Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Incident Management and Control (IMC)

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/

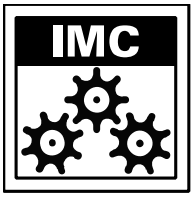
Carnegie Mellon

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.

DM-0003234

INCIDENT MANAGEMENT AND CONTROL

Operations



Purpose

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

Introductory Notes

Throughout an organization's operational environment, disruptions occur on a regular basis. They may occur as the result of intentional actions against the organization, such as a denial-of-service attack or the proliferation of a computer virus, or because of actions over which the organization has no control, such as a flood or earthquake. Disruptive events can be innocuous and go unnoticed by the organization or, at the other extreme, they can significantly impact operational capacities that affect the organization's ability to carry out its goals and objectives.

To manage operational resilience, an organization must become adept at preventing disruptions whenever possible and ensuring continuity of operations when a disruption occurs. However, because not all disruptions can be prevented, the organization must have the capability to identify events that can affect its operations and to respond appropriately. This requires the organization to have processes to recognize potential disruptions, analyze them, and determine how (or if) and when to respond.

The Incident Management and Control process area focuses the organization's attention on the life cycle of an incident—from event detection to analysis to response. The organization establishes the incident management plan and program and assigns appropriate resources. Event detection and reporting capabilities are established, and the organization sets criteria to establish when events become incidents that demand its attention. Events are triaged and analyzed, and incidents are validated. Supporting activities such as communication, logging and tracking events and incidents, and preserving event and incident evidence are defined and established. Most important, the organization performs post-incident review to determine what can be learned from incident management and applied to improve strategies for protecting and sustaining services and assets, as well as improvements in the incident management process and life cycle.

Incident management begins with event identification, triage, and analysis. An event can be one or more minor occurrences that affect organizational assets and have the potential to disrupt operations. An event may not require a formal response from the organization—it may be an isolated issue or problem that is immediately or imminently fixable and does not pose organizational harm. For example, a user may report opening an email attachment and then the user's workstation does not operate properly. This "event" may be an isolated problem or an operator error that requires attention but may not require an organizational response.

Other events (or series of events) require the organization to take notice. Upon triage and analysis, these events may be declared as "incidents" by the organization. An incident is an

event (or series of events) of higher magnitude that significantly affects organizational assets and associated services and requires the organization to respond in some way to prevent or limit organizational impact. For example, several customers may independently report that they are unable to place orders via the internet (events). The problem is deemed to be caused by a denial-of-service attack that is being targeted against the web portal (incident). In this case, the organization must be able to recognize, analyze, and manage the incident successfully. When an organization is dealing with an incident whose impact on the organization is rapidly escalating or immediate, the incident is deemed a "crisis." A crisis requires immediate organizational action because the effect of the incident is already being felt by the organization and must be limited or contained.

Incidents affect the productivity of the organization's assets and, in turn, associated services. Because assets span physical and electronic forms, incidents can be either cyber or physical in nature, depending on the target of the incident. Incidents that affect the people and facilities assets are typically physical in nature. In the case of information and technology assets, incidents can be cyber (such as unauthorized access to electronic information or to technology components) or physical (such as unauthorized access to paper or other media on which information assets are stored or to technology assets that are physically accessible).

Operational resilience is predicated on the organization's ability to identify disruptive events, prevent them where possible, and respond to them when the organization is impacted. The extent to which the organization performs event management must be commensurate with the desired level of operational resilience that it needs to achieve its mission.

Incident management is a broad organizational function. It includes many types of activities that traverse the enterprise and require varying skill sets. To provide effective coverage of these activities, the Incident Management and Control process area has five goals that address

- incident planning and assignment of resources
- event and incident identification and reporting
- event analysis
- incident response and recovery
- incident learning and knowledge management

Related Process Areas

The identification, definition, management, and control of assets are addressed in the Asset Definition and Management process area.

The identification and prioritization of high-value organizational services are performed in the Enterprise Focus process area.

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

The development, testing, and implementation of service continuity plans are addressed in the Service Continuity process area.

The reporting of incidents according to applicable laws, rules, and regulations is addressed in the Compliance process area.

The processes for identifying and detecting events that could become incidents are addressed in the Monitoring process area.

The management of risks to organizational assets that arise from incidents is addressed in the Risk Management process area.

The identification and analysis of vulnerabilities are performed in the Vulnerability Analysis and Resolution process area.

Summary of Specific Goals and Practices

Goals	Practices
IMC:SG1 Establish the Incident Management and Control Process	IMC:SG1.SP1 Plan for Incident Management
	IMC:SG1.SP2 Assign Staff to the Incident Management Plan
IMC:SG2 Detect Events	IMC:SG2.SP1 Detect and Report Events
	IMC:SG2.SP2 Log and Track Events
	IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence
	IMC:SG2.SP4 Analyze and Triage Events
IMC:SG3 Declare and Analyze Incidents	IMC:SG3.SP1 Declare Incidents
	IMC:SG3.SP2 Analyze Incidents
IMC:SG4 Respond to and Recover from Incidents	IMC:SG4.SP1 Escalate Incidents
	IMC:SG4.SP2 Develop Incident Response
	IMC:SG4.SP3 Communicate Incidents
	IMC:SG4.SP4 Close Incidents
IMC:SG5 Establish Incident Learning	IMC:SG5.SP1 Perform Post-Incident Review
	IMC:SG5.SP2 Translate Experience to Strategy

Specific Practices by Goal

IMC:SG1 Establish the Incident Management and Control Process

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

Incident management is a risk management activity that is foundational to managing the security and resilience of an organization's high-value assets and services. The organization must establish processes for identifying, analyzing, responding to, and learning from incidents to prevent the consequences of unanticipated risks and to manage these consequences when realized. The incident management process is also a source of knowledge that can be used by the organization to continually improve continuity plans and practices and strategies for protecting and sustaining services and assets.

The establishment of incident management and control processes begins with the planning for incident management and the identification and assignment of resources to carry out the plans.

IMC:SG1.SP1 Plan for Incident Management

Planning is performed for developing and implementing the organization's incident management and control process.

Because each organization is unique, it must develop an incident management plan and process that fit its organizational and strategic drivers, business objectives, critical success factors, and general risk environment. These factors should determine the organization's baseline philosophy regarding identification, analysis, and response to incidents and should be reflected in the organization's plan for carrying out these activities. Specifically, the organization must plan for how it will

- identify events and incidents (e.g., through a service desk or problem management reporting activity, or through monitoring)
- analyze these events and incidents and determine an appropriate response
- respond to incidents (e.g., a local response or a coordinated enterprise response)
- structure and staff the plan (by assigning individuals or groups to specific roles or by creating a specialized incident response team such as a computer security incident response team [CSIRT] or similar group)

The organization should develop and document its plan for incident management and outline the specific objectives of the plan. The plan should reflect the organization's philosophy of incident management and response. The objectives of the plan should be translated into specific actions and assigned to individuals or groups to be performed when necessary.

