**Unit III**

* Service Support Process

Configuration Management

The Configuration Management process establishes and maintains the consistency of a system’s functional, performance and physical attributes with its requirements, design and operational information and allows technical insight into all levels of the system design throughout the system’s life cycle. Effective configuration management supports the establishment and maintenance of the functional, allocated and product baseline. Establishing rigorous configuration control enables the successful development, test, production, delivery and sustainment of the needed capability to the end user. DoD Engineering policy pertaining to Configuration Management is contained in [DoDI 5000.88 paragraph 3.4.c. Configuration and Change Management](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500088p.PDF?ver=O8LFc8NzlyJX-SgM2Haalw%3d%3d).

Configuration Management activities support:

* Traceability of designs to requirements.
* Proper identification and documentation of system elements, interfaces, and interdependencies.
* Timely and thorough vetting and disposition of change requests.
* Control and documentation of approved changes to baselines
* Proper and timely incorporation of verified changes in all affected items and documentation.
* Consistent and appropriate provisions in the Engineering Change Proposal (ECP) and related contract actions.
* Consistency between a product and its design requirements, supporting documentation and associated production and sustainment systems.
* A complete audit trail of design decisions and modifications.
* Continued assurance of system supportability and interoperability, consistent with the approved acquisition and life-cycle sustainment strategies.

**Baselines**

Configuration Management facilitates the orderly development of a system through establishment of the technical baseline (including the functional, allocated and product baselines), and their assessment and approval at various technical reviews and audits. A baseline is an agreed-upon description of the attributes of a product at a point in time, which serves as a basis for change. Upon approval, the technical baseline documentation is placed under formal configuration control. Through Configuration Management, the program identifies, controls and tracks changes to the technical baseline, ensuring changes occur only after thorough assessments of performance, cost and schedule impacts, as well as associated risks.

The following baselines are critical to executing Configuration Management:

### Functional Baseline

Functional Baseline: Describes the system’s performance (functional, interoperability and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics. It is directly traceable to the operational requirements contained in the Initial Capabilities Document (ICD). The Program Manager (PM) establishes Government control of the functional baseline at the System Functional Review (SFR) and verifies it through Functional Configuration Audits (FCA) leading up to the system-level FCA or the System Verification Review (SVR). Attributes of the functional baseline include:

* Assessed to be achievable within cost and schedule constraints
* Documentation of established interfaces between functional segments
* Documented performance requirements traced to (draft) Capability Development Document (CDD) requirements
* Reflects design considerations and clear linkage in the systems of systems (SoS) context
* Documented verification requirements

### Allocated Baseline

Allocated Baseline: Describes the functional and interface characteristics for all system elements (allocated and derived from the higher-level product structure hierarchy) and the verification required to demonstrate achievement of those specified characteristics. The allocated baseline for each lower-level system element (hardware and software) is usually established and put under configuration control at the system element Preliminary Design Review (PDR). This process is repeated for each system element and culminates in the complete allocated baseline at the system-level PDR. The PM then verifies the allocated baseline at the FCA and/or SVR. Attributes of the allocated baseline include:

* All system-level functional performance requirements decomposed (or directly allocated) to lower-level specifications (configuration items (CI) for system elements)
* Uniquely identified CIs for all system elements at the lowest level of the specification tree
* All interfaces, both internal (between element CIs) and external (between the system under development and other systems), documented in interface control documents
* Verification requirements to demonstrate achievement of all specified functional performance characteristics (element CI to element CI level and at the system level) documented
* Design constraints documented and incorporated into the design

### Product Baseline

Product Baseline: Describes the detailed design for production, fielding/deployment and operations and support. The product baseline prescribes all necessary physical (form, fit and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements. It is traceable to the system performance requirements contained in the CDD. The initial product baseline includes "build-to" specifications for hardware (product, process, material specifications, engineering drawings and other related data) and software (software module design - "code-to" specifications). The initial system element product baseline is established and placed under configuration control at the system element Critical Design Review (CDR) and verified later at the Physical Configuration Audit. The PM assumes control of the initial product baseline at the completion of the system-level CDR to the extent that the competitive environment permits. This does not necessarily mean that the PM takes delivery and acceptance of the Technical Data Package. Attributes of the product baseline include:

