Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Controls Management (CTRL)

Richard A. Caralli
Julia H. Allen
David W. White
Lisa R. Young
Nader Mehravari
Pamela D. Curtis

February 2016

CERT Program

http://www.cert.org/resilience/

Carnegie Mellon

This material is based upon work funded and supported by various entities under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Various or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0003234

CONTROLS MANAGEMENT

Engineering

Purpose

The purpose of Controls Management is to establish, monitor, analyze, and manage an internal control system that ensures the effectiveness and efficiency of operations through assuring mission success of high-value services and the assets that support them.

Introductory Notes

Internal control is a governance process used by the organization to ensure effective and efficient achievement of organizational objectives and to provide reasonable assurance of success. The internal control process is pervasive throughout the organizational structure from higher level managers to staff and is reflected in all levels of operations—in many cases, down to the transaction level.

The organization's high-level managers have the responsibility to set the tone for internal control so that the objectives of the organization are reflected in all operational activities. In this way, the organization ensures success by building in success criteria at all operational levels.

The internal control process is typically reflected in the organization's *internal control system*. By definition, the internal control system is the aggregation of the activities an organization undertakes to ensure success. While this is primarily operational in implementation, there are other broad objectives of the internal control system, including promoting ethical behavior, preventing and detecting fraud, ensuring compliance with laws and regulations, and providing more predictability in the overall performance of the organization. At the operational level, the internal control system is the aggregation of the policies, procedures, methods, technologies, and tools that provide assurance that management directives are carried out. For example, an organization may find it vital to its profitability that all intellectual property be kept confidential and only provided to staff with a justifiable need to know. Thus, a policy may be drafted that provides guidance on the effective handling and distribution of this information. The policy is a means for implementing management's directives and minimizing impact on organizational success and achievement.

Internal control in a broad sense is focused on ensuring that the financial condition of an organization is accurately reflected in its financial and accounting records. However, at an operational level, internal control relates to implementing policies, procedures, methods, technologies, and tools that support service mission assurance. Typically this involves the development of high-level control objectives that align with service mission assurance requirements and strategies to protect and sustain services that satisfy these requirements. Control objectives are then translated into appropriate policies, procedures, methods, technologies, and tools—referred to as operational controls—that are needed to meet each objective. From an operational resilience management perspective, these operational controls are critical to protecting assets, sustaining assets, and preventing disruption to assets as they are deployed in the execution of a service. That said, effective controls management for operational resilience means identifying the most cost-effective strategies for protecting and sustaining assets and services. The organization should seek the optimum mix in contrast to, for example, deploying an extensive number of overlapping and redundant controls in reaction to new compliance requirements.

In the Controls Management process area, the organization establishes control objectives that reflect the organization’s objectives and mission and defines the target for the development of enterprise- and operational-level controls. Enterprise controls are developed to address organization-wide directives that universally affect all operational layers. Operational controls are developed, implemented, monitored, analyzed, and managed at the services level to ensure services meet their mission and, specifically, that assets related to services are protected from disruption. These controls may be administrative, technical, or physical in nature and typically are implemented in layers to reinforce strategies to protect and sustain assets and to meet control objectives. Enterprise and operational controls are analyzed and validated to ensure that they meet control objectives as implemented; gaps in effectiveness are identified on a periodic basis and addressed so that control objectives are attained on a consistent basis.

The internal control environment in an organization is vast; however, in Controls Management the focus is on controls that relate directly to the deployment of people and the use of information, technology, and facilities in executing services. Depending on the organization, this may include administrative controls, such as separation of duties, or more specific controls, such as the implementation of a physical access control system at a facility. In other words, the subset of operational controls used by the organization to ensure operational resilience is specific to the high-value services that the organization relies on to carry out its mission. Thus, this subset is likely only a small part of the organization’s overall internal control system.

The Controls Management and Service Continuity process areas establish the range of controls necessary to ensure that services achieve their missions even when disrupted. Controls Management focuses on controls that support protection and sustainment strategies—those that help to prevent services and assets from exposure to vulnerabilities and threats and those that help services and assets respond and recover when disrupted. However, all threat conditions cannot be known or anticipated. Service Continuity also focuses on sustaining services and assets under degraded conditions and in returning them to a normal operating state when possible. Service Continuity is also important because controls that have been implemented may not always meet control objectives or may not be operating effectively. In these cases, until control remediation actions can occur, the service continuity process sustains services and their supporting assets in the near term.

Related Process Areas

Strategic goals, objectives, critical success factors, and governance for the operational resilience management system, as well as the identification of high-value services, are addressed in the Enterprise Focus process area.

Identification, analysis, and mitigation strategies for operational risks are addressed in the Risk Management process area.

Ensuring compliance with identified obligations related to managing operational resilience, including those satisfied by the internal control system, is addressed in the Compliance process area.

The relationship between assets and services is established in the Asset Definition and Management process area.

The identification and implementation of controls for information assets are performed in the Knowledge and Information Management process area.

The identification and implementation of controls for facilities are performed in the Environmental Control process area.

The identification and implementation of controls for technology assets are performed in the Technology Management process area.

Controls related to establishing and managing the contributions and availability of people are identified and implemented in the People Management process area.

The development of service continuity plans as a control for protecting and sustaining services and assets is addressed in the Service Continuity process area.

Monitoring the internal control system for the operational resilience management system is addressed in the Monitoring process area.

