purpose

The purpose of Risk Management is to identify, analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services.

Concepts

Develop and document an operational risk management strategy

Set risk measurement criteria and communicating risk assumptions

Determine risk appetite and risk tolerance

Identify asset-level and service-level risks

Utilize risk information to review and adjust protection and sustainability strategies

RISK-1 PREPARE FOR RISK MANAGEMENT

Preparation for risk management is performed.

RISK-1.1 Determine Risk Sources and Categories
The sources of risk to assets and services are identified and the categories of risk that are relevant to the organization are determined.

RISK-1.2 Establish An Operational Risk Management Strategy
A strategy for managing operational risk relative to strategic objectives is established and maintained.

RISK-2 ESTABLISH RISK PARAMETERS AND FOCUS

Risk tolerances are identified and documented and the focus of risk management activities is established.

RISK-2.1 Define Risk Parameters
The organization's risk parameters are defined.

RISK-2.2 Establish Risk Measurement Criteria
Criteria for measuring the organizational impact of realized risk are established.

RISK-3 IDENTIFY RISK

Operational risks are identified.

RISK-3.1 Identify Asset-level Risks
Operational risks that affect assets that support services are identified.

RISK-3.2 Identify Service-level Risks
Operational risks that potentially affect services as a result of asset risk are identified.

RISK-4 ANALYZE RISK

Operational risks are analyzed to determine priority and importance.

RISK-4.1 Evaluate Risk
Risks are evaluated against risk tolerances and criteria, and the potential impact of risk is characterized.

RISK-4.2 Categorize and Prioritize Risk
Risks are categorized and prioritized relative to risk parameters and risks that need to be mitigated are identified.

RISK-4.3 Assign Risk Disposition
The disposition of each identified risk is documented and approved.

RISK-5 MITIGATE AND CONTROL RISK
Risks to assets and services are mitigated and controlled to prevent disruption of operational resiliency.

RISK-5.1 Develop Risk Mitigation Plans
Risk mitigation plans are developed.

RISK-5.2 Implement Risk Strategies
Risk strategies and mitigation plans are implemented and monitored.

RISK-6 UTILIZE RISK INFORMATION TO MANAGE RESILIENCY
Information gathered from identifying, analyzing, and mitigating risk is used to improve the resiliency engineering process.

RISK-6.1 Review and Adjust Protection Strategies
Controls implemented to protect assets and services from risk are evaluated and updated as required based on risk information.

RISK-6.2 Review and Adjust Sustainability Strategies
Service continuity plans are developed to ensure sustainability of services are evaluated and updated as required based on risk information.

RESILIENCY REQUIREMENTS DEVELOPMENT

Engineering

Purpose

The purpose of Resiliency Requirements Development is to identify, document, and analyze the operational resiliency requirements for services and related assets.

Concepts

Owners of assets determine resiliency and security requirements

Requirements are derived from organizational requirements

Validate requirements commensurate with the value of the asset

Identify and resolve conflicting requirements

RRD-1 IDENTIFY ENTERPRISE REQUIREMENTS

The organization's enterprise-level resiliency requirements are identified and established.

RRD-1.1 Establish Enterprise Resiliency Requirements
The resiliency requirements of the enterprise are established.

RRD-2 DEVELOP SERVICE REQUIREMENTS

The resiliency requirements for services are developed and established based on the service mission and the requirements of supporting assets.

RRD-2.1 Establish Asset Resiliency Requirements
The resiliency requirements of assets as they relate to the services they support are established.

RRD-2.2 Assign Enterprise Resiliency Requirements to Services
Enterprise requirements that affect services are assigned to the services.

RRD-3 ANALYZE AND VALIDATE REQUIREMENTS

The resiliency requirements for services are analyzed and validated.

RRD-3.1 Establish a Definition of Required Functionality
Establish and maintain a definition of the required functionality of assets in the context of the services they support.

RRD-3.2 Analyze Requirements
Analyze the requirements of assets to identify conflicts, interdependencies, and shared requirements.

RRD-3.3 Validate Requirements
Ensure that the asset-level resiliency requirements provide protection and continuity commensurate with the value of the asset.

RRD-3.4 Identify and Resolve Requirements Conflict
Conflicts in requirements due to sharing of assets across services are identified and resolved.

RESILIENCY REQUIREMENTS MANAGEMENT

Engineering

Purpose

The purpose of Resiliency Requirements Management is to manage the resiliency requirements of services and associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

Concepts

Asset owners manage requirements

Asset custodians implement requirements and may also manage requirements in partnership with asset owner

Maintain traceability of the requirements

Identify inconsistencies in requirements

RRM-1 MANAGE REQUIREMENTS

Resiliency requirements are actively managed and inconsistencies between requirements and the activities necessary to satisfy them are identified.

RRM-1.1 Obtain an Understanding of Requirements
An understanding of the requirements is obtained from providers to ensure consistency and accuracy.

RRM-1.2 Obtain Commitment to Requirements
Commitments to the requirements are obtained from those who are responsible for satisfying the requirements.

RRM-1.3 Manage Requirements Changes
Changes to requirements are managed as conditions dictate.