* Requirements Traceability Matrix (RTM) is complete.
* The detailed design (hardware and software), including interface descriptions, satisfies the CDD or any available draft Capability Production Document (CPD) and pertinent design considerations.
* Hardware, software and interface documentation are complete.
* Key product characteristics having the most impact on system performance, assembly, cost, reliability, ESOH and sustainment have been identified.
* Traceability from design documentation to system and system element verification requirements and methods is complete.
* Manufacturing processes that affect the key characteristics have been identified, and capability to meet design tolerances has been determined.

## Configuration Management Activities and Products

### Roles

The program office and developer share responsibility for planning, implementing and overseeing the Configuration Management process and its supporting activities. The distribution of responsibilities between the program office and the developer varies, based on the acquisition strategy and the life-cycle phase.

#### **Role of the Program Manager**

The PM approves the Configuration Management Plan and should ensure adequate resources are allocated for implementing Configuration Management throughout the life cycle. The PM assesses the impact of proposed changes to a baseline, approves changes -- usually through a Configuration Control Board (CCB) (see [MIL-HDBK-61 (Configuration Management Guidance)](http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=202239) and [SAE-GEIA-HB-649 (Configuration Management Standard Implementation Guide)](http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=281559) for additional information), and ensures proper documentation of decisions, rationale and coordination of changes.

#### **Role of the Systems Engineer**

The Systems Engineer ensures Configuration Management planning is complete, and should document details and activities in the program’s Systems Engineering Plan (SEP) and the supporting Configuration Management Plan (CMP) (as appropriate). In accordance with [DoDI 5000.88, paragraph 3.4.c.](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500088p.PDF?ver=O8LFc8NzlyJX-SgM2Haalw%3d%3d), the PM, with the support of the Systems Engineer, ensures that the configuration management approach is consistent with the Intellectual Property Strategy (See [DAG CH 3–4.1.7. Technical Data Management Process](https://shortcut.dau.edu/dag/CH03.04.01.07)).

### Configuration Management Activities/Products

The CM process described in the DoD-adopted standard American National Standards Institute/Electronic Industry Association (ANSI/EIA)-649, Configuration Management Standard, consists of five interrelated functions that, when collectively applied, allow the program to maintain consistency between product configuration information and the product throughout its life cycle.

The five CM functions are:

* Configuration Management Planning and Management
* Configuration Identification
* Configuration Change Management
* Configuration Status Accounting
* Configuration Verification and Audit

In addition, the DoD-adopted standard [EIA-649-1, Configuration Management Requirements for Defense Contracts](http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=280800), implements the principles outlined in ANSI/EIA-649B for use by defense organizations and industry partners during all phases of the acquisition life cycle. It makes provisions for innovative implementation and tailoring of specific configuration management processes to be used by system suppliers, developers, integrators, maintainers and sustainers.

Incident Management

An incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

One of the challenges to be faced in building an effective incident management capability is understanding the broader scope of incident management work. It is no longer enough to just “handle” events and incidents in a technical security context. Twenty years ago, many organizations relegated this responsibility to their IT or Security department—it was a “technical” issue to be solved, and these teams typically handled incidents in isolation. Back then there was limited sharing of knowledge about incidents or communication about the results to stakeholders across the enterprise to identify broader risk to the mission, reputation, brand, etc. But those days are gone, and today enterprises must be able to incorporate security into every aspect of their operations. (See the [Governance & Management](daisy:549-BSI) content area.)

Since incidents can have far-reaching consequences and implications affecting the internal protection (confidentiality, availability, integrity) of critical data and assets, privacy information, supply chain contacts, and beyond, incident management actions can involve many groups within the enterprise—board room and C-level managers[3](https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management/incident-management#footnote3_dbwz7ng) who handle governance, budget, and strategic issues; IT, CSIRT, and security staff who coordinate and implement incident response actions; groups such as human resources, privacy officers, risk, audit, legal, and public relations staff who might be brought in to handle aspects of an incident related to their areas of expertise; and others. External groups may also be involved, including regulatory bodies, law enforcement, and possibly other computer response security organizations.