Typical work products

1. Incident management plan
2. Documented requests for commitments to the plan
3. Documented commitments to the plan

Subpractices

1. Establish the incident management plan content.

   The incident management plan should address at a minimum

   - the organization's philosophy on incident management
   - the structure of the incident management process
   - the requirements and objectives of the incident management process relative to managing operational resilience
   - a description of how the organization will identify incidents, analyze them, and respond to them
   - the roles and responsibilities necessary to carry out the plan
   - applicable training needs and requirements

- resources that will be required to meet the objectives of the plan *(See IMC:SG1.SP2.)*
- relevant costs and budgets associated with incident management activities

2. Establish commitments to the plan.

   Documented commitments by those responsible for implementing and supporting the plan (particularly the commitment of higher level managers) are essential for plan effectiveness.

3. Revise the plan and commitments as necessary.

IMC:SG1.SP2 Assign Staff to the Incident Management Plan

Staff are identified and assigned to the incident management plan.

The incident management plan must be staffed to ensure the plan's objectives can be carried out when necessary. The organization must identify the staff necessary to achieve the plan's objectives and ensure that staff are assigned and aware of their roles and responsibilities with respect to satisfying these objectives. Staff should be provided sufficient autonomy and authority to carry out their duties as required by the plan. The organization must determine the types of training needed for those involved in the incident management process and provide training that is commensurate with incident management responsibilities and accountabilities.

Typical work products

1. Job descriptions for roles and responsibilities in the plan
2. List of available and skilled staff
3. List of skill gaps and gaps in the availability of staff
4. Mitigation plans to address skill and staff gaps
5. Updated incident management plan (with staff assignments)

Subpractices

1. Develop detailed job descriptions for each role and responsibility detailed in the incident management plan.
2. Establish a list of candidate and skilled staff to fill each role and responsibility in the incident management plan.

   Skill or staff gaps for each role and responsibility should be identified and resolved.

3. Assign staff to incident management roles and responsibilities.
4. Ensure that training is provided to staff respective to their incident management job responsibilities.

   The training of staff who are vital to the management of operational resilience is covered in the Organizational Training and Awareness process area.

IMC:SG2 Detect Events

A process for detecting, reporting, triaging, and analyzing events is established and maintained.

Incidents originate as organizational events. The organization must be able to monitor and identify events as they occur, as well as to determine when an event or a series of events constitutes an incident that requires a coordinated and planned response. Failure to properly identify events in a timely manner can shift the organization's resilience management burden from prevention to reactive management of organizational impact, which is much more costly.

In order to apply incident management processes, the organization must have a foundational structure for event detection, reporting, logging, and tracking, and for collecting and storing event evidence. Because incidents originate as one or more events, foundational processes related to event detection and reporting also support incident reporting, logging, and tracking.

IMC:SG2.SP1 Detect and Report Events

Events are detected and reported.

The monitoring, identification, and reporting of events are the foundation for incident identification and commence the incident life cycle. Events potentially affect the productivity of organizational assets and, in turn, associated services. These events must be captured and analyzed so that the organization can determine whether an event will become (or has become) an incident that requires organizational action. The extent to which an organization can identify events improves its ability to manage and control incidents and their potential effects.

At a minimum, the organization should identify the most effective methods for event detection and provide a process for reporting events so that they can be triaged, analyzed, and addressed. Staff should be assigned to the task of monitoring various organizational processes (both technical and non-technical) to identify and report events. Typically the organization's service desk is often the front line for collecting event data and for commencing the incident management process.

The processes that the organization uses to monitor the resilience of assets and to identify anomalies or problems (such as events) are addressed in the Monitoring process area.

These are examples of methods of event detection:

- monitoring of technical infrastructure, including network architecture and network traffic
- reporting of problems or issues to the organization's service desk
- observation of organizational managers and users of IT services
- environmental and geographical events reported through media such as television, radio, and the internet
- reporting from legal or law enforcement staff
- observation of a breakdown in processes or productivity of assets
- external notification from other entities such as CERT
- results of audits or assessments

Typical work products

1. Sources of event detection and reporting
2. Descriptions of event detection and reporting roles and responsibilities
3. Event detection and reporting procedures
4. Event reports

Subpractices

1. Define the methods of event detection and reporting.
2. Develop and communicate descriptions of event detection and reporting roles and responsibilities *(refer to IMC:SG1.SP1)*.
3. Assign the roles of event detection and reporting to appropriate staff throughout the organization *(refer to IMC:SG1.SP2)*.

   Ensure that those assigned the responsibility for event detection and reporting understand this responsibility and have committed to performing it.
4. Establish a process for event reporting. Document events as they are detected on an event report.
5. Submit event reports to appropriate incident management staff per the organization's event reporting process.
6. Provide proper training and awareness for managers and users of technology assets (systems, networks, etc.) to identify anomalies and report them to the service desk or other authorized source for investigation and resolution.

IMC:SG2.SP2 Log and Track Events

Events are logged and tracked from inception to disposition.

The organization should have a formal process for logging events as they are identified and for tracking them through the incident life cycle. Logging and tracking ensure that the event is properly progressing through the incident life cycle and, most important, is closed when an appropriate response and post-incident review have been completed. Logging and tracking facilitate event triage and analysis activities, provide the ability to quickly obtain a status of the event and the organization's disposition, provide the basis for conversion from event to incident declaration, and may be useful in post-incident review processes when trending and root-cause analysis are performed. Logging and tracking may also support forensic activities and in some cases may be required by law enforcement. In essence, logging and tracking create an incident knowledgebase of both events and incidents to which the organization has been subjected. *(Refer to IMC:SG5 for post-incident review practices.)*

The organization must decide the degree to which the logging and tracking process is formalized. *(Refer to MA:SG1 for measurement objectives that may need to be aligned with incident management information needs.)* Logging and tracking should allow for the possibility that some events will go on to be declared as incidents, and as a result, additional information will

be collected as the incident proceeds through incident handling and response activities. Basic information about events (and incidents) should include

- a unique organization-derived identifier (such as an event or incident number)
- a brief description of the event (type of event)
- an event category (based on categories predefined by the organization such as “denial of service,” “virus intrusion,” or “physical access violation”)
- the organizational assets, services, and organizational units that are affected by the event (including the seriousness of the organizational consequences)
- a brief description of how and by whom the event was identified and reported, and other relevant details as necessary (application system, network segment, operating system, etc.)
- if the event was determined to be an incident *(refer to IMC:SG2.SP4 and IMC:SG3)*, the individuals or teams to whom the incident was assigned for containment, analysis, and response (typically referred to as the “incident owner”)
- costs associated with the event or incident
- relevant dates (such as when the event or incident was detected or occurred, when the event or incident was closed, and, if applicable, when the post-incident review was performed)
- the actions taken in response to the event or incident

Typical work products

1. Logged event reports
2. Incident management knowledgebase
3. Event and incident status reports

Subpractices

1. Develop and implement an incident management knowledgebase that allows for the entry of event reports (and the tracking of declared incidents) through all phases of their life cycle.