Supporting information needs for managing the internal control system in support of operational resilience is addressed in the Measurement and Analysis process area.

Summary of Specific Goals and Practices

Goals	Practices
CTRL:SG1 Establish Control Objectives	CTRL:SG1.SP1 Define Control Objectives
CTRL:SG2 Establish Controls	CTRL:SG2.SP1 Define Controls
CTRL:SG3 Analyze Controls	CTRL:SG3.SP1 Analyze Controls
CTRL:SG4 Assess Control Effectiveness	CTRL:SG4.SP1 Assess Controls

Specific Practices by Goal

CTRL:SG1 Establish Control Objectives

Organizational objectives to be achieved through the selection and implementation of controls are established.

A control objective is a performance target for a control or an internal control system. The organization uses control objectives as a means for selecting, analyzing, and managing an appropriate level of controls to achieve the organization’s strategic objectives. Control objectives broadly reflect management’s directives at an enterprise, line of business, or organizational unit level.

Control objectives can be developed for various organizational processes and systems. For example, a set of financial control objectives can be established to ensure that accounting and financial transactions are accurate, timely, valid, and documented. Conversely, control objectives can be established for information technology processes to ensure that systems and software meet their objectives with reasonable assurance, in an efficient and effective manner, and with a high degree of fraud prevention.

Control objectives can also be established with varying degrees of specificity. For example, a control objective may be established at the enterprise level that requires separation of duties between staff who enter invoices into a payment system and staff who approve payment of invoices. Conversely, a control objective may be established for an application system to ensure that a vendor is not paid twice for the same invoice.

CTRL:SG1.SP1 Define Control Objectives

Control objectives are established as the basis for the selection, implementation, and management of the organization's internal control system.

Control objectives are broad-based targets for the effective and efficient performance of controls. Establishing control objectives is an activity that guides the organization's ability to link controls to management directives.

For operational resilience management, control objectives are defined relative to the organization's strategic objectives, risk appetite and environment, and the resilience requirements of high-value assets and services. The control objectives are driven by strategies for protecting and sustaining service-related assets to ensure that their exposure to vulnerabilities and threats is managed. Based on the control objectives and the larger protection and sustainment strategies, specific controls are selected, analyzed, and managed to ensure that control objectives are satisfied.

Typical work products

1. Management directives and guidelines for selecting control objectives
2. Control objectives
3. Criteria for prioritizing control objectives
4. List of prioritized control objectives

Subpractices

1. Identify management directives and organizational guidelines upon which to base the definition of control objectives. (*Refer to EF:SG1.SP1 for more information.*)

   Sources of management directives and guidelines may include the following:

   - strategic objectives and statements of risk appetite, tolerance, and thresholds
   - internal policies, procedures, standards, and guidelines that the organization establishes to promote acceptable behaviors, ethics, and practices
   - line of business and organizational unit business objectives and operating plans supported by interviews with organizational unit and line of business managers
   - resilience requirements for services and supporting assets supported by interviews with service owners, business process owners, and asset owners and custodians
   - relationships, contracts, service level agreements, and obligations with external entities (*Refer to the External Dependencies Management process area for additional information about managing relationships with external entities.*)
   - legal and regulatory compliance obligations supported by interviews with auditors and legal staff
   - ethics and integrity codes of practice and statements

2. Define and document control objectives that result from management directives and guidelines.

   Affinity analysis of directives and guidelines may be useful in identifying categories of control objectives.

   These are examples of control objectives:

   - Prevent unauthorized use of purchase orders.
   - Ensure adequate supplies of materials.
   - Establish an enterprise architecture for information technology.
   - Develop and communicate policies regarding standards of ethical behavior.
   - Identify and assess risks that may cause material misstatements of financial records.
   - Educate and train staff.
   - Manage external entity relationships.
   - Establish a compliance program.

3. Prioritize control objectives.

   The intent of prioritization is to determine the control objectives that most need attention because of their potential to affect operational resilience.

   Assigning a relative priority to each control objective or category aids in determining the level of resources to apply when defining, analyzing, assessing, and addressing gaps in controls *(refer to CTRL:SG2, CTRL:SG3, and CTRL:SG4)*.

   Management directives and guidelines can be used to establish criteria for prioritizing control objectives.

CTRL:SG2 Establish Controls

Controls that support control objectives and strategies for protecting and sustaining high-value services and assets are established.

A control is a policy, procedure, method, technology, or tool that satisfies a stated control objective. For operational resilience management, the focus is limited to the subset of controls that reduce exposure to threats and vulnerabilities that can affect the productive capacity of people, information, technology, and facilities as they are deployed in services, as well as those that help services and assets respond and recover when disrupted.

Controls can be broad or specific. Enterprise-level controls typically apply universally to all operational processes. An example of such a control is to perform required background checks on all prospective employees before they are hired. Operational-level controls are more specific. The implementation of an access control system on a data center is an operational-level control.

All controls can be categorized as one of three types:

- **Administrative controls** (often called “management” controls) ensure alignment to management’s intentions and include such actions as governance, setting policy, monitoring, auditing, enforcing separation of duties, and developing and implementing service continuity plans. Enterprise-level controls are typically administrative in nature because other than stating management’s intention, they have little ability to *prevent* unwanted activities or disruptions. Administrative controls can be used to implement resilience requirements for confidentiality, integrity, and availability, although generally they have to be coupled with technical and physical controls to be effective.