For computer security incident response to occur in an effective and successful way, all the tasks and processes being performed must be viewed from an enterprise perspective. This means identifying the interactions and communications that need to occur, how tasks are done and how the processes relate, how information is exchanged, and how actions are coordinated—no matter who is performing the work.

Focusing only on the response part of the process, for example, misses key actions that if not done in a timely, consistent, and quality-driven manner will impact the overall response, possibly delaying actions due to the confusion of roles and responsibilities, ownership of data and systems, and authority. Response can also be delayed or ineffective if communications are not clear, if appropriate contacts are not known, or if the quality of information provided is inadequate, incomplete, or inaccurate. Any impact on the response timeliness and quality can cause further damage to critical assets and data during an incident.

How a computer security incident management capability is instituted or structured within an organization can differ greatly. Because so many groups can be involved, depending on the nature of the incident and the required response, having defined interfaces and assigned roles and responsibilities is a key requirement. Often, even though others throughout the organization may be involved, a core group is established to help coordinate the overall incident management function. This core group may take the form of a defined group of people or a designated unit such as a CSIRT. This can be seen in organizations such as

* local, state, and provincial governments
* educational institutions and research networks
* national initiatives

The group can also be part of other security, IT, risk management, or business continuity functions. This is common in commercial industry, where this function may be served by

* crisis management teams
* resiliency teams
* security response teams

Some organizations may choose to outsource this capacity to a managed security service provider.

In whatever way the incident management capability is structured, any group responsible for performing incident management actions must recognize that they don’t operate in isolation and that communication and interaction with all appropriate entities is key—whether internal to the organization or with other external contacts. An overall security strategy must be implemented to ensure that all operational units understand their role in the incident management process.

In this article we describe five high-level processes[4](https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management/incident-management#footnote4_hp1eo9n) that compose a model for the various functions that are undertaken as part of an incident management capability:

* Prepare/Sustain/Improve (Prepare) – establish, sustain, and improve the CSIRT
* Protect Infrastructure (Protect) – make changes in the infrastructure to protect systems or mitigate an ongoing computer security event
* Detect Events (Detect) – recognize and report events when they occur and look for indicators that might identify future events/incidents
* Triage Events (Triage) – categorize, correlate, and prioritize events and assign them to someone for further investigation and possible response
* Respond – plan, coordinate, and carry out effective response to incidents

This incident management model can be used by an organization to identify what processes it is already performing, benchmark against what others are doing (including third parties), identify where gaps exist, and highlight what interfaces need to exist between all the processes and all the participants. It can be used to help build a consistent, reliable, and repeatable set of processes to identify, detect, analyze, and respond to computer security incidents.[5](https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management/incident-management#footnote5_djd76qe) This model can also be used to help an organization

* identify the components of such a capability and the processes that should be in place to perform effective incident management
* develop workflows and tasks that can be followed to implement or improve the incident management capability

## Incident Management as Part of the CERT® Resiliency Engineering Framework

Very often in organizations and institutions, there is a question of where incident management fits—is it in IT operations? Is it part of security management? Is it in risk management? Is it in disaster recovery? Over the past few years, members of the SEI’s CERT Program have been working with the Financial Services Technology Consortium (FSTC) to identify mature practices in banking and financial services industries. Research and development in this area has produced a framework that shows how all these areas fit together and complement each other. This framework is called the CERT® Resiliency Engineering Framework (REF).[6](https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management/incident-management#footnote6_0os7dtw)

Operational resiliency is the organization’s ability to sustain the mission in the face of operational risks such as those resulting from

* failed internal processes
* inadvertent or deliberate actions of people
* problems with systems and technology
* external events

Operational resiliency depends on effective management of core operational risk management activities such as security management (SM), business continuity and disaster recovery (BC/DR), and IT operations.

The REF model states that SM, BC/DR, and IT are three separate areas, but they work together to support and sustain operational resiliency. These three areas (SM, BC/DR, IT)

* are dependent on each other to complete their missions
* share the same goals, objectives, requirements—driven by organizational needs
* focus on the protection and productivity of the same objects
* rely on shared, common practices

Risk management focuses on keeping critical objects or assets productive by limiting risk and managing the impact of realized risk.