RRM-1.4 Maintain Traceability of Requirements
Traceability of requirements between requirements and the activities performed to satisfy the requirements is established.

RRM-1.5 Identify Inconsistencies Between Requirements and Activities Performed to Meet The Requirements
Inconsistencies between requirements and the activities performed to satisfy the requirements are identified and managed.

SERVICE CONTINUITY

Engineering

Purpose

The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets in the event of an incident or disaster.

Concepts

Service continuity program

Continuity of operations plan development

Plan testing, exercising, execution

Lessons learned from past disruptions

SC-1 PREPARE FOR SERVICE CONTINUITY

The organizational processes for sustainability planning and execution are established.

SC-1.1 Plan for Service Continuity
Planning for the service continuity process is performed.

SC-1.2 Establish Standards and Guidelines for Service Continuity
The guidelines and standards for service continuity are established.

SC-2 IDENTIFY AND PRIORITIZE ESSENTIAL SERVICES

The essential services that are required to meet the organization's mission are identified and prioritized.

SC-2.1 Identify the Organization's Essential Services
The essential services of the organization, related functions and activities, and associated assets are identified.

SC-2.2 Identify Internal and External Dependencies and Interdependencies
The internal and external relationships necessary to ensure service continuity are identified and analyzed.

SC-2.3 Identify Vital Organizational Records and Databases
Vital information required for service continuity is identified.

SC-3 DEVELOP SERVICE CONTINUITY PLANS

Service continuity plans for essential organizational services are developed.

SC-3.1 Identify Plans to be Developed
The service continuity plans that must be developed, tested, and executed are identified.

SC-3.2 Develop and Document Service Continuity Plans
The required service continuity plans are developed and documented.

SC-3.3 Resource Service Continuity Plans
Resources are assigned to the service continuity plans to ensure effective execution.

SC-3.4 Store and Secure Service Continuity Plans
Service continuity plans are stored and made accessible to those who have a need to know.

SC-3.5 Communicate Plans to Relevant Stakeholders
Plans are communicated to relevant stakeholders.

SC-3.6 Develop Service Continuity Plan Training
Training for stakeholders in the service continuity plans is developed and administered.

SC-4 VALIDATE SERVICE CONTINUITY PLANS

Service continuity plans are validated to ensure they satisfy requirements and standards and to resolve conflict between plans.

SC-4.1 Validate Plans to Requirements and Standards
Service continuity plans are examined to ensure they satisfy requirements and standards.

SC-4.2 Identify and Resolve Plan Conflicts
Conflicts between service continuity plans are identified and resolved.

SC-5 EXERCISE PLANS

Service continuity plans are tested to ensure they meet their stated objectives.

SC-5.1 Develop Testing Program and Standards
A program and standards for plan testing is established and implemented.

SC-5.2 Develop and Document Plan Exercises
Service continuity plan exercises are developed and documented.

SC-5.3 Exercise Plans
Service continuity plans are exercised on a regular basis and results are documented.

SC-5.4 Evaluate Plan Test Results
Opportunities for improving service continuity plans are identified and implemented as a result of testing.

SC-6 EXECUTE PLANS

Service continuity plans are executed and reviewed.

SC-6.1 Execute Plans
Service continuity plans are executed as required.

SC-6.2 Measure the Effectiveness of the Plan in Operation
Post-execution review is performed to identify corrective actions.

SC-7 MAINTAIN SERVICE CONTINUITY PLANS

Changes to service continuity plans are identified and managed.

SC-7.1 Establish Change Criteria
Change criteria for service continuity plans are established.

SC-7.2 Maintain Changes to Plans
Changes are made to service continuity plans as conditions dictate.

TECHNOLOGY MANAGEMENT

Operations

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.

Concepts

Encompasses hardware, software, systems, tools, and infrastructure (such as cabling and networks)

Focus is integrity and availability of technology

Perform access control, change control, and release management

Address interaction with suppliers who may provide or support technology assets

Architecture interoperability

TM-1 ESTABLISH AND PRIORITIZE TECHNOLOGY ASSETS

Technology assets are prioritized to ensure resiliency of key services which they support.

TM-1.1 Prioritize Technology Assets
Technology assets are prioritized relative to their importance in supporting the delivery of key services.

TM-1.2 Establish Resiliency-Focused Technology Assets
Technology assets that specifically support key services are identified and established.

TM-2 PROTECT TECHNOLOGY ASSETS

Administrative, technical, and physical controls for technology assets are identified, implemented, monitored, and managed.

TM-2.1 Assign Resiliency Requirements to Technology Assets
Resiliency requirements that have been defined are assigned to technology assets.

TM-2.2 Establish and Implement Controls
Administrative, technical, and physical controls that are required to meet the established resiliency requirements are identified and implemented.

TM-3 MANAGE TECHNOLOGY ASSET RISK

Operational risks to technology assets are identified and managed.

TM-3.2 Mitigate Technology Risk
Risk mitigation strategies for technology assets are developed and implemented.

TM-4 MANAGE TECHNOLOGY ASSET INTEGRITY

The integrity of technology assets is managed.