- **Technical controls** are operational controls that are implemented through technological means. They include electronic access controls, firewalls, encryption, and intrusion detection systems. Operational controls are often technical because they exist in automated processes, manifested in software, systems, hardware, networks, and telecommunications infrastructure. Technical controls are effective for implementing all types of resilience requirements.
- **Physical controls** are operational controls that provide physical barriers to access. Physical controls can apply to people (in a safety sense), technology, and other tangible assets such as facilities. These controls typically include picture IDs, card readers and locks on file room doors, and other physical security methods. Physical controls are most effective for implementing integrity and availability requirements but can also be used to ensure confidentiality.

Controls can also be categorized by where and when they are implemented in the execution of a service to ensure the effective and efficient operation of that service (as well as protecting and sustaining its supporting assets). Controls can be preventive, detective, compensating, or correcting. Preventive controls attempt to deter or prevent undesirable events from occurring. Preventive controls are typically technical or physical in nature, but some administrative controls can also be used in a preventive way. Detective controls, on the other hand, attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Compensating controls may provide a level of redundancy that helps to further reduce the risk that undesirable events could affect a service. Correcting controls support detective controls by helping to “fix” a problem that has been detected.

A layering of all types of controls is essential to an effective internal control system. From an operational resilience standpoint, preventive controls are essential because they are proactive and contribute to protection of assets. However, detective controls play a critical role in providing evidence that the preventive controls are (or are not) functioning adequately.

The most effective mix of controls depends on the management directives and guidelines that have to be satisfied and the overall cost to the organization. Controls are often expensive to implement and to manage long term, particularly preventive controls, so the organization must strike an optimal balance between the satisfaction of directives and the cost of controls.

These are examples of preventive controls:

- separation of duties
- two-person rules to limit risk of fraud or error by one person
- proper authorization and approval of transactions
- physical safeguards and electronic access control for assets
- supervision and monitoring of ongoing operational activity
- adequate documentation
- use of passwords

These are examples of detective controls:

- audits
- reviews
- variance analyses
- physical inventory
- retention of documentation, logs, and records to substantiate transactions
- periodic and regular operational reviews

CTRL:SG2.SP1 Define Controls

Controls that protect services and assets from disruption are identified and established.

Administrative, technical, and physical controls are established to meet operational resilience management control objectives. Controls can be at the enterprise level or at the service and asset level.

Enterprise-level controls derive from enterprise-level control objectives. At a strategic level, they establish the boundaries, parameters, checks, and balances that the organization imposes on all organizational units and lines of business to ensure objectives are achieved. This includes any external control requirements that the organization inherits from its market sector affiliations and competitive environment. An example of this type of requirement is laws and regulations—they broadly affect the sector in which an organization operates and must be met by all organizational units. Ensuring the confidentiality of health-related information is an example of an enterprise-level control objective; the use of encryption for sensitive patient information is an example of an enterprise-level control.

Enterprise-level controls may also be derived from the results of risk identification activities such as security assessments and business impact analysis.

Table CTRL-1 provides one example of the relationships among an enterprise control objective, a risk, and controls to meet the objective and mitigate the risk.

Table CTRL-1

Enterprise Control Objective	Risk	Enterprise Controls
The person who requisitions the purchase of goods or services should not be the person who approves the purchase.	Fraud, mistake, or error by one person	End-to-end responsibility for any series of financially related transactions to be distributed among two or more staff members or departments
		Periodic rotation of job duties between staff members or departments

With respect to service-level controls, high-value services are identified, prioritized, and communicated in the Enterprise Focus process area *(refer to EF:SG1.SP3)*. Assuring service mission success is the focus for defining service-level controls that meet their corresponding control objectives.

Table CTRL-2 provides one example of the relationships among a service-level control objective, a risk, and controls to meet the objective and mitigate the risk.

Table CTRL-2

Service-Level Control Objective	Risk	Service Controls
Access to the network and any network-connected system (e.g., file and print services, application servers, database servers) is controlled to prevent access by unauthorized entities.	Users may have inappropriate or unauthorized access to the network and network-connected systems and services.	System owner grants network access to staff based on approved access request forms.
		Periodically, IT managers verify the current network/system access list with system owners to ensure network/system access is appropriate and accurate.
		Administrative access, enabling the administrator to grant network/ system access, is restricted to IT managers.

In large part, service-level controls derive from the aggregation of all supporting asset-level controls. Using the example above, access controls on the network asset, network-connected system assets, application server assets, and database server assets are the access controls for the service they support. In addition, controls such as the service continuity plans developed in the Service Continuity process area serve as essential controls for sustaining services.

With respect to asset-level controls, the relationship between assets and services is established in the Asset Definition and Management process area *(ADM:SG2)*. Controls for protecting and sustaining high-value assets that support high-value services are also required for service mission assurance.

Asset-level controls are identified and implemented in the following process areas:

- information assets: Knowledge and Information Management process area *(See KIM:SG2.SP2.)*
- facilities: Environmental Control process area *(See EC:SG2.SP2.)*
- technology assets: Technology Management process area *(See TM:SG2.SP2.)*
- people: People Management process area *(See all SGs and SPs.)*

Service-level and asset-level controls that are identified in other CERT-RMM process areas are established in this specific practice as the basis for satisfying control objectives.