Operational resiliency is the concept of managing operational risk to ensure mission viability by being able to adapt to new risks as they emerge and acting before reacting. Because resiliency is a function of risk management and security is a risk management activity, security contributes to operational resiliency through the risk management link. Incident management is one part of security management and therefore also a risk management activity.

The REF model also describes a foundation for a process improvement approach to security and business continuity. It does this by describing a collection of 21 capability areas. One of those capability areas is “Incident Management and Control (IMC).”

The IMC capability within REF, just like the IM Process Model, promotes the establishment of processes for detecting, analyzing, responding to, and learning from incidents to

* prevent the impact of unanticipated risks
* manage their impact when realized
* provide a source of knowledge to improve protection strategies and continuity and sustainability plans and practices

Having an incident management capability in place contributes to the operational resiliency of the organization. Once again, however, since incident management is a risk management activity, it must be recognized that technology solutions are not the only important part of the response. Achievement of the business and operational mission must be balanced in light of any response strategies, and organizational process and human actions must be taken into account. Technology alone does not achieve success.

The definition of an incident within the REF context is very broad; it can relate to anything that disrupts achieving the mission. The focus of computer security incident management is on a smaller subset of events: those that are malicious or unauthorized.

The REF model also highlights other capability areas that relate to or are influenced by activities from the incident management and control capability, such as vulnerability management, compliance management, service continuity, monitoring, root cause analysis, training and awareness, and communication. To be successful at incident management, an organization must also look at being successful in these areas and defining the interfaces between them and the incident management process.

As new products, services, or technologies are deployed, computing infrastructures or business partners change, or business strategies are realigned, organizations need to understand the importance of aligning their incident management activities with broader enterprise activities.

Approaching security in this managed and strategic way, sharing the vision, balancing enterprise-wide drivers and costs with business risks, etc., can enable the security effort to ultimately be more successful [REF 08].

## Incident Management Process Model

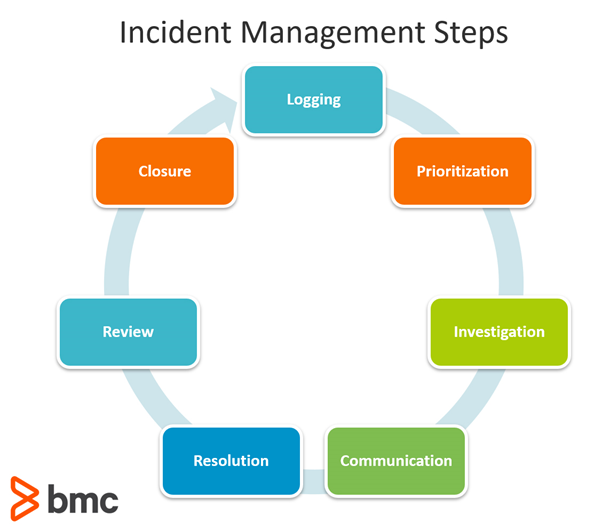
Incident management, then, can be seen as an abstract, enterprise-wide capability, potentially involving every business unit within the organization. It can be viewed as a subset of the organization’s broader security, risk, and IT management activities and functions. It can often cross into general security and IT management tasks and practices. Because of the large amount of staff inside and outside an organization who might be involved, it is important that a plan exists for how these pieces interact with each other so that incidents are handled in a smooth and timely manner.

To be successful, this plan should

* integrate into existing processes and organizational structures so that it enables rather than hinders critical business functions
* strengthen and improve the capability of the constituency, where required, to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization’s systems and critical assets
* support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate
* support, complement, and provide input into existing business and IT policies that impact the security of an organization’s infrastructure
* implement a command and control structure, clearly defining roles and responsibilities, as well as accountability for decisions and actions
* be part of an overall strategy to protect and secure critical business functions and assets
* include the establishment of processes for
  + detection and triage
  + categorization and prioritization
  + notification and communication
  + analysis and response
  + collaboration and coordination
  + maintenance and tracking of records

Figure 1 provides a graphical representation of the CERT incident management process model.