   Guidelines and standards for the consistent documentation of events should be developed and communicated to all who are involved in the reporting and logging processes.

2. Enter event reports into the incident management knowledgebase as they are received.

   Refer to IMC:SG2.SP4 and IMC:SG3 for a description of events that are determined to be incidents.

3. Establish and distribute standard reports that provide status information about events as they move through the life cycle.

The status of events should be checked regularly to ensure that they are moving through the organization's established incident management process and are not stalled or awaiting activity. Events that need additional attention should be identified and resolved.

IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence

The process for collecting, documenting, and preserving event evidence is established and managed.

An event may become an organizational incident that has the potential to be a violation of local, state, or federal rules, laws, and regulations. This is often not known early in the investigation of an event, so the organization must be vigilant in ensuring that all event and incident evidence is handled properly in case an eventual legal issue, civil or criminal, is raised.

To properly collect, document, and preserve evidence, the organization must have processes for these activities, and the processes must be known to all staff who are involved in any aspect of the incident life cycle. Staff must be trained in proper identification and handling of evidence, ensuring that the integrity of the evidence is not altered. Because it is unpredictable whether an event or incident will result in legal action, an organization must also consider early involvement of legal and possibly law enforcement staff in the incident identification and analysis process to avoid problems with evidence retention, destruction, and tampering.

Typical work products

1. List of relevant rules, laws, regulations, and policies regarding incident forensics
2. Event/incident evidence documentation and preservation guidelines

Subpractices

1. Identify relevant rules, laws, regulations, and policies for which incident evidence may be required.

   Because there may be compliance issues related to the collection and preservation of incident data, this practice must be considered in the context of the organization's compliance program. *(This is addressed in the Compliance process area.)*

2. Develop and communicate consistent guidelines and standards for the collection, documentation, and preservation of evidence for events/incidents.
3. Document events and related evidence information in the incident management knowledgebase where practical *(see IMC:SG2.SP2).*

   Rules, laws, regulations, and policies may require specific documentation for forensic purposes. These specific requirements must be included in the organization's logging and tracking process as described in IMC:SG2.SP2. Some information about events may be confidential or sensitive, so the organization must be careful to appropriately limit access to event information to only those who need to know about it. *(Controls for information assets are addressed in the Knowledge and Information Management process area.)*

IMC:SG2.SP4 Analyze and Triage Events

Events are analyzed and triaged to support event resolution and incident declaration.

The triage of event reports is an analysis activity that helps the organization to gather additional information for event resolution and to assist in incident declaration, handling, and response. Triage consists of categorizing, correlating, prioritizing, and analyzing events. Through triage, the organization determines the type and extent of an event (e.g., physical versus technical), whether the event correlates to other events (to determine if they are symptomatic of a larger issue, problem, or incident), and in what order events should be addressed or assigned for incident declaration, handling, and response. Triage also helps the organization to determine if the event needs to be escalated to other organizational or external staff (outside of the incident management staff) for additional analysis and resolution.

Some events will never proceed to incident declaration; the organization determines these events to be inconsequential. For events that the organization deems as low priority or of low impact or consequence, the triage process results in closure of the event and no further actions are performed.

Events that exit the triage process warranting additional attention may be referred to additional analysis processes for resolution or declared as an incident and subsequently referred to incident response processes for resolution. These events may be declared as incidents during triage, through further event analysis, through the application of incident declaration criteria, or during the development of response strategies, depending on the organization's incident criteria, the nature and timing of the event(s), and the consequences of the event that the organization is currently experiencing or that is imminent. *(Incident declaration and analysis are addressed in IMC:SG3.)*

Typical work products

1. Updated event reports (categorized and prioritized; disposition)
2. Updated incident knowledgebase
3. Open events status report

Subpractices

1. Assign a category to events from the organization's standard category definitions.
2. Perform correlation analysis on event reports to determine if there is affinity between two or more events.
3. Prioritize events.

   Events may be prioritized based on event knowledge, the results of categorization and correlation analysis, incident declaration criteria *(refer to IMC:SG3.SP1)*, and experience with past declared incidents.

4. Assign a disposition to events as available.

   Possible dispositions for event reports include

   - closed
   - referred for further analysis
   - referred to organizational unit or line of business for disposition
   - declared as incident and referred to incident handling and response process

5. Escalate events to the appropriate stakeholders if they require additional analysis.
6. Update the incident knowledgebase with information gathered in the triage process and the event disposition.

   Events that have been declared as incidents as a result of the triage process should be appropriately designated in the incident knowledgebase.

7. Assign events that have not been assigned a "closed" status for further analysis and resolution.
8. Periodically review the incident knowledgebase for events that have not been closed or for which there is no disposition.

   Events that have not been closed or that do not have a disposition should be reprioritized and analyzed for resolution.

IMC:SG3 Declare and Analyze Incidents

Incidents are declared and analyzed to support response planning.

Incident declaration defines the point at which the organization has established that an incident has occurred, is occurring, or is imminent and will have to be handled and responded to.

Transition from event detection to incident declaration can be immediate, particularly when it is clear to the organization that there are significant effects on organizational assets and associated services and a response is required to limit these effects and their impact. Thus, the time from event detection to incident declaration may be immediate, requiring little additional review and analysis. In other cases, incident declaration requires more thoughtful analysis; thus, the organization may need to use predefined criteria developed from experience to help guide incident declaration.

Once an incident has been declared, the organization must perform additional analysis to develop and implement an appropriate action plan for handling and response. This action plan may represent a routine activity (such as asking users to stop opening email messages containing greeting card announcements) or a specifically designed response that is unique to the incident and requires significant levels of organizational coordination and logistical support.

The development of the organization's response to an incident is addressed in IMC:SG4.

IMC:SG3.SP1 Declare Incidents

Incidents are declared based on criteria that are established and maintained.

Each organization has many unique factors that must be considered in determining when to declare an incident. Through experience, an organization may have a baseline set of events that define standard incidents, such as a virus outbreak, unauthorized access to a user account, or a denial-of-service attack. However, in reality, incident declaration may occur on an event-by-event basis.

To guide the organization in determining when to declare an incident (particularly if incident declaration is not immediately apparent), the organization must define incident declaration criteria. Incident declaration criteria may be derived from risk evaluation criteria developed in the risk management process area.

These are examples of criteria that guide an organization's determination of an incident:

- Is the event common to the organization? Has it occurred before? Did past occurrences of the event result in an incident declaration?
- Is the event isolated (i.e., only one user has reported it) or are there multiple occurrences of the same event being reported across the enterprise (through the service desk or similar construct)?
- Is the impact of the event imminent or immediate? Is the organization already suffering some effects from the event? Is there a crisis that has been precipitated by the event?
- Does the event affect core business drivers such as a high-value service that produces revenue?
- Does the event constitute a violation of organizational policy or constitute fraud or theft?
- Is the life or safety of staff or external entities at risk?
- Are the integrity and operability of a facility at risk?
- Are the integrity and operability of a high-value service or system at risk?
- Are there other organizational impacts that are imminent or already being incurred, such as damage to the organization's reputation?
- Is there a potential legal infraction or possible future legal (civil or criminal) concerns?

