Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Compliance (COMP)

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

February 2016

CERT Program
Unlimited distribution subject to the copyright.

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

Carnegie Mellon

Copyright 2016 Carnegie Mellon University

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.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0003234

COMPLIANCE

Enterprise

Purpose

The purpose of Compliance is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, and legislation, and other obligations (such as contracts and service level agreements) related to managing operational resilience.

Introductory Notes

Regulations, standards, and guidelines are developed and issued by a variety of governmental, regulatory, and industry bodies. Their purpose is to enforce (and reinforce) acceptable levels of behavior to ensure that organizations and the services they provide to citizens and customers remain viable and sustainable. In particular, the evolving importance of security and resilience has resulted in a new wave of regulatory bodies and regulations that seek not only to ensure organizational survivability but the survivability of entire industries and to limit undesirable events that have the potential to affect the socioeconomic structure of the global economy.

“Compliance” characterizes the activities that the organization performs to identify the internal and external guidelines, standards, practices, policies, regulations, and legislation to which it is subject and to comply with these obligations in an orderly, systematic, efficient, timely, and accurate manner. Compliance management addresses the policies and practices in the organization that support the satisfaction of compliance obligations as an enterprise-wide activity that involves more than just legal and administrative activities.

Organizations typically focus their efforts on compliance with externally directed obligations, but compliance processes also often address compliance with internally generated standards and policies such as the organization’s information security policy and internal control system. In addition, compliance is not only important for reinforcing appropriate behaviors; it is also a primary tool in governing the security and resilience activities in the organization and ensuring they are effectively meeting their goals and objectives.

The Compliance process area addresses the organization’s ability to establish a compliance plan and program, to identify relevant regulations, standards, and guidelines (to which it must comply), and to develop and implement the proper procedures and activities to ensure compliance in a timely and accurate manner. Compliance management requires the organization to understand its obligations and to collect relevant data in a manner that supports and enables the satisfaction of obligations in a way that meets the organization’s requirements but does not divert focus from its core service delivery.

Related Process Areas

A primary component of the compliance process—governance and oversight—is addressed in the Enterprise Focus process area.

Addressing the risks of non-compliance and the risks related to weaknesses identified in the compliance process is performed in the Risk Management process area.

The monitor process, which may provide information about the effectiveness of internal controls for compliance purposes, is addressed in the Monitoring process area.

Summary of Specific Goals and Practices

Goals	Practices
COMP:SG1 Prepare for Compliance Management	COMP:SG1.SP1 Establish a Compliance Plan
	COMP:SG1.SP2 Establish a Compliance Program
	COMP:SG1.SP3 Establish Compliance Guidelines and Standards
COMP:SG2 Establish Compliance Obligations	COMP:SG2.SP1 Identify Compliance Obligations
	COMP:SG2.SP2 Analyze Obligations
	COMP:SG2.SP3 Establish Ownership for Meeting Obligations
COMP:SG3 Demonstrate Satisfaction of Compliance Obligations	COMP:SG3.SP1 Collect and Validate Compliance Data
	COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction
	COMP:SG3.SP3 Remediate Areas of Non-Compliance
COMP:SG4 Monitor Compliance Activities	COMP:SG4.SP1 Evaluate Compliance Activities

Specific Practices by Goal

COMP:SG1 Prepare for Compliance Management

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

Many organizations and industries (both public and private) are highly regulated by government, their industry, or other agencies. In addition, as part of their governance structure, most organizations have their own internal regulations in the form of policies and procedures, as well as commitments to quality programs. Compliance with all of these obligations (many of which overlap) requires significant organizational resources and commitment. It can be a complex and time-consuming activity that results in duplication of effort and diverts resources away from meeting the organization's strategic objectives.

To be effective and efficient, compliance must be integrated with an organization's operational processes. Thus, regardless of the origins of compliance obligations, the organization is collecting, documenting, analyzing, coordinating, and reporting the data it needs for compliance as a natural outcome of operating its services. From a governance perspective, higher level managers must be able to be confident that compliance obligations have been satisfied, and where they have not, that the organization has good reason to be non-compliant based on a thorough examination of risk.

To achieve this, the organization must establish a foundation for managing compliance as an organization-wide process that emanates from its operational commitments. This

helps the organization avoid “fire-drill” compliance activities that pull resources from operational activities to collect data and fulfill obligations, and keeps the organization from realizing fines and penalties that could result from lack of compliance.

To establish a foundation for managing compliance, the organization must create a compliance plan and program and establish compliance standards and guidelines for consistency and repeatability.

COMP:SG1.SP1 Establish a Compliance Plan

A strategic plan for managing compliance to obligations is established.

The strategic plan for addressing compliance helps the organization to make organization-focused decisions about the most effective and efficient approach for meeting compliance obligations and for managing the activities required to meet these obligations. The plan is developed to minimize duplication of effort, facilitate compliance with diverse bodies of regulation, and provide maximum assurance that obligations will be met in a timely manner.

The plan establishes the basis for the development and implementation of the organization’s compliance program, which directs the compliance activities from an enterprise view and seeks to meet the broad compliance objectives of the plan.

Typical work products

1. Plan for compliance management
2. Documented requests for commitment to the plan
3. Resource commitments to the plan

Subpractices

1. Develop a strategic plan for managing compliance.

   A plan for compliance management should address at a minimum

   - the organization’s stated approach to compliance management
   - objectives for the organization’s compliance program
   - the roles and responsibilities for carrying out the compliance plan
   - resources that will be required to meet the objectives of the plan
   - applicable training needs and requirements
   - relevant costs and budgets associated with carrying out the plan

2. Establish sponsorship and resource commitments for the compliance plan.
3. Revise the plan and commitments on a cycle commensurate with the organization’s strategic planning process.