Typical work products

1. Enterprise-level controls (including responsible entity)
2. Service- and asset-level controls (including responsible entity)
3. Traceability matrix of control objectives and controls

Subpractices

1. Establish enterprise-level controls to satisfy control objectives.

   These can be a combination of controls that already exist, controls that have to be updated, and new controls that have to be implemented.

2. Confirm or assign responsibility for implementing enterprise-level controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls. This responsibility is typically assumed by organizational unit and line of business managers or their designees and is accomplished through operating plans and directives and guidelines at this level.

   Enterprise-level controls may also be implemented through service- and asset-level controls as described in subpractices 3, 4, and 5.

3. Establish service- and asset-level controls to satisfy control objectives.

   These can be a combination of controls that already exist, controls that have to be updated, and new controls that have to be implemented.

4. Confirm or assign responsibility for implementing service- and asset-level controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls. This responsibility is typically assumed by service and asset owners and asset custodians and is accomplished in the service and asset process areas referenced above.

5. Develop a bidirectional traceability matrix that maps control objectives and enterprise-, service-, and asset-level controls.

   Service- and asset-level controls that are identified in other CERT-RMM process areas are mapped to control objectives in this specific practice. Each control objective has one or more controls that are intended to satisfy it.

   Refer to CTRL:SG3 and CTRL:SG4 for the treatment of control objectives that are not adequately addressed by existing, updated, and new controls.

CTRL:SG3 Analyze Controls

Controls are analyzed to ensure they satisfy control objectives.

Existing controls must be analyzed to determine that they meet resilience requirements and can achieve stated control objectives. In addition, proposed new controls must be analyzed to ensure that they harmonize with and enhance the internal control system in a cost-effective manner.

Analysis of controls includes the activities that the organization performs to

- ensure a proper mix and layering of controls to meet a stated control objective or a series of objectives
- identify control gaps
- identify updates to existing controls and identify proposed new controls and other methods to address control gaps

- identify risks that could arise as a result of remaining gaps even when controls are operating effectively *(Refer to CTRL:SG4 and the Risk Management process area.)*
- identify costly control redundancy and conflicting controls and eliminate them where possible

CTRL:SG3 establishes a baseline analysis of the extent to which existing controls and proposed new controls cover and achieve control objectives for the resilience of services and supporting assets. CTRL:SG4 uses this established baseline as the foundation for periodically assessing the extent to which controls continue to achieve control objectives and the extent to which control objectives continue to meet resilience requirements.

Refer to the Risk Management process area for further details about identifying, analyzing, and mitigating risks to services and assets arising from inadequate controls.

CTRL:SG3.SP1 Analyze Controls

Controls are analyzed to determine their ability to achieve control objectives.

Analysis of controls is focused on ensuring that controls (both existing and proposed) meet one or more control objectives and, by extension, resilience requirements. Analysis also ensures that all service-level control objectives are adequately satisfied by one or more service-level controls and asset-level controls for assets that support the service. Analysis may range from a subjective review of the control’s ability to meet the control objective to the development and execution of tests that demonstrate the control’s capability. The organization must determine the level of analysis necessary in each case; however, the importance of the control in supporting operational resilience should determine the extent of analysis required and which analysis techniques are deployed.

Controls analysis should also help the organization to identify

- any gaps where the control does not fully meet one or more control objectives
- any gaps where an enterprise-level control objective that addresses the resilience of services and supporting assets is not adequately satisfied by one or more controls
- any gaps where a service control objective is not adequately satisfied by one or more service- or asset-level controls

In these cases, the organization must either redesign and update existing controls or identify proposed new controls (including “helper” controls such as compensating controls). Analysis is repeated to ensure the control objective is satisfied by updated and proposed controls.

The analysis process should facilitate the identification of risks that arise when a control cannot fully satisfy control objectives. Such risks are referred to the risk management process, where they can either be mitigated in other ways, or the organization may have to choose to accept and manage the risk over time. Accepting the risk of a gap in controls may be the disposition when the control objective’s priority does not warrant further investment in updated or new controls.

Finally, controls analysis should be used to determine how any proposed new control fits with the current internal control system and whether the proposed control is redundant or conflicts with any existing control. Often, control layering is confused with control redundancy. Control layering is a purposeful design and implementation of controls that collectively meet one or more control objectives. However, control redundancy results when more than one type of control is used to meet the same control objective but is unnecessary. Because controls can be costly, the identification and treatment of redundant and conflicting controls must be performed during the analysis process.

Typical work products

1. Analysis results
2. Control objectives that are satisfied by controls
3. Updated traceability matrix of control objectives and the controls that satisfy them
4. Control gaps
5. Updates to existing controls
6. Proposed new controls
7. Risks related to unsatisfied control objectives
8. Risks related to redundant and conflicting controls

Subpractices

1. Analyze existing controls against control objectives.

   Affinity analysis of control objectives may be useful in identifying categories of controls needed to satisfy these. Conversely, affinity analysis of controls may be useful in determining the extent to which they cover control objectives.

   Conducting surveys and interviews with the owners of enterprise-level controls, owners of service-level controls, and owners and custodians of asset-level controls may aid the analysis process. The assessment practices described in CTRL:SG4.SP1 may also aid in the analysis process.

2. Identify gaps where an existing control does not fully meet one or more control objectives.
3. Identify gaps where enterprise control objectives for the resilience of services and assets and service control objectives are not adequately satisfied by existing controls.