Typical work products

1. Incident declaration criteria

Subpractices

1. Establish incident declaration criteria for use in guiding when to declare an incident.

   Risk measurement and evaluation criteria provide the thresholds to understand the consequences to the organization for an organizationally defined impact area (RISK:SG2.SP2), and ensures that risks are prioritized according to organizational importance.

2. Distribute incident declaration criteria to all sources and relevant staff who may need to declare an incident.

3. Update incident declaration criteria as required based on experience in past declarations.
4. Declare incidents based on criteria.

IMC:SG3.SP2 Analyze Incidents

Incidents are analyzed to support the development of an appropriate incident response.

Incident analysis is primarily focused on helping the organization to determine an appropriate response to a declared incident by examining its underlying causes and actions and the effects of the underlying event(s) that have already been detected by the organization. Analysis is performed to further understand the incident, to develop and implement action to contain its impact, and to recover from any resulting damage. Incident analysis may be informed by the correlation and prioritization activities performed in event triage.

Incident analysis requires skills from across the organization. Depending on the nature of the incident, analysis may involve asset owners, information technology staff, physical security staff, auditors, and legal staff, as well as external stakeholders such as vendors and suppliers, law enforcement staff, and vulnerability clearinghouses. *(Sources of vulnerability information are identified in the Vulnerability Analysis and Resolution process area.)* Incident analysis may involve staff to whom the incident has been escalated or assigned (including the incident owner). *(Incident escalation is addressed in IMC:SG4.SP1.)*

Incident analysis should be focused on properly defining the underlying problem, condition, or issue and in helping the organization to prepare the most appropriate and timely response to the incident. It should also help the organization to determine whether the incident has legal ramifications. Analysis activities must feed the organization's evidence collection process in case of future legal actions *(see IMC:SG2.SP3)* as well as the post-incident review processes *(see IMC:SG5)* for process improvement.

These are examples of activities that may be performed to analyze incidents:

- interviews with those who reported the underlying event(s), as well as those who are involved in its investigation
- interviews of specific knowledge experts who have a detailed understanding of the area affected
- interviews of asset owners for assets (such as information) that have been affected by the incident
- review of relevant logs and audit trails of network and physical activity
- consultation of vulnerability and incident databases such as the US-CERT Vulnerability Notes Database and the MITRE Corporation's Common Vulnerabilities and Exposures list
- consultation with law enforcement staff
- consultation with legal and audit staff

- consultation with product vendors and software/hardware suppliers (if their products are involved)
- consultation with emergency management staff (if the incident is a safety concern)

Typical work products

1. Incident analysis report
2. Reports from analysis tools and techniques
3. Updated incident knowledgebase

Subpractices

1. Establish and communicate a standardized and consistent incident analysis approach and structure.
2. Identify relevant analysis tools, techniques, and activities that the organization will use to analyze incidents and develop appropriate responses.

   Provide appropriate levels of training for incident management staff on analysis tools and techniques.
3. Analyze open event reports and previously declared incidents.

   Open event reports may correlate to the incident under analysis and provide additional information that is useful in developing an appropriate response. Reviewing documentation on previously declared incidents may inform the development of a response action plan, particularly if significant organizational (and external) coordination is required.
4. Document analysis on an incident analysis report.

   Ensure that analysis is appropriately documented on the incident analysis report and in the incident knowledgebase and made available for use in evidence collection, response development, and post-incident review.

IMC:SG4 Respond to and Recover from Incidents

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

The nature of a declared incident is that the organization has already incurred some effect, however limited, that requires the organization to act. Responding to and recovering from an incident often requires two primary actions from the organization:

- immediate limitation or containment of the scope and impact of the incident
- the development and implementation of an appropriate response to stop the ongoing or future effect of the incident, repairing any remaining damage, and restoring organizational assets and services to the state in which they existed prior to the disruption

Responding and recovering may also require a carefully coordinated and executed collaboration between organizational units and external entities (such as emergency providers) and a plan for handling incident logistics, particularly if the incident is significant or catastrophic. The logistics of these coordinating activities can often be planned in advance; however, execution may occur on demand or spontaneously.

In addition, to avoid reputation damage, the organization must also craft and implement a communications process that facilitates collaboration and logistical execution and keeps stakeholders aware of the incident's evolution and resolution. *(Refer to the Communications process area for more information about developing, deploying, and managing internal and external communications in support of a declared incident.)*

IMC:SG4.SP1 Escalate Incidents

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

Incidents that the organization has declared and that require an organizational response must be escalated to those stakeholders that can implement, manage, and bring to closure an appropriate and timely solution. These stakeholders are typically internal to the organization (such as a standing incident response team or an incident-specific team) but could be external in the form of contractors or other suppliers. *(Refer to the External Dependencies Management process area for information about managing relationships with external entities.)* The organization must establish processes to ensure that incidents are referred to the appropriate stakeholders because failure to do so will impede the organization's response and may increase the level to which the organization is impacted.

Because communication is a vital tool in incident escalation, the organization's incident communications plan must be developed, implemented, and tested in order to support effective escalation *(see IMC:SG4.SP3). (Communications activities in support of operational resilience, including when dealing with an incident, are described in the Communications process area.)*

Typical work products

1. Incident escalation procedures
2. Escalation criteria

Subpractices

1. Develop incident escalation criteria.

   These criteria should provide guidance on when escalation is appropriate and necessary, and the level of escalation required.

2. Develop incident escalation procedures.

   Incident escalation procedures should consider the type and extent of the incident and the appropriate stakeholders.

3. Communicate incident escalation criteria and procedures to those who have responsibility for identifying and escalating incidents.

   Ensure that stakeholders such as the service desk are included in the escalation process.

4. Escalate incidents to appropriate stakeholders for resolution.

IMC:SG4.SP2 Develop Incident Response

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

Responding to an organizational incident is often dependent on proper advance planning by the organization in establishing, defining, and staffing an incident management capability. In addition, the organization typically has service continuity plans that can be executed in parallel if an incident has resulted in drastically affected operations. *(Developing, testing, and implementing service continuity plans are addressed in the Service Continuity process area.)*

Responding to an incident describes the actions the organization takes to prevent or contain the impact of an incident on the organization while it is occurring or shortly after it has occurred. The range, scope, and breadth of the organizational response will vary widely depending on the nature of the incident. Incident response may be as simple as notifying users to avoid opening a specific type of email message or as complicated as having to implement service continuity plans that require relocation of services and operations to an off-site provider. The broad range of potential incidents requires the organization to have a broad range of capability in incident response.