TM-4.2 Perform Configuration Management
The configuration of technology assets is managed.

TM-4.3 Perform Change Control and Management
Changes to technology assets are managed.

TM-4.4 Perform Release Management
The iteration of technology assets placed into the production environment is managed.

TM-5 MANAGE TECHNOLOGY AVAILABILITY

The availability of technology assets to support key services is managed.

TM-5.1 Perform Technology Sustainability Planning
The availability and functionality of key technology assets is ensured through sustainability planning.

TM-5.2 Manage Technology Asset Maintenance
Operational maintenance is performed on technology assets.

TM-5.3 Manage Technology Capacity
The operating capacity of technology assets is managed.

TM-5.4 Manage Technology Interoperability
The interoperability of technology assets is managed.

TM-5.5 Manage Technology Asset Acquisition
Suppliers that provide technology assets or support technology assets are managed.

VULNERABILITY ANALYSIS AND RESOLUTION

Operations

Purpose

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

Concepts

Threat and vulnerability identification and monitoring

Vulnerability analysis

Manage exposure to identified vulnerabilities

Supply input to Risk Management

VAR-1 PREPARE FOR VULNERABILITY ANALYSIS AND RESOLUTION

Preparation for vulnerability analysis and resolution activities is conducted.

VAR-1.1 Establish Scope
The assets and operational environments that must be examined for vulnerabilities are identified.

VAR-1.2 Establish a Vulnerability Analysis and Resolution Strategy
Establish and maintain an operational vulnerability analysis and resolution strategy.

VAR-2 IDENTIFY AND ANALYZE VULNERABILITIES

Establish and maintain a process for identifying and analyzing vulnerabilities.

VAR-2.1 Identify Sources of Vulnerability Information
The sources of vulnerability information are identified.

VAR-2.2 Discover Vulnerabilities
A process is established to actively discover vulnerabilities.

VAR-2.3 Analyze Vulnerabilities
Vulnerabilities are analyzed to determine if they need to be reduced or eliminated.

VAR-3 MANAGE EXPOSURE TO VULNERABILITIES

Strategies are developed to manage exposure to identified vulnerabilities.

VAR-3.1 Manage Exposure to Vulnerabilities
Strategies are developed and implemented to manage exposure to identified vulnerabilities.

VAR-4 IDENTIFY ROOT CAUSES

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

VAR-4.1 Perform Root-Cause Analysis
Perform review of identified vulnerabilities to determine and address underlying causes.

Generic Common Goals and Practices

Common Goal 1 ACHIEVE CAPABILITY GOALS

The operational resiliency management process supports and enables achievement of the objectives of the capability area by transforming identifiable input work products to produce identifiable output process artifacts.

Common Practice 1.1 Perform Capability Area Practices

Perform the practices of the capability area to develop process artifacts and provide services to achieve the goals of the capability area.

Common Goal 2 INSTITUTIONALIZE RESILIENCY ENGINEERING AS A MANAGED PROCESS

Resiliency engineering is institutionalized as a managed process.

Common Practice 2.1 Establish Process Governance

Establish and maintain governance over the planning and performance of the process.

Common Practice 2.2 Create the Process Plan

Establish and maintain the plan for performing the process.

Common Practice 2.3 Provide Resources

Assign responsibility and authority for performing the process, developing the process artifacts, and providing the services of the process.

Common Practice 2.4 Assign Responsibility

Assign responsibility and authority for performing the process, developing the process artifacts, and providing the services of the process.

Common Practice 2.5 Train Resources

Train the people performing or supporting the process as needed.

Common Practice 2.6 Manage Process Artifacts

Place designated process artifacts of the process under appropriate levels of control.

Common Practice 2.7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the process as planned.

Common Practice 2.8 Establish and Manage Supporting Infrastructure [CERT]

Define, implement, and maintain the appropriate infrastructure to support the production of process artifacts and the delivery of services.

Common Practice 2.9 Monitor and Control Processes

Monitor and control the process against the plan for performing the process and take appropriate correction action.

Common Practice 2.10 Objectively Evaluate Adherence

Objectively evaluate adherence of the process against its process description, standards, and procedures, and address noncompliance.

Common Practice 2.11 Review Status with Senior Management

Review the activities, status, and results of the process with senior management and resolve issues.

Common Goal 3 INSTITUTIONALIZE OPERATIONAL RESILIENCY AS A DIRECTED PROCESS

Operational resiliency is institutionalized as a directed process.

Common Practice 3.1 Establish a Defined Process

Establish and maintain the description of a defined process.

Common Practice 3.2 Measure Performance to Requirements [CERT]

Measure the performance of processes in terms of the satisfaction of resiliency requirements for assets and services that are the focus of processes.

Common Practice 3.3 Collect Improvement Information

Collect process artifacts, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

Common Goal 4 INSTITUTIONALIZE OPERATIONAL RESILIENCY AS A CONTINUALLY-IMPROVED PROCESS

Operational resiliency is institutionalized as a continually-improved process.

[Author's note: The detailed practices and subpractices for Common Goal 4 are under development and will be included in future versions of CERT-REF.]