COMP:SG1.SP2 Establish a Compliance Program

A program is established to carry out the activities and practices of the compliance plan.

The organization's compliance program is established to carry out the compliance plan. The program establishes the tasks, functions, and activities that are performed to ensure that compliance is managed as envisioned in the plan.

In the compliance program, the organization states the structure and processes it will use to meet the compliance objectives (as stated in the compliance plan) and outlines the roles and responsibilities of staff throughout the organization for their contributions to compliance activities. In many cases, the compliance program includes the definition and installation of a "compliance office" that assumes the responsibility for compliance activities, but this may vary widely across organizations and industries.

Another important element of the compliance program is the formal connection to the organization's governance and oversight functions. In the area of resilience management, the compliance program seeks to relay information about lack of compliance to the governance function so that appropriate organizational actions can be commenced. Some organizations seek to formalize this role by the establishment of a higher level compliance officer position.

The compliance program may call for centralized management or may be decentralized into organizational units and lines of business. The decision on how to structure the compliance program is made by the organization depending on its organizational structure, the extensiveness of its compliance obligations, and other factors (such as technical infrastructure).

Typical work products

1. Compliance program charter
2. Compliance program management plan
3. Compliance program objectives
4. Compliance organizational structure

Subpractices

1. Establish a compliance program.

   The compliance program is responsible for ensuring that the objectives of the compliance plan are achieved. Program management includes staffing the program, assigning accountability and responsibility to plan activities, tasks, and projects, and measuring performance. Much of what is included in the Compliance process area is expected to be carried out through the direction of the organization's compliance program.

   The compliance program should address

   - a compliance program charter that addresses the objectives of the compliance plan

- the establishment of a compliance office or similar construct
- the structure of the compliance program
- the roles and responsibilities for carrying out the compliance program, including the establishment of the compliance officer role if warranted
- procedures for identifying compliance obligations
- procedures for data collection, analysis, and reporting
- compliance standards and guidelines
- reporting mechanisms to receive complaints
- procedures for response to improper activities
- monitoring, auditing, and other evaluation techniques to identify problem areas
- investigation procedures
- enforcement process to take appropriate corrective action for violations of compliance obligations
- remediation procedures
- the selection and use of tools for data collection and analysis
- the selection and use of tools for reducing redundancy in duplicative obligations

2. Assign resources to the compliance program.

   Resources are required to perform the activities of the compliance program. Staffing for the compliance program, depending on its size and complexity, may be virtual (i.e., spread throughout the organization) or dedicated (program-specific staff). Depending on complexity, compliance program activities may have to be pushed out into the organization, and the organization may have to implement automated means (i.e., software-based tools and programs) to collect data, analyze overlap of obligations, and coordinate activities across many organizational units and lines of business.

3. Provide funding for the compliance program.

   Funding the organization's operational resilience management system and related activities, tasks, and projects is addressed in the Financial Resource Management process area.

4. Provide sponsorship and oversight to the compliance program.

   As an increasingly critical organizational entity, the compliance program must be viewed as the responsibility of all staff and managed so that compliance objectives are met consistently. Sponsorship provides the support for the importance of the program, and oversight ensures that compliance issues are identified and addressed on a timely basis. This may be the role of the compliance officer if that position is established.

COMP:SG1.SP3 Establish Compliance Guidelines and Standards

The guidelines and standards for satisfying compliance obligations are established and communicated.

Guidelines and standards for compliance activities ensure consistent levels of data collection, formatting, analysis, reporting, quality, and performance management. They also provide a foundation from which a common understanding of compliance can be communicated as a means for improving efficiency and effectiveness in meeting compliance obligations satisfactorily. Guidelines and standards also facilitate an enterprise view of compliance and an ability to manage compliance activities in alignment with strategic objectives.

In addition, guidelines and standards for compliance provide a basis for performing compliance activities that must be coordinated with suppliers and vendors.

Typical work products

1. Compliance guidelines and standards

Subpractices

1. Develop and communicate compliance guidelines and standards.

   Guidelines and standards for compliance management are typically organization-specific. However, guidelines and standards may address areas such as

   - formats and methods for collecting and coordinating data
   - formats for preparing and submitting compliance reports
   - remediation standards—documentation, approvals, reporting, follow-up, etc.
   - tool evaluation, acquisition, installation, and use
   - data retention, storage, and access control
   - requirements for identification and documentation of risks related to non-compliance
   - requirements and formats for inclusion of compliance requirements in external entity contracts

COMP:SG2 Establish Compliance Obligations

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

The foundation of efficient and effective compliance management is an understanding of the organization's compliance obligations. Otherwise, the organization cannot effectively design a compliance plan and program that specifically address its unique needs and support the organization's timely satisfaction of these obligations. An inventory of compliance obligations ensures that all staff who are responsible for compliance activities are aware of the range of organizational obligations. This also avoids the potential for surprise obligations that the organization has not planned for or has not considered in its compliance plans and program.

COMP:SG2.SP1 Identify Compliance Obligations

Compliance obligations are identified and documented.