The organization's response to an incident must be founded on a well-structured incident response capability and plan *(as developed in IMC:SG1.SP1)*. Depending on the organization, the actions related to incident response can include

- containing damage (e.g., by taking hardware or systems offline or by locking down a facility)
- collecting evidence (including logs and audit trails)
- interviewing relevant staff (those who are involved in reporting or analyzing the incident and those who are affected by it)
- communicating to stakeholders, including asset owners and incident owners
- developing and implementing corrective actions and controls
- implementing continuity and restoration plans or other emergency actions *(See the Service Continuity process area for more information about continuity planning and response.)*

The organization must consider the best response structure for its unique organizational structure and context. For some organizations, it makes sense to establish one or more permanent teams that are responsible for repeatable capabilities to respond to a broad range of incidents, supplementing the response with subject matter experts where necessary. In other cases, an organization may establish a virtual "team" of individuals who may be quickly called upon to perform specific duties to respond to an incident. In addition, the organization may have standardized responses for certain types of incidents (such as denial-of-service attacks) that have been developed through lessons learned. Some of these responses might be

reflected in standard service continuity plans that the organization has already developed.

In responding to any incident, the organization must consider who is responsible for coordinating the overall response and ensure that those who must be involved in the response have been notified. Responders must update the incident knowledgebase to detail and document the steps taken to contain and repair incident damage so that future incidents can use this information in root-cause analysis and problem diagnosis. *(See IMC:SG2.SP4 and IMC:SG3.SP2 for more details.)* In addition, the organization must ensure that actions taken to contain or repair incident damage are performed in a way that ensures no additional vulnerabilities are introduced and that the effect on day-to-day operations is limited.

Typical work products

1. Incident response strategy and plan
2. Service continuity plans
3. Updated incident knowledgebase

Subpractices

1. Develop an incident response strategy and plan to limit incident effects and to repair incident damage.

   The incident response strategy and plan should address at a minimum

   - the essential activities (administrative, technical, and physical) that are required to contain or limit damage and provide service continuity
   - existing continuity of operations and restoration plans in the organization's plan inventory
   - the resources and skills required to perform the incident response strategy and plan
   - coordination activities with other internal staff and external agencies that must be performed to implement the strategy
   - the levels of authority and access needed by responders to carry out the strategy and plan
   - objectives for measuring when the strategy and plan are successful
   - the estimated cost of implementing the strategy and plan
   - the essential activities necessary to restore services to normal operation (recovery), the resources involved in these activities, and their estimated cost
   - legal and regulatory obligations that must be met by the strategy
   - standardized responses for certain types of incidents
2. Identify staff who are responsible for coordinating incident response (across all potential types of incidents) and ensure they have the authority and responsibility to act.
3. Update the incident knowledgebase with information about the incident response strategy and plan.

IMC:SG4.SP3 Communicate Incidents

A plan for the communication of incidents to relevant stakeholders and a process for managing ongoing incident communications are established.

Miscommunications or inaccurate information about organizational incidents can have dire effects that far exceed the potential damage caused by an incident itself. As a result, the organization must proactively manage communications when incidents are detected and throughout their life cycle. This requires the organization to develop and implement a communications plan that can be readily implemented to manage communications to internal and external stakeholders on a regular basis and as needed. This plan should provide relevant information to these entities and control or limit the degree to which misinformation and conjecture can develop. It must also consider the needs of a wide range of stakeholders that have a vested interest in obtaining information about organizational incidents in a controlled and regular manner.

The basic structure of the plan may be static, but the plan should be flexible to address a broad range of incident types, stakeholders, and corresponding communications needs. In addition, the organization should consider developing partnerships with external stakeholders so that a coordinated communications strategy can be developed and implemented when incidents affect the organization's external operational environment as well.

These are examples of stakeholders that may have to be included in an incident communication plan:

- members of the incident handling and management team (if the organization has established such a team), or internal staff who have incident handling and management job responsibilities
- shareholders
- asset owners (if their asset is the target of the incident) and service owners
- information technology staff (if the target of the incident is the organization's technical architecture and infrastructure)
- middle and higher level managers
- business continuity staff (if they will be required to enact continuity or restoration plans as a result of the incident)
- human resources departments, particularly if safety is an issue
- communications and public relations staff
- support functions such as legal, audit, and human resources
- legal and law enforcement staff (including federal agencies), if the incident may have legal ramifications
- external media outlets, including newspaper, television, radio, and internet
- affected customers or upstream suppliers
- local, state, and federal emergency management staff
- local utilities (power, gas, telecommunications, water, etc.), if affected

- regulatory and governing agencies

Typical work products

1. List of incident stakeholders, communications protocols, and channels
2. Incident communications plan
3. Incident status reports (from incident knowledgebase)

Subpractices

1. Identify relevant stakeholders that may have a vested interest or vital role in communications about an organizational incident.
2. Identify the appropriate communications protocols and channels (media and message) for each type of stakeholder.
3. Develop and implement an organizational incident management communications plan.

   The incident communications plan should address at a minimum

   - the stakeholders with which communications about incidents are required
   - the types of media by which communications will be handled
   - the various message types and level of communications appropriate to various stakeholders (For example, incident communications may be vastly different for incident responders than for those who may simply need to know.)
   - special controls over communications (i.e., encryption or secured communications) that are appropriate for some stakeholders
   - the roles and responsibilities necessary to carry out the plan
   - the frequency and timing of communications
   - internal and external resources that are involved in supporting the communications process
4. Identify and obtain commitment from staff who are required to carry out the incident communications plan.

   Ensure that these staff members have the appropriate level of training and skills necessary to execute and support the plan.
5. Identify and train staff responsible for incident communication and provide general guidelines for incident response and other staff for appropriate communication of incident information.

IMC:SG4.SP4 Close Incidents

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

(Closure of an incident can be performed only after post-incident review practices have been completed. Practices in IMC:SG5 must be completed before IMC:SG4.SP4 can be accomplished.)

Incident closure refers to the retirement of an incident that has been responded to (i.e., there are no further actions required and the organization is satisfied with the result) and for which the organization has performed a formal post-incident review *(see IMC:SG5)*. The organization

must have a process for formal closure of incidents (including the practices in IMC:SG5) which results in formally logging a status of "closed" in the incident knowledgebase.

A "closed" status indicates to all relevant stakeholders that no further actions are required or outstanding for the incident. It also provides notification to those affected by the incident that it has been addressed and that they should not be subject to continuing effects.

Typical work products

1. Criteria for incident closure
2. Updated incident knowledgebase

Subpractices

1. Establish criteria for incident closure.

   The criteria for incident closure will vary by organization but will generally occur after post-incident review has occurred. However, some organizations may establish concrete closure rules.

2. Define and assign the responsibility for incident closure.

   Typically, this action will be the responsibility of the incident owner or incident manager. Only authorized staff should be permitted to close an incident.