   For example, the organization may have

   - resource (human and financial) limitations or constraints
   - lack of adequate infrastructure or supporting processes and technology
   - insufficient funding for risk mitigation

- an inability to determine benefits that outweigh the investment in controls to satisfy a compliance obligation

4. Identify updates to existing controls and proposed new controls to address gaps.

   This includes identifying gaps where the control objective's priority *(refer to CTRL:SG1. SP1 subpractice 3)* does not warrant further investment in updated or new controls. *(Such gaps are addressed in subpractice 6.)*

5. Identify redundant and conflicting controls and make changes to address them.

   This includes identifying conflicts between enterprise-level controls, service-level controls, and asset-level controls *(refer to CTRL:SG2.SP1)*.

   Additional updates to existing controls and proposed new (perhaps combined) controls are identified to resolve these issues.

6. Identify risks that may result from unsatisfied control objectives as well as redundant and conflicting controls.

   Risks resulting from unsatisfied control objectives and redundant and conflicting controls should be documented and referred to the risk management process for analysis and resolution.

CTRL:SG4 Assess Control Effectiveness

The ability of the internal control system to satisfy resilience requirements is assessed.

Enterprise- and service-level control objectives and associated controls are objectively assessed to ensure that they support the required resilience of services and their associated assets. A review of the alignment between the organization's resilience requirements and the internal control system is performed to determine if control objectives are missing or inadequately covered. Risks associated with unsatisfied control objectives are also considered *(refer to CTRL:SG3.SP1)*.

Assessing the internal control system is an ongoing activity that allows the organization to measure the effectiveness of controls across resilience activities. For example, through monitoring and ongoing measurement and analysis, the organization can determine whether controls are satisfying control objectives, strategies for protecting and sustaining services and assets, and resilience requirements. These activities can also ascertain if controls for resilience activities are effective and producing the intended results. Monitoring and measurement are two ways that the organization collects necessary data (and invokes a vital feedback loop) to know how well controls are performing in support of the operational resilience management system.

Weaknesses in the internal control system may be identified by a variety of means, including control self-assessments, business impact analyses, internal audits, external audits, and assessments against an established standard *(in addition, refer to the Compliance process area)*.

Some key questions to ask (in concert with practices in the Risk Management and Compliance process areas) include these:

- Has the organization identified control gaps resulting in risks that are not cost-effective to control?
- Is the justification to accept a gap in the internal control system commensurate with the risk appetite, risk tolerance, and value of the services and assets that remain unprotected?
- Are there areas of non-compliance that can be addressed in a cost-effective manner by updating existing controls or adding new controls?

CTRL:SG3 establishes a baseline analysis of the extent to which existing controls and proposed new controls cover and achieve control objectives for the resilience of services and supporting assets. CTRL:SG4 uses this established baseline as the foundation for periodically assessing the extent to which controls continue to achieve control objectives and the extent to which control objectives continue to meet resilience requirements. Thus, CTRL:SG4 captures the continuous monitoring, review, and improvement activities that are essential to ensure that controls remain effective.

Refer to the Compliance process area for further details about ensuring that compliance obligations are fulfilled, including those that rely on the internal control system.

Refer to the Risk Management process area for further details about identifying, analyzing, and mitigating risks to services and assets arising from inadequate controls.

Refer to the Monitoring process area for further details about collecting, recording, and distributing information about the internal control system for the operational resilience management system.

Refer to the Measurement and Analysis process area for further details about supporting management information needs for managing the internal control system in support of operational resilience.

CTRL:SG4.SP1 Assess Controls

Controls are assessed for effectiveness in meeting control objectives and satisfying resilience requirements.

Performing periodic assessment of the internal control system is necessary to ensure that controls continue to meet control objectives, that control objectives continue to implement strategies for protecting and sustaining services (and their supporting assets), and that resilience requirements are satisfied. Conversely, assessment of the internal control system identifies areas where controls are ineffective and inefficient along with determining whether controls have to be modified to reflect changing business and risk conditions. Control assessment provides opportunities to save costs by eliminating redundant controls and resolving control conflicts.

One of the objectives of the assessment process is to identify areas where the internal control system is not performing as expected, when measured against relevant internal and external guidelines, standards, practices, policies, regulations, legislation, and other obligations such as contracts and service level agreements related to managing operational resilience *(refer also to the Compliance process area)*. As a result of conducting the assessment process, the organization may learn of areas that need attention, particularly if they are keeping the organization from meeting business objectives or compliance obligations. These areas may require the creation of detailed remediation plans and strategies to ensure that control objectives are sufficiently achieved by controls.

Typical work products

1. Assessment scope
2. Assessment results
3. Problem areas
4. Updates to existing controls
5. Proposed new controls
6. Remediation plans
7. Updates to service continuity plans
8. Risks related to unresolved problems

Subpractices

1. Select the scope for the assessment.

Typically this will be one or more high-value services and the high-value assets that support them. The scope of an assessment should also periodically include enterprise-level control objectives and controls for operational resilience *(refer to CTRL:SG2.SP1)*.

2. Perform the assessment.

Various assessment techniques can be used ranging from informal self-assessments to more structured formal assessments against established standards. Affinity analysis, interviews, and surveys *(refer to CTRL:SG3.SP1)* may provide useful insight. In addition, results from business impact analyses *(refer to the Service Continuity process area)*, risk assessments *(refer to the Risk Management process area)*, and internal audits and external audits *(refer to the Compliance process area)* can contribute.