Compliance obligations for the organization come from several sources:

- federal, state, and local governments
- foreign governments and trade associations
- industry associations and groups
- external codes of practice
- internal policies, procedures, and guidelines
- quality and process improvement certifications
- contracts and agreements with external entities such as suppliers and vendors

Compliance obligations from these (and other organization-defined) sources form the basis for the extent and scope of the activities the organization must perform to satisfy these obligations. Identification of compliance obligations not only gives the organization a starting point for improving the compliance process, but it also provides a basis for analyzing the overlap of compliance obligations, which ultimately helps the organization to streamline and simplify compliance activities.

An inventory of compliance obligations also provides a baseline from which new obligations can be identified and integrated into the organization's compliance processes. This helps the organization to avoid surprises that may render the compliance process ineffective and force the organization to resort to ad hoc practices as it must become familiar with and satisfy new obligations.

These are examples of compliance obligations:

- the organization's internal policies and procedures, including the information security policy, policy on sexual harassment, ethics policy, and other human resources and workforce directives
- internal agreements, including non-disclosure agreements, confidentiality agreements, and non-compete agreements
- industry-specific obligations, such as
  - Gramm-Leach-Bliley Act (GLBA)
  - European Union Data Protection Directive (EUDPD)
  - FERC regulations
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Family Educational Rights and Privacy Act (FERPA)
  - Basel Accords
  - Patriot Act
- general obligations affecting many organizations, such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA)
- compliance obligations related to retaining certifications, such as ISO 9000, CMMI, and ITIL
- contracts and agreements with external entities such as suppliers

Typical work products

1. Sources of compliance obligations
2. Inventory of compliance obligations

Subpractices

1. Interview service owners, auditors, and legal staff to identify compliance obligations.
2. Identify compliance obligations that the organization may have to satisfy because of its external entity affiliations.

   By virtue of its association with external entities, the organization may inherit obligations as part of its contractual relationship. These obligations must be identified so that the organization places them in its scope for compliance management and so that it does not incur fines and penalties as a result of non-compliance.

3. Identify internal policies and procedures that should be included in the inventory of compliance obligations.

   Internal compliance obligations can represent the policies, procedures, standards, and guidelines that the organization establishes to promote acceptable behaviors, ethics, and practices. These obligations can be as important to the organization as those that are levied by outside agencies and thus should be included in the compliance management process.

4. Identify sources of potential new compliance obligations.

   Sources of information for potential compliance obligations include
   - compliance journals and mailing lists
   - trade associations
   - professional associations such as ISACA, ISSA, DRII, ITIL user groups, IIA, and RMA
   - industry trade shows
   - internal departments such as audit, legal, and risk management

5. Develop an inventory of compliance obligations.

   This inventory serves as the basis for the organization's compliance management program. The obligations should be identified and documented. Information about each obligation such as the following should be captured:

   - source of the obligation (internal department, vendor contract, internal policies and procedures)
   - requirements of the obligation (the specifics regarding what needs to be complied with)
   - obligation categorization (data privacy and security, risk, etc.)
   - organizational unit or line of business that owns the obligation
   - time parameters for satisfying the obligation (e.g., due dates and requirements for recertification of results)

- standards and guidelines for compliance (e.g., how the organization must report data)
- known information about fines and penalties that may be levied for non-reporting or for lack of compliance

COMP:SG2.SP2 Analyze Obligations

Compliance obligations are analyzed and organized to facilitate satisfaction.

Detailed analysis is needed to help the organization to avoid duplication in its efforts to satisfy diverse obligations that have similar requirements. For example, a governmental agency and an industry body may both require categorization and protection of a certain type of data (such as health care records), and because of the similarity of the requirements, the organization could satisfy both obligations through fewer, less redundant activities.

The organization can perform analysis on compliance obligations in many ways. As a simple activity, the organization can use affinity analysis, in which similar obligations are mapped into categories based on the nature, type, and extent of their requirements. Regardless of the technique used, the objective is to group the requirements of compliance obligations in a way that makes efficient use of the organization's compliance processes, especially data collection and analysis, which can be time-consuming and tedious.

Typical work products

1. Analysis results
2. Mapping or categorization of similar compliance obligations
3. List of conflicting obligations

Subpractices

1. Establish a technique for performing analysis on compliance obligations.

   The technique should allow the organization to establish categories of obligations and requirements (such as privacy and data security) and use these categories to map obligations from their sources. The organization should be able to integrate the categories with its compliance data collection and analysis processes.

2. Analyze compliance obligations and document results.

   These results form the foundation for the organization's compliance activities. They also allow the organization to prioritize obligations for satisfaction.

3. Identify conflicting obligations.

   In some cases, analysis will reveal compliance obligations and requirements that conflict. By identifying these requirements early, the organization can perform additional review and analysis to determine the most effective strategy for satisfaction.

COMP:SG2.SP3 Establish Ownership for Meeting Obligations

The responsibility for satisfying compliance obligations is established.

Establishing ownership for satisfying compliance obligations is a way to ensure that these obligations are known, accepted, and planned for. When ownership is established, compliance activities may be integrated into the day-to-day operational activities of owners because they are aware of their responsibilities and can address them in the course of normal business. In addition, owners can ensure that the compliance obligations for which they are responsible are also reflected in the resilience requirements for the high-value assets and services under their control. Reflecting compliance obligations in resilience requirements ensures that they are considered in controls that the organization implements and manages for protecting and sustaining assets and services. In this way, the organization "embeds" compliance controls into services and may even provide for streamlined testing and reporting on these controls as part of satisfying compliance obligations.