**Figure 1. Incident management best practice model**



The figure can be explained as follows:

* The Prepare and Protect processes are shown as continuous, ongoing processes above and below the Detect, Triage, and Respond processes. This is signified by the arrows going across the diagram and by having the icons for each at the beginning and end of the arrows. These processes involve putting into place all the necessary staff, technology, infrastructure, policies, and procedures needed for incident management activities to occur in a timely, coordinated, and effective manner. The use of the arrows surrounding the Detect, Triage, and Respond processes show that Prepare and Protect support and enable the other processes.
* The small arrows coming into the Prepare and Protect process indicate requirements, policies, or rules that will govern the structure and function of these processes. These arrows also indicate incoming process improvement recommendations.
* The line from the Prepare to the Protect process signifies a handoff between these two processes. In this case, the information passed is process improvement recommendations for changes in the computing infrastructure that result from a postmortem review done in the Prepare process. These changes in the infrastructure, for example, will help harden and secure the infrastructure to help prevent similar events or incidents from happening or the same activities from re-occurring.
* The Detect, Triage, and Respond processes are shown in sequence as information coming into the Detect process is evaluated to determine whether it is actionable and needs to be passed on to the Triage process for further analysis and assessment. If in the Triage process the received information (an incident report, a vulnerability report, a general information request, or a suspicious event) requires a response, it is passed on to the Respond process.
* The arrow going from Protect to Detect indicates the passage of any incident or vulnerability reports that may result from infrastructure evaluations. It is possible that during an evaluation or assessment, a vulnerability, ongoing incident, or remnant of a past incident may be discovered. This information would need to be passed to the Detect process for further evaluation.
* The arrows going from the Respond process to the Prepare (or Protect) process signify the handoff of process improvements and corresponding incident data or response actions and decisions where appropriate. The handoff from Respond to Prepare passes this information to the postmortem review subprocess within the Prepare process (and similarly as it relates to the Protect process).

Over the last several years a number of books and articles have been written about incident management and incident response activities [Fraser 97, ISS 01, Kruse 02, Mandia 01, SANS 03, Schultz 02, Sokol 00, van Wyk 01]. Although many use slightly different terminology, a similar set of tasks is discussed. Most of the tasks include detecting and reporting events and incidents, containing and resolving incidents, and recovery of systems. Other steps that relate to these functions include identification, containment, eradication, investigation, and notification.

In this context, incident management is not just the application of technology to resolve computer security events. It is also the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency.

### **Building an Incident Management Capability**

In developing an incident management capability, an organization must determine who is currently performing incident management and related tasks and identify who will be part of the incident management team. Identifying people across the enterprise who must work together to analyze and resolve incidents and then assigning them specific roles and responsibilities is one of the most critical tasks that can be done in building and improving a capability.

Getting management buy-in and consensus within the organization is always the first recommendation for implementing a formalized process. This establishes a foundation that is needed for success. If possible, have executive management establish a policy and corresponding procedures that define the incident management process and key participants. This policy and set of procedures must then be announced, taught, and enforced.

The purpose of each group within the capability and their roles and responsibilities should be defined and documented. Corresponding workflows that illustrate how an incident flows through the incident management process, including detection, reporting, triage, analysis, response, and closure, should be completed.

Incident reporting forms, guidelines, and procedures should be created and distributed to all organizational employees, including becoming part of employee orientation programs and annual security training. If employees do not know how and what to report, computer security events and incidents might occur that are not detected in a timely manner.

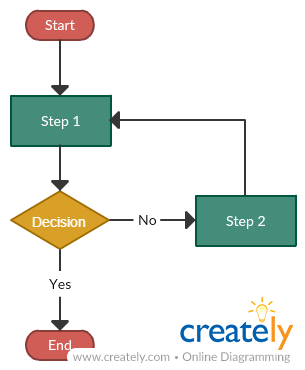
Postmortems on all key incidents should be done to determine ways to improve infrastructure protection strategies and response policies, procedures, and processes. Mock incident exercises should be conducted at least on an annual basis to test that everyone knows what to do, how to report, and how to respond.