3. Identify problem areas.

Problem areas arise where controls are ineffective or inefficient or provide insufficient coverage of control objectives, and where controls are redundant and conflicting.

While controls may be effective and efficient in support of a specific control objective, this may not be the case when controls span control objectives.

4. Identify updates to existing controls and proposed new controls to address problem areas.

Organizations can realize efficiencies of scale by requiring specific controls for a given type of asset. For example, standardizing desktop and laptop system configurations or deploying access control systems across a range of technology assets that support multiple high-value services can reduce the cost of controls.

Straightforward changes can be addressed by service and asset owners and the line of business and organizational unit managers to whom they report. For more complex changes that require broader organizational planning and coordination, a remediation plan may be required.

Remediation plans should address

- the actions the organization must take to ensure that controls satisfy control objectives effectively and efficiently
- changes to the internal control system
- assignment of responsibility and authority to perform the work
- schedule and costs to perform the work
- documentation of risk mitigation strategies and residual risks

The actions called for in remediation plans must be tracked to closure. Plans are updated as required.

Any changes to existing controls and the addition of any new controls may result in the need for a reassessment.

5. Identify updates to service continuity plans that may result from changes to the internal control system.

Refer to the Service Continuity process area.

6. Identify risks that may result from unresolved problems.

Risks resulting from unresolved problems in the internal control system should be documented and referred to the risk management process for analysis and resolution.

Unresolved problems that result in new mitigation strategies and residual risks that have to be managed should be periodically included in the scope for reassessment of the originally selected services and assets.

Elaborated Generic Practices by Goal

Refer to the Generic Goals and Practices document in Appendix A for general guidance that applies to all process areas. This section provides elaborations relative to the application of the Generic Goals and Practices to the Controls Management process area.

CTRL:GG1 Achieve Specific Goals

The operational resilience management system supports and enables achievement of the specific goals of the Controls Management process area by transforming identifiable input work products to produce identifiable output work products.

CTRL:GG1.GP1 Perform Specific Practices

Perform the specific practices of the Controls Management process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices CTRL:SG1.SP1 through CTRL:SG4.SP1 are performed to achieve the goals of the controls management process.

CTRL:GG2 Institutionalize a Managed Process

Controls management is institutionalized as a managed process.

CTRL:GG2.GP1 Establish Process Governance

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

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the controls management process.

Subpractices

1. Establish governance over process activities.

Elaboration:

Governance over the controls management process may be exhibited by

- developing and publicizing higher level managers' objectives and charter for establishing and managing the internal control system
- establishing a higher level position, such as a chief compliance officer, to provide direct oversight of the process and to interface with higher level managers
- sponsoring and providing oversight of process policies, procedures, standards, and guidelines, including management directives and guidelines that serve as the basis for selecting control objectives
- sponsoring and providing oversight over the organization's internal control system, remediation plans, and process plan
- regular reporting from organizational units to higher level managers on process activities and results
- making higher level managers aware of applicable compliance obligations related to the internal control system, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- sponsoring and funding process activities
- aligning control objectives with identified resilience needs and objectives and stakeholder needs and requirements
- verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
- creating dedicated higher level management feedback loops on decisions about the internal control system and recommendations for improving the process
- providing inputs on identifying, assessing, and managing risks due to missing, ineffective, inefficient, redundant, and conflicting controls
- conducting regular internal and external audits and related reporting to audit committees on process effectiveness
- creating formal programs to measure the effectiveness and efficiency of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

   Elaboration:

   The controls management policy should address

   - responsibility, authority, and ownership for performing process activities
   - procedures, standards, and guidelines for
     - defining and selecting control objectives
     - prioritizing control objectives
     - evaluating and acquiring tools for monitoring the performance of controls
     - analyzing and assessing controls
     - identifying gaps in controls and approaches for addressing them
     - identifying redundant and conflicting controls
     - identifying risks associated with problems in the internal control system
   - periodically assessing the internal control system
   - methods for measuring adherence to policy, exceptions granted, and policy violations

CTRL:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the controls management process.

Elaboration:

The plan for the controls management process should be directly influenced by the management directives and guidelines and resilience requirements that serve as the basis for defining control objectives.

The plan for the controls management process should not be confused with remediation plans for changes to the internal control system that require broad organizational planning and coordination as described in CTRL:SG4.SP1. The plan for the controls management process details how the organization will perform controls management, including the development of remediation plans.

Subpractices

1. Define and document the plan for performing the process.
2. Define and document the process description.
3. Review the plan with relevant stakeholders and get their agreement.
4. Revise the plan as necessary.

CTRL:GG2.GP3 Provide Resources

Provide adequate resources for performing the controls management process, developing the work products, and providing the services of the process.

Subpractices

1. Staff the process.

These are examples of staff required to perform the controls management process; such people may include organizational unit managers, line of business managers, project managers, and asset and service owners and custodians:

- staff responsible for
  - developing the process plan and ensuring it is aligned with stakeholder requirements and needs
  - defining process standards, guidelines, and procedures
  - implementing process standards, guidelines, and procedures, including implementing automated means to collect, analyze, validate, and report on the status and effectiveness of controls
  - coordinating process activities across organizational units and lines of business
  - analyzing and assessing controls
  - addressing issues and problem areas in controls resulting from analysis and assessment, including developing and executing remediation plans
  - managing external entities that have contractual obligations for process activities
- owners of enterprise-level controls that affect the resilience of services and assets
- service owners and asset owners and custodians responsible for implementing controls
- a compliance officer who assumes responsibility for all process activities as they affect the organization's ability to meet compliance obligations
- owners and custodians of high-value services and assets that support the accomplishment of operational resilience and process objectives
- internal and external auditors responsible for reporting to appropriate committees on the satisfaction of control objectives and process effectiveness

Refer to the Organizational Training and Awareness process area for information about training staff for resilience roles and responsibilities.