Typically, ownership may be defined in the organization's compliance plan and program (as established in COMP:SG1.SP1 and COMPSG1.SP2) and it may be included in the documentation of compliance obligations (as established in COMP:SG2.SP1). However, additional resources throughout the organization may have to be identified and assigned to compliance activities and tasks.

Typical work products

1. Designated compliance roles
2. Updated inventory of compliance obligations
3. List of unassigned compliance obligations

Subpractices

1. Establish the owner for each compliance obligation.

   Ownership may be assigned either to a specific compliance obligation or to a category of obligations (as defined through analysis). The owner of the obligation must confirm acceptance of the obligation and the responsibility for satisfaction. Including these tasks in job responsibilities and performance management activities may further enforce this responsibility.

2. Establish training requirements for compliance roles, if necessary.
3. Identify compliance obligations that have not been assigned or accepted.

   Compliance obligations that have not been assigned pose a risk to the organization that the obligations will not be satisfied, possibly resulting in fines, legal penalties, or even damage to reputation.

COMP:SG3 Demonstrate Satisfaction of Compliance Obligations

The organization demonstrates that its compliance obligations are being satisfied.

Demonstrating that compliance obligations are satisfied is a process that begins with data collection and includes activities for data validation, formatting, and reporting (disclosure). The organization collects the data necessary to "prove" that it is meeting compliance obligations, formats this data according to the requirements of the obligation, and reports it to satisfy the obligation. However, for the organization, this is not the end of the compliance process. In some cases, the organization may not be able to comply and may have to commence remediation processes that will ensure it complies within an acceptable time frame.

COMP:SG3.SP1 Collect and Validate Compliance Data

Data required to satisfy compliance obligations is collected and validated.

Data collection and validation are often the most time-consuming tasks in meeting compliance obligations. The effectiveness of data collection significantly affects the organization's ability to demonstrate that it meets obligations in a timely and high-quality manner. Challenges in data collection can include inconsistency, poor quality, lack of ability to verify, lack of integrity, and lack of repeatability of data collection processes.

In many cases, data collection is not as simple as data accumulation. For example, control testing may have to be done in order to verify compliance, after which data on compliance is accumulated, formatted, and reported. When designing data collection processes, the organization must thoroughly understand its compliance obligations so that the antecedent processes (such as control testing) can be incorporated and addressed.

Data collection also extends to storage and retrieval processes. The data collected for compliance purposes can be organizationally sensitive, and the resulting compliance reports (including cases of non-compliance) may be harmful to the organization. As part of data collection and validation, the organization must consider storage and retrieval processes that are commensurate with the level of sensitivity of the data being collected and reported.

Because compliance is a cyclical activity, the organization should implement an appropriate infrastructure to support repeatability of compliance activities. As related to data, this infrastructure should allow for ease of data accumulation, inquiry, analysis, and reporting, as well as provide for the implementation and management of access controls to ensure appropriate handling of compliance data.

Typical work products

1. List of key controls and process control points
2. Data collection strategy (by obligation)
3. Data quality criteria

4. Compliance knowledgebase
5. Policies for appropriate handling of compliance data

Subpractices

1. Develop strategies for data collection and validation.

   These strategies should be commensurate with the compliance obligations and the structure of the organization and must take into consideration that data collection may be pushed out to lower levels of the organization. In addition, the strategy should address issues related to data collection, storage, and retrieval infrastructure to facilitate these processes.

2. Establish compliance knowledgebase or information repository.

   A common accessible repository for compliance data provides a mechanism to ensure that all staff involved in compliance processes have access to data that is accurate, complete, and timely. It also allows the organization to enforce access control policies for appropriate handling of compliance data.

   The repository may include documentation of the compliance obligations and their owners and due dates, the results of compliance and substantive testing of controls, compliance targets and metrics, compliance reports, non-compliance reports, remediation plans, and tracking data to provide status on satisfying compliance obligations.

   The data in the information repository may be arranged by category of compliance obligation or by other categories such as key control points.

3. Implement processes for data validation and integrity checking.

   Data that is accumulated and collected in the information repository is not necessarily ready for analysis or disposition. The organization must develop processes for data validation and integrity checking to ensure that compliance data is accurate, complete, and timely. The processes should establish data quality criteria and track the quality of compliance documentation.

   Fundamental qualities of data include

   - accuracy
   - integrity
   - standards
   - consistency
   - completeness
   - timeliness
   - accessibility or availability
   - usability
   - auditability

COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction

The extent to which compliance obligations are satisfied is demonstrated through compliance activities.

Demonstrating that compliance obligations are satisfied, or that remediation actions are required, goes beyond simply preparing and submitting compliance reports. The organization must address non-compliance issues (such as identifying associated risk and relevant costs) by establishing activities that interface with the organization's governance process and determine areas that may need remediation to meet compliance obligations.

The organization must also gather data related to the efficiency and effectiveness of the compliance process in order to identify areas that must be improved.

Typical work products

1. Minimum requirements for compliance
2. List of compliance stakeholders
3. Compliance reports
4. Required remediation actions
5. List of risks and potential costs related to areas of non-compliance
6. Compliance knowledgebase

Subpractices

1. Establish minimum requirements for compliance.

   The organization should specify the minimum requirements for an adequate level of compliance using the guidelines and standards identified in COMP:SG1.SP3 subpractice 1.

2. Determine the stakeholders of the compliance reports and data.

   The stakeholders that will be the recipients of compliance information should be identified, as well as those that will have to be notified of non-compliance.