3. Update the incident knowledgebase to indicate that an incident has been closed.

4. Track incidents that have been open for an extended period of time without closure and resolve.

   Incidents that appear to be open for an extended period of time may not have followed the organization's incident management process or may not have been formally closed. The status of incidents in the incident database should be reviewed regularly to determine if open incidents should be closed or need additional action.

IMC:SG5 Establish Incident Learning

Lessons learned from identifying, analyzing, and responding to incidents are translated into actions to improve strategies for protecting and sustaining services and assets.

One of the most important aspects of incident management and control is the ability to understand why an incident occurred and what can be done by the organization to prevent it in the future. From a risk management standpoint, using incident lessons learned to improve controls and protection strategies and to optimize these strategies with continuity planning and response effectively shifts the organization's attention from a response mode to a preventive mode.

Incident learning involves a post-incident review by relevant stakeholders and a formal translation of lessons learned to improve strategies for protecting and sustaining services and assets.

The practices of this goal should be considered as part of the closure activity as described in IMC:SG4.SP4.

IMC:SG5.SP1 Perform Post-Incident Review

Post-incident review is performed to determine underlying causes.

Post-incident review is a formal part of the incident closure process. The organization conducts a formal examination of the causes of the incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the incident to occur.

To be effective, post-incident review requires the input of all relevant stakeholders in the incident management process. This includes those who

- reported the incident
- detected the incident
- triaged and analyzed the incident
- responded to the incident
- were affected by the incident
- had the incident communicated to them

Post-incident review should include a significant root-cause analysis process. The organization should employ commonly available techniques (such as cause-and-effect diagrams) to perform root-cause analysis as a means of potentially preventing future incidents of similar type and impact. Considerations of other processes that may have caused or aided the incident should be given, particularly as they may exist in processes such as change management and configuration management.

Typical work products

1. Criteria for incident closure
2. Post-incident analysis report
3. Recommendations for control improvement
4. Recommendations for improvements to incident management process
5. Updated incident knowledgebase

Subpractices

1. Establish and implement a formal post-incident review activity and require it as part of closing an incident.
2. Assign responsibility for post-incident review activities to appropriate staff and ensure they are properly trained.
3. Identify root-cause analysis tools and techniques and ensure all staff who participate in analysis are trained in their use.

   These tools and techniques may include cause-and-effect diagrams, interrelationship diagrams, causal factor tree analysis, etc.
4. Prepare a post-incident analysis report.

This report should detail the organization's recommendations for improvement in administrative, technical, and physical controls, as well as improvements to the incident management process.

5. Document the results of post-incident root-cause analysis in the incident knowledgebase so that this information is available for use in other processes such as problem management.

IMC:SG5.SP2 Translate Experience to Strategy

The lessons learned from incident management are analyzed and translated into improvements.

The costs associated with incident detection and response are an investment for the organization only to the extent that what is learned in these processes can be used by the organization to make it more efficient and effective in dealing with future events and in enhancing its approach to resilience. Lessons learned in incident management should serve as a benchmark for determining the validity and effectiveness of the organization's current strategies for protecting and sustaining assets. In addition, lessons learned should provide valuable information for continuous improvement of the incident management process.

These are examples of areas that have to be addressed after an incident:

- Update protection strategies and controls to protect assets and services from future incidents of similar type and nature.
- Update policies to reflect lessons learned.
- Update training for employees regarding the incident.
- Revise continuity plans and strategies to protect and sustain services and assets.
- Review and revise life-cycle processes.
- Review and revise asset-level resilience requirements, if necessary.
- Revise incident criteria.
- Develop standardized responses to common incidents.
- Improve incident management processes.

Typical work products

1. Controls strategy
2. Service continuity plans
3. Resilience policy
4. Training needs and requirements
5. Incident management process improvements list
6. Service and asset resilience requirements
7. Updated incident knowledgebase

Subpractices

1. Review incident knowledgebase information and update the following areas accordingly:

- protection strategies and controls for assets involved in the incident
- continuity plans and strategies for sustaining assets involved in the incident
- information security and other organizational policies that need to reflect new standards, procedures, and guidelines based on what is learned in the incident handling
- training for staff on information security, business continuity, and IT operations

2. Review incident management and control processes and update them for any perceived deficiencies or omissions.
3. Update resilience requirements for assets and services based on what is learned in the incident management process.
4. Quantify and monitor the types, volumes, and costs of incidents.
5. Improve risk management based on lessons learned from managing incidents.
6. Document problem reports that arise from incident management and deliver these reports to the organization's problem management process (if such a process is present).

   The organization's incident knowledgebase can serve as a central repository that links the incident management and problem management processes so that duplicative effort in documenting issues and problems can be avoided.

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 Incident Management and Control process area.

IMC:GG1 Achieve Specific Goals

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

IMC:GG1.GP1 Perform Specific Practices

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

Elaboration:

Specific practices IMC:SG1.SP1 through IMC:SG5.SP2 are performed to achieve the goals of the incident management and control process.

IMC:GG2 Institutionalize a Managed Process

Incident management and control is institutionalized as a managed process.

IMC:GG2.GP1 Establish Process Governance

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

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

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the incident management and control process may be exhibited by

   - developing and publicizing higher level managers' objectives and requirements for the process
   - sponsoring process policies, procedures, standards, and guidelines and the roles of staff in the process
   - making higher level managers aware of applicable compliance obligations related to the process, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
   - sponsoring and funding process activities
   - providing input to the organization's designated process for identifying, analyzing, and responding to events and incidents and the chosen means for implementing and managing the process (i.e., dedicated team, virtual team, etc.)
   - regular reporting from organizational units to higher level managers on events and incidents that may affect the organization's ability to achieve its goals
   - 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 and oversight on incident management and recommendations for improving the process
   - providing input on identifying, assessing, and managing operational risks resulting from incidents
   - conducting regular internal and external audits and related reporting to audit committees on process effectiveness
   - providing visible, continued support for the process through board-level activities such as inclusion on meeting agendas or committees
   - creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

   Elaboration:

   The incident management and control policy should address

   - responsibility, authority, and ownership for performing process activities

- procedures, standards, and guidelines for
  - detecting, logging, reporting, and tracking events
  - collecting and preserving evidence
  - triaging events
  - analyzing events
  - declaring an incident from one or more events
  - responding to incidents, including escalation procedures and developing incident response
  - recovering from incidents
  - communicating incidents
- post-incident review, problem resolution, and closure
- methods for measuring adherence to policy, exceptions granted, and policy violations

IMC:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the incident management and control process.

Elaboration:

Specific practice IMC:SG1.SP1 requires the development of a plan for how the organization will carry out incident management and control. In generic practice IMC:GG2.GP2 as related to incident management, the planning elements required in IMC:SG1.SP1 are formalized and structured and are performed in a managed way. The plan for the incident management and control process should reflect the organization's stated philosophy of incident management and the preferred means for handling incidents (i.e., through a dedicated or permanent team, a virtual team, etc.).

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 commitment.
4. Revise the plan as necessary.