Refer to the Human Resource Management process area for information about acquiring staff to fulfill roles and responsibilities.

2. Fund the process.

Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for controls management.

3. Provide necessary tools, techniques, and methods to perform the process.

Elaboration:

These are examples of tools, techniques, and methods to support the controls management process:

- affinity analysis methods for categorizing control objectives and analyzing controls
- methods for prioritizing control objectives
- techniques and tools for developing and maintaining traceability between control objectives and controls
- methods for conducting surveys and interviews

- methods and techniques for identifying and addressing gaps in controls as well as conflicting and redundant controls
- methods, techniques, and tools for control analysis and assessment
- methods, techniques, and tools for coordinating process activities across organizational units and lines of business
- methods, techniques, and tools for collecting, analyzing, validating, and managing information about the internal control system
- monitoring, auditing, and other assessment techniques to identify problem areas
- methods and tools for managing changes to controls

CTRL:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the controls management process, developing the work products, and providing the services of the process.

Elaboration:

As identified in specific practice CTRL:SG2.SP1, responsibility for enterprise-level controls is typically assumed by organizational unit and line of business managers or their designees; responsibility for service- and asset-level controls is typically assumed by service and asset owners and custodians.

Refer to the Human Resource Management process area for more information about establishing resilience as a job responsibility, developing resilience performance goals and objectives, and measuring and assessing performance against these goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   From an enterprise perspective, the organization may assign responsibility to a compliance group or a compliance process group led by a compliance officer to take responsibility for coordinating the overall controls management process as it relates to the fulfillment of compliance obligations. This group may also formally interface with higher level managers for the purposes of reporting on the internal control system and the satisfaction of process goals as part of the governance process *(refer to CTRL:GG2.GP1)*.

2. Assign responsibility and authority for performing the specific tasks of the process.

   Elaboration:

   Responsibility and authority for performing controls management tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - including process tasks and responsibility for these tasks in specific job descriptions
   - identifying ownership of specific control objectives and controls in job descriptions
   - assigning staff to monitor and measure the internal control system

- developing policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
- including process tasks in staff performance management goals and objectives with requisite measurement of progress against these goals
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
- including process tasks in measuring performance of external entities against contractual instruments

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

CTRL:GG2.GP5 Train People

Train the people performing or supporting the controls management process as needed.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about inventorying skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

Elaboration:

These are examples of skills required in the controls management process:

- knowledge of the tools, techniques, and methods necessary to analyze, assess, and manage the internal control system, including those necessary to perform the process using the selected methods, techniques, and tools identified in CTRL:GG2.GP3 subpractice 3
- knowledge unique to each control objective
- knowledge necessary to successfully remediate control gaps, problem areas, redundancies, and conflicts
- knowledge necessary to work effectively with asset and service owners and custodians
- oral and written communication skills to prepare reports on the effectiveness of the internal control system and defend these reports if required
- knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective control objectives and controls

2. Identify process skill gaps based on available resources and their current skill levels.

3. Identify training opportunities to address skill gaps.

Elaboration:

These are examples of training topics:

- affinity analysis techniques
- control analysis and assessment methods
- survey and interview techniques
- specific training on management directives and guidelines
- managing and controlling changes to controls
- supporting asset and service owners and custodians in understanding the process and their roles and responsibilities with respect to its activities
- working with external entities that have responsibility for process activities
- using process methods, tools, and techniques, including those identified in CTRL:GG2:GP3 subpractice 3

4. Provide training and review the training needs as necessary.

CTRL:GG2.GP6 Control Work Products

Place designated work products of the controls management process under appropriate levels of control.

Elaboration:

These are examples of controls management work products placed under control:

- management directives and guidelines
- control objectives and their priorities
- enterprise-, service-, and asset-level controls
- traceability matrix of control objectives and controls, including responsible staff
- analysis and assessment results, including control gaps
- updates to existing controls
- proposed new controls
- redundant and conflicting controls
- risks related to unsatisfied control objectives
- risks related to redundant and conflicting controls
- remediation plans
- updates to service continuity plans
- process plan
- policies and procedures
- contracts with external entities

CTRL:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Subpractices

1. Identify process stakeholders and their appropriate involvement.

Elaboration:

Stakeholders of the controls management process include those that are responsible for control objectives and controls, oversee the controls management process, and are involved in any aspect of ensuring the effectiveness of the internal control system and managing risks resulting from unresolved problems.

Stakeholders of the compliance process are also stakeholders of the controls management process for controls that directly support compliance process activities and the fulfillment of compliance obligations.