   One of the primary stakeholders for compliance data is the organization's governance and oversight processes.

3. Prepare and submit compliance reports as necessary.

   If the organization has to disclose that it is not in compliance, it should have processes to address the potential resulting fallout. This may require public relations campaigns, notification of risk and financial managers, and other actions. The organization may also need to notify its customers or vendors, business partners, and suppliers.

   Situations of non-compliance or the need for remediation as a result of non-compliance should also be referred to the organization's governance process.

   Public relations and other communications processes are addressed in the Communications process area.

   Governance and oversight processes are addressed in the Enterprise Focus process area.

4. Track progress against compliance obligations and identify obligations that may not be met on time.

   Obligations that will not be met should be reported to appropriate stakeholders on a timely basis. These instances may pose additional risk to the organization.

5. Identify risks and potential costs of non-compliance.

   In some cases the organization may consider not complying with certain obligations. In these cases, the organization should determine and thoroughly analyze the risks associated with non-compliance in advance of a decision not to comply and report these risks to appropriate stakeholders.

   These are examples of risks of non-compliance:

   - significant fines
   - potential imprisonment
   - damage to the organization's reputation
   - loss of trust from customers or suppliers
   - legal action or lawsuits

   The identification of risks should also include risks related to weaknesses that resulted in the inability to satisfy compliance obligations. (Such weaknesses typically are identified as areas requiring remediation.)

   There may also be costs to the organization associated with non-compliance. These costs should be itemized and presented to appropriate stakeholders in advance of a decision not to comply.

   These are examples of costs of non-compliance:

   - productivity loss
   - reputation damage and resulting loss in sales or revenue
   - forensic investigation fees
   - costs of notifying victims in the event of a privacy or security breach
   - remediation costs
   - fines and penalties
   - legal costs associated with non-compliance, and lawsuits resulting from non-compliance

   These risks and costs may also have to be reported through the organization's governance process to obtain input from oversight committees.

   If the organization decides that non-compliance is the best course of action, the decision should be documented, along with a detailed description of the risks associated with non-compliance and the organization's plan to address those risks. The decision should also be appropriately approved by management and reviewed in the organization's governance process.

   All risks should be referred to the organization's formal risk management process as outlined in the Risk Management process area.

6. Identify areas that may need remediation for compliance purposes.

   One of the objectives of the compliance process is to identify areas where the organization is not performing as expected, whether measured against external regulations and laws or internally generated policies and procedures. As a result of going through the compliance process, the organization may learn of areas that need attention, particularly if they are keeping the organization from complying. These areas may require the creation of detailed remediation plans and strategies so that compliance can be achieved.

   For example, if the organization is required to protect health care records and finds that the proper access controls are not in place to meet this requirement, an area of remediation is created.

   Areas of remediation may be reported directly by staff or others associated with the organization. This reporting may occur through ethics hotlines or other anonymous methods or on employees' yearly code of ethics reports.

   Activities related to the development and tracking of remediation plans are addressed in COMP:SG3.SP3.

7. Gather performance data on the achievement of compliance obligations.

   Actual data regarding compliance (date of submission of compliance reports, effort expended on compliance activities, etc.) should be recorded in the compliance knowledgebase for use in improving compliance processes.

COMP:SG3.SP3 Remediate Areas of Non-Compliance

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

Areas of non-compliance are deficiencies in practices, processes, and procedures that not only affect the organization's ability to satisfy compliance obligations but may indicate serious weaknesses in the organization's internal control system and governance structure. As part of the organization's formal risk management process, these areas must be identified, analyzed, and addressed (typically through remediation plans) to ensure satisfaction of compliance obligations and to improve the organization's operational resilience by addressing weaknesses that can result in disruptions.

Typical work products

1. Required remediation actions
2. Remediation plans and strategies

Subpractices

1. Analyze areas of suggested remediation and develop detailed remediation plans.

   Analysis includes determining the activities that must be performed to bring the organization into compliance, as well as to identify associated operational risks and develop dispositions for them.

Remediation plans should address

- the actions the organization must take to satisfy obligations
- changes to the internal control system
- assignment of responsibility and authority to perform the work
- relevant time considerations (i.e., deadlines)
- relevant costs associated with the actions
- documentation of any decisions related to non-compliance and risk

2. Assign resources to perform remediation.

   Assign accountability and responsibility to carry out remediation plans.

4. Track remediation activities to completion.

5. Assess remediation activities to determine if satisfaction of compliance obligations has been performed.

   The organization should verify that remediation activities result in satisfaction of compliance obligations. If they don't, the organization should develop additional actions to remedy any gaps.

6. Update satisfaction of compliance obligations (as a result of remediation), if appropriate.

   In addition to communication with stakeholders and submission of compliance reports, this may include notification of oversight committees and the governance process that appropriate actions have been taken.

COMP:SG4 Monitor Compliance Activities

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

Continuous improvement in the compliance process reduces the type and extent of resources that the organization must devote to compliance-related activities. Because there is often a trade-off between compliance activities and those that contribute directly to accomplishing the organization's mission, the ability to make the compliance process more efficient results in less disruption to services and reduces the extent to which the organization is drawn off course to meet its compliance obligations.

COMP:SG4.SP1 Evaluate Compliance Activities

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

Objective and independent evaluation of the organization's compliance process is a means for obtaining critical information about the efficiency and effectiveness of the organization's compliance activities. In addition, and perhaps more important, it is a means for the organization to evaluate the effectiveness of the internal control system in meeting compliance obligations. Internal controls are often expensive to implement and operate in production. Reducing the number and extent of internal controls while maintaining the ability to meet compliance obligations is a way that

improvement in the compliance process can translate to direct cost savings and efficiency for the organization.