IMC:GG2.GP3 Provide Resources

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

Elaboration:

Specific practice IMC:SG1.SP2 requires the formal assignment of resources to the incident management and control process plan.

Subpractices

1. Staff the process.

Elaboration:

These are examples of staff required to perform the incident management and control process:

- staff responsible for
  - identifying, detecting, logging, reporting, and tracking events
  - collecting and preserving evidence for events and incidents
  - triaging events
  - analyzing events and incidents, including declaring an incident from one or more events
  - developing and executing plans for responding to incidents, including escalation
  - recovering from incidents
  - communicating incidents
  - performing post-incident reviews, resolving problems, and closing incidents
  - developing incident management plans and ensuring they are aligned with stakeholder requirements and needs
  - managing external entities that have contractual obligations for process activities
- owners and custodians of high-value assets that support the accomplishment of operational resilience management objectives
- internal and external auditors responsible for reporting to appropriate committees on 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.

Elaboration:

In the case of incident management and control, funding must extend to supporting the incident life cycle and consideration must be given to unknown funding requirements related to incident management that are relative to the type and extent of incident and the impact on the organization. Extending consideration to these unpredictable needs provides the organization a level of control over unplanned and potentially unconstrained costs.

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

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

Elaboration:

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

- methods, techniques, and tools for
  - event identification, detection *(refer to IMC:SG2),* and reporting

  - analyzing events and incidents, including determining when one or more events should be declared an incident
  - collecting, documenting, and preserving evidence for events and incidents
  - recovering from events
- methods and tools for event and incident logging and tracking
- methods for triaging events
- root-cause analysis techniques and tools, such as cause-and-effect diagrams, interrelationship diagrams, and causal factor tree analysis
- incident databases and knowledgebases, including predetermined response and recovery actions for specific types of incidents
- methods and techniques for responding to events
- communications methods for reporting and escalating incidents
- methods for conducting post-incident reviews and ensuring lessons learned are reflected in process activities

IMC:GG2.GP4 Assign Responsibility

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

Elaboration:

Specific practice IMG:SG1.SP1 indicates that the incident management plan should define the roles and responsibilities necessary to carry out the plan, as well as document commitments from those responsible. Specific practice IMC:SG1.SP2 requires the assignment of staff to the incident management plan, as well as the identification of skill and staff gaps for each area of responsibility. Generic practice IMC:GG2.GP4 requires the assignment of responsibility for the activities in the incident management life cycle, including the identification of events and incidents, analysis of incidents, and incident response.

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:

   Incident management and control activities may be temporal (i.e., involved with response to a specific incident) or permanent (involved with support activities that are not related to any specific incident).

   To assign responsibility and authority for performing the incident management and control process, organizations may establish dedicated incident management teams that address the majority of incident handling and management activities or assign staff to virtual teams that come together when required. Other structures may also be implemented, such as decentralized dedicated teams, which would require varying levels of responsibility and authority to be assigned.

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

   Elaboration:

   Responsibility and authority for performing incident management and control tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - assigning staff to dedicated or virtual incident handling and management teams as a primary job responsibility
   - including process tasks and responsibility for these tasks in specific job descriptions
   - including process tasks in staff performance management goals and objectives with requisite measurement of progress against these goals
   - 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
   - developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions, assets, and services
   - including process tasks in measuring performance of external entities against contractual instruments

   Refer to the External Dependencies Management process area for additional details about managing relationships with external entities.

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

IMC:GG2.GP5 Train People

Train the people performing or supporting the incident management and control 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 incident management and control process:

   - event detection, reporting, and tracking, including service desk activities
   - documenting and logging event reports
   - collecting and preserving evidence
   - technical analysis of events and incidents, including triage

- declaring incidents
- escalating and communicating incidents
- understanding and applying laws, rules, and regulations
- performing incident response, including damage containment
- creating, managing, and deploying incident response teams
- developing and implementing administrative, technical, and physical controls
- performing root-cause analysis and post-incident review
- using tools, techniques, and methods necessary to handle incidents throughout their life cycle, including those necessary to perform the process using the selected methods, techniques, and tools identified in IMC:GG2.GP3 subpractice 3
- knowledge unique to each type of asset or service that may be the target of an incident
- working effectively and collaborating with asset owners and custodians
- eliciting and prioritizing stakeholder requirements and needs and interpreting them to develop effective incident management plans and plans for handling specific types of incidents

2. Identify process skill gaps based on available resources and their current skill levels.
3. Identify training opportunities to address skill gaps.

Elaboration:

Training can be obtained for all aspects of incident handling and for forming and managing formal incident teams. In addition, certification programs are available to certify incident handlers and for developing and participating on incident management teams.

These are examples of training topics:

- event and incident detection
- event and incident logging
- incident containment and evidence preservation
- incident forensics tools and techniques
- event and incident analysis
- event triaging
- incident declaration
- escalation procedures
- incident response
- incident response teams
- incident communications, including general communications skill development
- post-incident review
- supporting asset 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 IMC:GG2:GP3 subpractice 3

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

IMC:GG2.GP6 Control Work Products

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

Elaboration:

Generic practice IMC:GG2.GP6 generically covers the recommended updating of the incident knowledgebase as described in several IMC-specific practices, as well as other work products of the incident management and control process.

The tools, techniques, and methods used to populate and maintain the incident knowledgebase should be employed to perform consistent and structured version control over the knowledgebase to ensure that incident information is current, accurate, and "official." The tools, techniques, and methods can also be used to securely store the knowledgebase, provide access control over inquiry, modification, and deletion, and to track version changes and updates.

These are examples of incident management and control work products placed under control:

- event reports, including sources of event detection and reporting
- incident management plans and the process plan
- incident response strategy and plan
- event and incident status reports
- incident communications plan
- list of incident stakeholders
- incident management policies, procedures, standards, and guidelines
- incident knowledgebase
- event and incident evidence
- incident declaration criteria
- incident escalation procedures and criteria
- post-incident analysis reports
- list of incident management process improvements
- contracts with external entities

IMC:GG2.GP7 Identify and Involve Relevant Stakeholders

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

Elaboration:

Stakeholders of the incident management and control process may extend across the organization and externally to business partners and vendors. The identification of these stakeholders in generic practice IMC:GG2.GP7 is in addition to the identification of stakeholders of the incident communications process described in IMC:SG4.SP3, although it is recognized that these may be the same or similar.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the incident management and control process:

   - incident owners
   - asset owners and custodians
   - service owners
   - organizational unit and line of business managers responsible for high-value assets and the services they support
   - staff who serve key roles in incident communications activities, such as public relations
   - staff who provide input to and resolution of incidents as they are escalated
   - staff responsible for developing, implementing, and managing an internal control system for assets
   - external entities involved in process activities and responsible for managing high-value assets
   - human resources
   - information technology staff
   - service desk staff
   - staff responsible for physical security
   - legal and law enforcement staff, including federal agencies
   - internal and external auditors
   - regulatory and governing agencies

   Stakeholders are involved in various tasks in the incident management and control process, such as

   - detecting events and incidents
   - planning for incident handling, management, and response
   - making commitments to process plans and activities
   - collecting, documenting, and preserving event and incident evidence
   - analyzing events and incidents
   - declaring incidents
   - responding to incidents, including participating on incident response teams
   - communicating events and incidents and the status of incidents as they move through the incident life cycle
   - escalating incidents
   - coordinating process activities
   - reviewing and appraising the effectiveness of process activities
   - performing post-incident review and improvement processes

2. Communicate the list of stakeholders to planners and those responsible for process performance.

3. Involve relevant stakeholders in the process as planned.

IMC:GG2.GP8 Measure and Control the Process

Measure and control the incident management and control 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.