These are examples of stakeholders of the controls management process:

- stakeholders of the compliance process for compliance obligations that are satisfied by controls
- organizational unit and line of business managers responsible for high-value assets and the services they support
- service owners
- asset owners and custodians
- staff responsible for developing, implementing, and managing an internal control system for assets and services
- higher level managers responsible for the organization's governance and oversight processes for the internal control system
- staff responsible for participating in decisions to not resolve control problem areas, including gaps in controls and ineffective, inefficient, missing, redundant, and conflicting controls
- external entities responsible for managing high-value services and assets and the controls associated with them
- staff involved in self-assessment
- internal and external auditors

Stakeholders are involved in various tasks in the controls management process, such as

- planning for the process
- making decisions about the process
- making commitments to the process plan and activities
- communicating the process plan and activities
- coordinating process activities
- satisfying compliance obligations that rely on controls
- reviewing and appraising the effectiveness of process activities
- establishing requirements for the process
- resolving issues and risks identified in the process

2. Communicate the list of stakeholders to planners and those responsible for process performance.
3. Involve relevant stakeholders in the process as planned.

CTRL:GG2.GP8 Measure and Control the Process

Measure and control the controls management process against the plan for performing the process and take appropriate corrective action.

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for measuring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

These are examples of metrics for the controls management process:

- confidence factor that control objectives from all relevant management directives and guidelines have been identified at the enterprise level
- confidence factor that control objectives from all relevant management directives and guidelines have been identified at the service level (perhaps by service type)
- confidence factor that control objectives from all relevant management directives and guidelines have been identified at the asset level (perhaps by asset type)
- percentage of control objectives that have been prioritized (should be 100%)
- percentage of enterprise-level controls for which responsibility has been confirmed or assigned
- percentage of enterprise-level controls that do not map to one or more control objectives
- percentage of service-level controls for which responsibility has been confirmed or assigned
- percentage of service-level controls that do not map to one or more control objectives
- percentage of asset-level controls for which responsibility has been confirmed or assigned
- percentage of asset-level controls that do not map to one or more control objectives
- percentage of control objectives that are fully satisfied by existing controls at the enterprise level
- percentage of control objectives that are fully satisfied by existing controls at the service level (perhaps by service type)
- percentage of control objectives that are fully satisfied by existing controls at the asset level (perhaps by asset type)

- percentage of controls that satisfy multiple control objectives (and mean, median number of control objectives satisfied)
- percentage of controls that require updates to address gaps (perhaps by control objective)
- percentage of control objectives that are affected by updated controls

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

   Elaboration:

   Reviews of the controls management process may result from periodic assessment or post-event audits that seek to identify problems that must be corrected. Elevating the results of these assessments and audits to managers provides an opportunity to correct controls management process deficiencies and to make managers aware of variations in the process that not only have localized impact but may also affect the organization’s resilience as a whole.

   Periodic reviews of the controls management process are needed to ensure that

   - control objectives are satisfied and continue to be satisfied across time and in the face of changing business and risk conditions
   - control problem areas have been identified and remediated
   - risks related to control problem areas have been identified, properly referred, and addressed
   - actions requiring management involvement are elevated in a timely manner
   - the performance of process activities is being monitored and regularly reported
   - key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
   - actions requiring management involvement are elevated in a timely manner
   - actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.
5. Identify problems in the plan for performing and executing the process.
6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.
7. Track corrective action to closure.

CTRL:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the controls management process against its process description, standards, and procedures, and address non-compliance.

Elaboration:

- These are examples of activities to be reviewed:
- establishing management directives and guidelines that serve as the basis for defining control objectives

- identifying and documenting control objectives
- satisfying control objectives
- identifying problem areas in controls (gaps, updates, need for new controls, remediation of redundant and conflicting controls)
- identifying risks and remediation plans arising from problem areas in controls
- the alignment of stakeholder requirements with the process plan
- assignment of responsibility, accountability, and authority for process activities
- determination of the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- use of process work products for improving strategies for protecting and sustaining assets and services

These are examples of work products to be reviewed:

- management directives and guidelines
- control objectives and their priorities
- assessment results
- risks resulting from problem areas in controls that have been referred to the risk management process
- remediation plans
- process plan and policies
- process methods, techniques, and tools
- metrics for the process *(Refer to CTRL:GG2.GP8 subpractice 2.)*
- contracts with external entities

CTRL:GG2.GP10 Review Status with Higher level Managers

Review the activities, status, and results of the controls management process with higher level managers and resolve issues.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management system.

CTRL:GG3 Institutionalize a Defined Process

Controls management is institutionalized as a defined process.

CTRL:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined controls management process.

Establishing and tailoring process assets, including standard processes, are addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, are addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization’s set of standard processes those processes that cover the controls management process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization’s tailoring guidelines.
3. Ensure that the organization’s process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

CTRL:GG3.GP2 Collect Improvement Information

Collect controls management work products, 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.

Elaboration:

These are examples of improvement work products and information:

- metrics and measurements of the viability of the process *(Refer to CTRL:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned from control analyses and assessments
- lessons learned from satisfying control objectives
- lessons learned in post-event review of continuity exercises, incidents, and disruptions in continuity
- lessons learned that can be applied to improve operational resilience management performance and controls, such as remediation plans and risks resulting from control problem areas
- resilience requirements that are not being satisfied or are being exceeded

Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process improvement and deployment is addressed in the Organizational Process Focus process area.

Subpractices

1. Store process and work product measures in the organization’s measurement repository.
2. Submit documentation for inclusion in the organization’s process asset library.

3. Document lessons learned from the process for inclusion in the organization’s process asset library.
4. Propose improvements to the organizational process assets.