The organization can employ a number of assessment methods with increasing levels of efficacy. Objective and independent evaluations are most desirable, but the organization may also want to implement a self-assessment capability to allow improvement at the lowest levels of the organization. Audits, as commissioned through the governance and oversight processes, are typically the most objective and independent measure of the organization's compliance processes and satisfaction of compliance obligations; however, evidence from these activities can be damaging to the organization, particularly if the audits are performed by external auditors or agencies.

In some cases, the organization may invest in monitoring processes that collect and accumulate data at the control level. This can be an efficient way of not only providing data for satisfying compliance obligations but also facilitating the evaluation process by providing a more continuous examination of the efficacy of the controls.

The ongoing compliance process can be costly and time-consuming to an organization. The extent to which the organization learns to make these processes more efficient and repeatable significantly affects their overall impact on the organization's resources.

There are many areas that can be improved in the compliance process, such as

- data collection, accumulation, and analysis
- consolidation and coordination of obligations (collect data once, comply many times)
- standards and guidelines for compliance
- improvements in the organization's internal control system (which would improve ability to comply in the future)

Typical work products

1. Evaluation methods
2. Evaluation reports

Subpractices

1. Establish and maintain clearly stated criteria for evaluations.

   Criteria for evaluations should address

   - what will be evaluated
   - when or how often a process will be evaluated
   - how the evaluation will be conducted
   - who must be involved in the evaluation

2. Evaluate compliance processes for adherence to compliance standards and guidelines and for meeting compliance obligations using the stated criteria.

3. Identify deficiencies and areas for improvement, particularly where the satisfaction of compliance obligations has been impaired.

   The deficiencies identified can be related to the efficacy of the compliance process or the efficacy of internal controls in meeting the objectives of the compliance obligations.

3. Identify and apply lessons learned that could improve the organization's compliance process.

   This practice may result in the reduction and/or elimination of overlapping and redundant controls, identification of areas where compliance activities can be automated, and overall improvements in the organization's approach to compliance. Cost data may be collected in the evaluation process that the organization can use to determine if it is complying with obligations at the lowest possible cost.

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 Compliance process area.

COMP:GG1 Achieve Specific Goals

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

COMP:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices COMP:SG1.SP1 through COMP:SG4.SP1 are performed to achieve the goals of the compliance process.

COMP:GG2 Institutionalize a Managed Process

Compliance is institutionalized as a managed process.

COMP:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

Elaboration:

Governance over the compliance process may be exhibited by

- developing and publicizing higher level managers' objectives and charter for the process
- establishing a higher level compliance officer position to provide direct oversight of the process and to interface with higher level managers
- sponsoring process policies, procedures, standards, and guidelines, including submitting compliance reports and remediating areas of non-compliance
- sponsoring and providing oversight over the organization's compliance plan and program
- regular reporting from organizational units to higher level managers on process activities and results
- making higher level managers aware of applicable compliance obligations, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
- sponsoring and funding process activities
- aligning compliance obligations and the controls that satisfy these 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 compliance and recommendations for improving the process
- providing inputs on identifying, assessing, and managing risks due to non-compliance
- conducting regular internal and external audits and related reporting to audit committees on compliance issues, failures to meet compliance obligations, and 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 compliance management policy should address

- responsibility, authority, and ownership for performing process activities, including the identification of all compliance obligations and the remediation action for areas that are non-compliant
- procedures, standards, and guidelines for
  - collecting and formatting data
  - data sufficiency and validation
  - approvals and approval processes
  - preparing and submitting compliance reports
  - tool evaluation and acquisition
  - remediation for non-compliance
  - data retention and access control

- the identification and analysis of compliance obligations
- appropriate handling of compliance data
- monitoring the status of compliance obligations
- methods for measuring adherence to policy, exceptions granted, and policy violations

COMP:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the compliance process.

Elaboration:

Specific practice COMP:SG1.SP1 requires a plan for managing compliance obligations for operational resilience. Specific practice COMP:SG1.SP2 calls for establishing a compliance charter and program based on the plan.

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.

COMP:GG2.GP3 Provide Resources

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

Elaboration:

Specific practices COMP:SG1.SP1 and COMP:SG1.SP2 require the assignment of resources to the compliance plan and program.

Subpractices

1. Staff the process.

   Elaboration:

   Because compliance is an activity that is typically shared across the organization and is often an extension of job responsibilities, the assignment of human resources to carrying out the compliance plan and program may be virtual and temporal. However, the organization may have resources dedicated to specific types of compliance activities (such as compliance with Sarbanes-Oxley requirements) or who are assigned to manage the overall compliance program and plan (such as a compliance officer); in these cases, compliance activities may compose the majority of their job responsibilities.

   These are examples of staff required to perform the compliance process:

   - staff responsible for
     - developing the compliance plan and program and the process plan and ensuring they are aligned with stakeholder requirements and needs

  - carrying out and meeting the objectives of the compliance plan and process plan
  - defining compliance standards, guidelines, and procedures, including the identification of compliance obligations and data collection, analysis, and reporting approaches for these obligations
  - implementing compliance standards, guidelines, and procedures, including implementing automated means to collect, analyze, validate, and report compliance data
  - coordinating process activities across organizational units and lines of business
  - remediating obligations that are in non-compliance, including obligation owners
  - managing external entities that have contractual obligations for process activities
- owners responsible for satisfying compliance obligations
- a compliance officer responsible for all compliance activities, if one is called for in the plan
- owners and custodians of high-value services and assets that support the accomplishment of operational resilience and compliance objectives
- internal and external auditors responsible for reporting to appropriate committees on the satisfaction of compliance obligations 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.