   Elaboration:

   These are examples of metrics for the incident management and control process:

   - percentage of coverage of plan (extent to which incident management plan includes all organizational units and functions that require coverage)
   - percentage of roles/responsibilities assigned to staff roles/members (extent to which plan roles and tasks are assigned to specific staff roles/members)
   - percentage of staff who have not been trained on their roles and responsibilities as defined in plans
   - percentage of staff (managers, users) who have not completed training and awareness to identify anomalies and report them in the required timeframe (initial, refresher
   - percentage of events triaged (events reported vs. events analyzed)
   - percentage of events that are stalled or awaiting activity beyond an established threshold
   - percentage of events whose documentation does not meet rules, laws, regulations, policies, or other requirements for forensic purposes
   - percentage of events without a disposition
   - percentage of events open beyond scheduled threshold (such as specified number of days for closure)
   - mean, median time to close an event, categorized in some meaningful manner
   - percentage change in the number of logged events
   - percentage of events that recur and result in declared incidents
   - percentage of events (or sets of related events) declared as incidents
   - percentage of events declared as incidents that do not match the current incident declaration criteria
   - number of incidents by incident type

- percentage of incidents that have been declared but not closed
- percentage of incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds
- percentage of operational time that services and assets were unavailable (as seen by users and customers) due to incidents
- number of incidents by incident type and impact
- number of incidents by incident type and root cause
- impact due to incidents by incident type
- change in impact due to incidents by incident type
- percentage of incidents that recur
- percentage change in the number of incidents by incident type
- time (mean, median, range) between event detection and related incident declaration
- time (mean, median, range) between event detection and related incident response
- time (mean, median, range) between event detection and related incident closure percentage of incidents that require escalation
- percentage change in the elapsed time of the incident life cycle by incident type (mean, median, ranges)
- percentage of incidents that require escalation
- percentage of incidents that require the involvement of law enforcement
- percentage of incidents that require the involvement of regulatory and governing agencies
- percentage of post-incident review recommendations that result in control changes or improvements to the process
- extent to which incident occurrence (prevent) is reduced as a result of implementing RMM appraisal findings
- reduction in incident occurrence and impact (detect, respond, recover) as a result of implementing CERT-RMM appraisal findings

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

Elaboration:

Incident learning processes as described in IMC:SG5 are intended to provide a standard and consistent post-incident review and examination. However, reviews of the incident management and control process may result from periodic audits or examinations, particularly if metrics indicate a rise in incidents of specific types or with increasing impact, or an extension of time required to resolve incidents.

If the incident management and control process is decentralized (i.e., spread across organizational units), post-incident reviews may provide management insight into variations between the organizational units that could impact the organization's overall incident management capability.

Periodic reviews of the incident management and control process are needed to ensure that

- the process is known and accessible

- events and incidents are identified, reported, and addressed on a timely basis
- events and incidents are logged and closed
- proper forensic procedures are used to collect and preserve evidence
- events are properly triaged and analyzed for root causes
- incidents are properly declared
- incidents are properly escalated to designated stakeholders
- incident response capabilities are commensurate with the priority of an incident
- incidents are communicated appropriately to stakeholders at a level commensurate with their involvement
- event and incident status reports are provided to appropriate stakeholders in a timely manner
- post-incident reviews are performed to improve the process
- 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
- administrative, technical, and physical controls are operating as intended
- controls are meeting the stated intent of the resilience requirements
- 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.

IMC:GG2.GP9 Objectively Evaluate Adherence

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

Elaboration:

These are examples of activities to be reviewed:

- identifying and detecting events and incidents, including service desk procedures
- logging, tracking, and reporting events and incidents
- establishing incident validation criteria
- collecting, documenting, and preserving evidence
- triaging events
- analyzing events and incidents
- declaring incidents
- escalating incidents

- communicating incidents
- responding to incidents
- recovering from incidents so as to minimize disruption and impact
- closing incidents (and addressing incidents that have not been closed)
- performing post-incident reviews
- the alignment of stakeholder requirements with process plans
- 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:

- incident management plans
- event and incident service desk reports and documentation
- incident management policies, procedures, standards, and guidelines
- incident knowledgebase
- evidence collection and preservation guidelines, as well as documentation on past collection activities
- event and incident analysis reports
- incident declaration criteria
- incident escalation criteria and procedures
- incident response documentation (of past response actions)
- incident communications plan and status reports
- post-incident review reports
- issues that have been referred to the risk management process
- process methods, techniques, and tools
- metrics for the process *(Refer to IMC:GG2.GP8 subpractice 2.)*
- contracts with external entities

IMC:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the incident management and control 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.

IMC:GG3 Institutionalize a Defined Process

Incident management and control is institutionalized as a defined process.

IMC:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined incident management and control process.

Elaboration:

Incident management and control may be performed in either a centralized or decentralized manner. The way in which the organization institutionalizes the incident management and control process varies based on the size of the organization, the diversity of operational environments, and other factors. This may lead to a range of implementation methods, including the use of a dedicated centralized team, dedicated virtual teams, decentralized dedicated teams, or other combinations.

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 incident management and control 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.

IMC:GG3.GP2 Collect Improvement Information

Collect incident management and control 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:

Specific goal IMC:SG5 and its specific practices describe capturing lessons learned in post-incident review and translating these into improvements to incident management and control process activities. Such improvement directly supports the improvement of service continuity and strategies to protect and sustain assets and services.

These are examples of improvement work products and information:

- service desk reports or similar documentation of reported events
- incident reports from the incident knowledgebase and the level to which the knowledgebase reflects the current status of all incidents
- issues related to collecting, documenting, and preserving evidence
- issues related to deploying forensic tools and techniques
- lessons learned in triaging and analyzing events and in analyzing incidents
- communications issues
- issues related to declaring incidents
- incident response successes and failures
- issues related to closing incidents
- lessons learned in post-incident review
- problem reports and corresponding actions
- changes to asset and service resilience requirements resulting from post-incident review
- metrics and measurements of the viability of the process *(Refer to IMC:GG2.GP8 subpractice 2.)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- recommendations for control improvements
- recommended updates to service continuity plans

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.