Considerations for funding the compliance process should extend beyond the initial development of the compliance knowledgebase or information repository to the maintenance of the knowledgebase. Initial costs may be higher if the organization does not have a formal or usable baseline of identified compliance obligations to serve as a foundation.

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

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

Elaboration:

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

- evaluation methods for tools acquired to support process activities
- compliance database management system, knowledgebase, or information repository
- techniques and tools for developing and maintaining traceability between the sources of compliance obligations and compliance plans, programs, and obligation owners (includes establishing categories of obligations and requirements)
- methods, techniques, and tools for coordinating process activities across organizational units and lines of business

- tools for enforcing compliance reporting formats and for compliance reporting
- methods, techniques, and tools for compliance evaluation and self-assessment
- methods, techniques, and tools for collecting, analyzing, validating, and managing compliance data
- tools for reducing redundancy in duplicative obligations
- monitoring, auditing, and other evaluation techniques to identify problem areas
- methods and tools for managing changes to compliance data
- methods and tools for compliance data retention, storage, and access control
- methods such as ethics hotlines and other anonymous methods for staff who are concerned about areas of potential non-compliance

COMP:GG2.GP4 Assign Responsibility

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

Elaboration:

Specific practices COMP:SG1.SP1 and COMP:SG1.SP2 require the assignment of roles and responsibilities for carrying out the compliance plan and program. Ownership of compliance obligations is specifically assigned in COMP:SG2.SP3 so that the responsibility and authority for meeting all relevant compliance obligations are established.

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 establish a compliance group or a compliance process group led by a compliance officer to take responsibility for coordinating the overall compliance process. This group may also formally interface with higher level managers for the purposes of reporting on organizational progress against compliance obligations and process goals as part of the governance process.

   However, on a tactical level, meeting compliance obligations typically involves organizational unit staff and those who have been established as the owners of compliance obligations.

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

   Elaboration:

   Responsibility and authority for performing compliance 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 compliance obligation ownership in job descriptions
- assigning staff to compliance program management activities
- 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.

COMP:GG2.GP5 Train People

Train the people performing or supporting the compliance 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 compliance process:

   - knowledge of the tools, techniques, and methods necessary to identify, analyze, and report on the fulfillment of compliance obligations, including those necessary to perform the process using the selected methods, techniques, and tools identified in COMP:GG2.GP3 subpractice 3
   - knowledge unique to each source of compliance obligations
   - knowledge necessary to successfully remediate areas of non-compliance
   - knowledge necessary to work effectively with asset and service owners and custodians
   - oral and written communications skills to prepare compliance reports and defend these reports if required with regulatory bodies
   - knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective compliance obligations, plans, and programs

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

Elaboration:

Because staff involved in the compliance process may perform these activities on an ad hoc basis as part of their job responsibilities, it cannot be assumed that they possess the necessary skills for collecting data, organizing and analyzing it, and preparing reports.

3. Identify training opportunities to address skill gaps.

Elaboration:

Certification and training are effective ways to improve compliance skills and attain competency. Education in specialized standards or regulations that necessitate compliance activities is useful, as is generalized training in procedures designed to audit compliance activities. Certification is often available for standards bodies and codes of practice, which requires participants to demonstrate understanding of the related body of knowledge.

These are examples of training topics:

- data collection, analysis, and validation
- data mapping and affinity analysis techniques
- compliance reporting
- key compliance controls
- compliance evaluation methods
- specific training on compliance sources, obligations, guidelines, and standards
- managing and controlling changes to the compliance obligation inventory, knowledgebase, and information repository
- 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 methods, tools, and techniques, including those identified in COMP:GG2:GP3 subpractice 3

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

COMP:GG2.GP6 Control Work Products

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

Elaboration:

Work products of the compliance process (such as the compliance process plan and compliance process policies) must be managed and controlled. The organization may also include work products such as compliance reports that may require strict version control to ensure that only the "approved" version is remitted to compliance bodies and regulators.

Tools, techniques, and methods used to capture and maintain the compliance obligations inventory, knowledgebase, and information repository should be employed to perform consistent and structured version control over these work products to ensure that the information is current, accurate, and "official." The tools, techniques, and methods can also be used to securely store these work products, to provide access control over

inquiry, modification, and deletion, and to track version changes and updates.

These are examples of compliance work products placed under control:

- plans, program plans, program charters, process plan, procedures, and policies
- guidelines and standards
- obligations, including sources of obligations
- obligation inventory, mapping, and categorization
- obligation roles and owners
- data, including collection strategy and quality criteria
- knowledgebase or information repository
- evaluation criteria, methods, and reports
- list of stakeholders
- remediation risks
- required remediation actions, plans, and strategies
- contracts with external entities

COMP:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Elaboration:

Many COMP-specific practices address the involvement of stakeholders in the compliance process. For example, specific practice COMP:SG2.SP3 addresses the identification of stakeholders as owners responsible for compliance obligations. Specific practice COMP:SG3.SP2 identifies stakeholders that will receive compliance reports and data, including areas of non-compliance and the risks associated with them.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   Stakeholders of the compliance process include those that own compliance obligations (are responsible for identifying and meeting compliance obligations), oversee the compliance process, and are involved in any aspect of compliance (data collection, reporting, etc.).

   The constituents that establish compliance obligations (i.e., governing bodies or industry organizations that issue regulations, laws, etc.) may also be considered stakeholders of the organization's plan for the compliance process because they are recipients of compliance information and ultimately decide whether compliance obligations have been met.

   These are examples of stakeholders of the compliance process:

   - regulators, governing bodies, and agencies that establish sources of compliance obligations
   - asset owners and custodians
   - service owners

- organizational unit and line of business managers responsible for high-value assets and the services they support
- 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 including oversight committees
- staff responsible for participating in decisions to not comply with certain obligations
- external entities responsible for managing high-value assets
- staff involved in self-assessment
- internal and external auditors

Stakeholders are involved in various tasks in the compliance process, such as

- planning for the process
- making decisions about the process
- making commitments to compliance plans and activities and to the process plan
- communicating compliance plans and activities
- coordinating process activities
- satisfying compliance obligations
- reviewing and appraising the effectiveness of process activities
- establishing requirements for the process
- resolving issues in the process, including participating in decisions regarding non-compliance and evaluating the costs and risks associated with such decisions

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

COMP:GG2.GP8 Measure and Control the Process

Measure and control the compliance 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 compliance process:

- time expended to gather, organize, analyze, and report data for compliance obligations
- percentage of compliance obligation data collection activities that are/are not automated
- number of compliance obligations (may require some prioritization of obligations such as high, medium, low)
- percentage of compliance obligations that have been inventoried
- percentage of compliance obligations with/without a designated owner (organizational unit, line of business)
- number of external entities with agreements to meet compliance obligations
- percentage of compliance obligations that rely upon external dependencies
- percentage of compliance obligations that rely upon external entities
- percentage of compliance obligations that are not met
- percentage of compliance obligations not met by deadline
- percentage of compliance activities that do not meet standards and guidelines
- percentage of controls required solely to meet compliance obligations
- percentage of service continuity guidelines and standards that are more/less stringent than required to meet compliance obligations
- number of compliance risks (exceptions, non-compliance, remediation) referred to key stakeholders (the risk management process, the organization's governance process, etc.)
- percentage of compliance obligation violations requiring corrective action for which such action has not been taken as scheduled
- percentage of compliance obligations that are conflicting (could also include duplicates, redundancies, and overlaps, but conflicts are likely of greatest interest)
- percentage of compliance obligations requiring remediation for which the remediation action results in the obligation being met
- cost to satisfy compliance obligations
- costs of non-compliance, including amount of fines and penalties levied for non-reporting and amount of fines and penalties levied for non-compliance
- number of deficiencies in the compliance process that directly resulted in compliance obligations not being met
- number of deficiencies in internal controls that directly resulted in compliance obligations not being met
- number of errors in the compliance process caused by inaccurate or unavailable data

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

Elaboration:

Periodic reviews of the compliance process are needed to ensure that

- relevant obligations have been identified and communicated
- data has been collected, analyzed, and validated

- data residing in obligation inventories, knowledgebases, and information repositories is subject to change management and has been properly validated
- obligations have been satisfied
- areas of non-compliance have been identified and remediated or referred to decision makers for disposition
- risks related to non-compliance have been identified, properly referred, and addressed

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.

   Elaboration:

   Deviations from the compliance plan may occur because compliance obligations vary widely, and thus the satisfaction of these obligations may require process deviations. The organization must determine if the deviations are appropriate given the compliance obligations and whether the deviation will result in an impact on operational resilience. Deviations that occur due to differences between the enterprise view of compliance and the activities performed at the organizational unit level may be less significant to the overall process but should be reviewed to ensure that the intent of the enterprise process is preserved.

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.

COMP:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- identifying and documenting compliance obligations
- collecting, analyzing, and validating compliance data
- satisfying compliance obligations
- identifying areas of non-compliance
- identifying risks related to non-compliance
- the alignment of stakeholder requirements with process plans and programs
- assignment of responsibility, accountability, and authority for process activities
- determination of the adequacy of compliance reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- verification of compliance controls
- use of compliance process work products for improving strategies for protecting and sustaining assets and services

These are examples of work products to be reviewed:

- process plans, programs, charters, and policies
- obligations and their status
- remediation and non-compliance issues that have been referred to the risk management process
- compliance reports
- compliance methods, techniques, and tools
- metrics for the process *(Refer to COMP:GG2.GP8 subpractice 2.)*
- contracts with external entities

COMP:GG2.GP10 Review Status with Higher level Managers

Review the activities, status, and results of the compliance 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.

COMP:GG3 Institutionalize a Defined Process

Compliance is institutionalized as a defined process.

COMP:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined compliance 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 compliance 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.

COMP:GG3.GP2 Collect Improvement Information

Collect compliance 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:

- compliance knowledgebase or information repository
- satisfied compliance obligations and compliance reports
- lessons learned from data collection, analysis, and validation
- lessons learned from satisfying compliance obligations
- metrics and measurements of the viability of the process *(Refer to COMP:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned in post-event review of incidents and disruptions in continuity
- compliance lessons learned that can be applied to improve operational resilience management performance, such as remediation actions and risks and decisions to not comply with specific obligations
- the current status of compliance obligations, including the inventory
- reports on the effectiveness and weaknesses of controls
- 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.