Incident management, just like other key security management functions, must be shown to be important to the organization.

### **Process Diagrams**

Process modeling techniques are useful for illustrating an abstraction of a business process, highlighting key activities and artifacts required to conduct the process. Figure 2 shows a simplified example.

**Figure 2. A simple example of a process diagram for answering the telephone**



A workflow model is a specific type of process modeling technique, providing a description of how tasks are done, by whom, in what order, and how quickly. It differs from other modeling techniques, such as data flow diagrams and flow charts, because it specifically defines interrelationships and dependencies among tasks and activities. Understanding these interrelationships and dependencies among tasks and activities is important when analyzing the risk inherent in a business process such as incident management.

Benefits to be gained by mapping the incident management processes include

* enabling a comprehensive understanding of the current (as-is) state
* identifying risks to successful completion of the mission of the incident management capability
* supporting decisions about improvements to incident management operations (to-be state)

Said another way, mapping the incident management processes can help an organization understand all the activities, roles and responsibilities, technology, interfaces, and dependencies that are occurring during the incident response activities and how they relate to and depend on one another. It also can highlight missing activities or those with inherent weaknesses that can be then targeted for improvement. Risks that affect the successful response to incidents can be recognized and mitigated. By understanding the whole set of processes, improvements can be made in to avoid the waste of isolated fixes.

So, for each high-level process, the categories and descriptions that are used in describing the incident management workflow are listed in Table 1. These provide details about multiple aspects of a process and its associated activities (the goals and objectives for doing a piece of the process, what triggers it, what rules or regulations ”drive” the need to do it, how you know it has been completed, inputs and outputs, subprocesses, etc.). Substituting explicit (real) names, labels, and associations in place of these generic terms provides an organization with a range of information that can be used to pinpoint where processes are well defined and where they may not be. Handoffs (or interfaces) are the exchanges between actors (e.g., from one person to another, a technology to a person, a person to a technology, or even technology to technology) and occur between the major processes, from Detect to Triage, Triage to Respond, etc.

# **What is problem management?**

Problem management is the process of identifying and managing the causes of incidents on an IT service. It is a core component of ITSM frameworks.

The closer you get to real incident experts, the less you actually hear the question: “What caused the incident?”  Sure, you’ll hear it plenty from executives, and customers, and the press..  
  
Because the answer to “what caused the incident” is often dry and non-helpful: a rewritten config file, a corrupted database entry.

But what were the contributing causes behind the thing that caused the incident? What were the factors that led up to the incident? How is it possible that a config file could be rewritten? What conditions create a corrupted database entry? These are the questions you hear experts ask. And they’re at the heart of problem management.

Problem management isn’t just about finding and fixing incidents, but identifying and understanding the underlying causes of an incident as well as identifying the best method to eliminate that root cause. Moreover, pinpointing the cause has no value to an organization if it’s a cut-off process completed by a siloed team, so problem management should be constant and widely practiced across multiple teams, including IT, security, and software developers. An incident may be over once the service is up and running again, but until the underlying causes and contributing factors are addressed, the problem remains.

 problem management unleashes many benefits for the business.

### **Decrease time to resolution**

Teams that unlock the problems behind today’s incident will be better prepared to attack incidents in the future. By codifying best practices around problem analysis, teams will be able to more quickly respond and take action during the next service disruption.

### **Avoid costly incidents**

Avoiding incidents will save time, money, and lots of pain. [According to Gartner](https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/), many organizations report downtime costing more than $300,000 per hour. For some web-based services, that number can be dramatically higher.

### **Increase productivity**

Stop responding to incidents so frequently and return resources and time to teams who could be shipping new value to customers.

### **Empower your team to find and learn from underlying causes**

When organizations effectively practice problem management, teams continually investigate, learn from incidents, and ship valuable updates. Unfortunately, many enterprises create a siloed problem management team that is too far removed from day-to-day operations to eliminate the most pressing problems.

### **Promote continuous service improvement**

Problem management prevents incidents and also delivers value. For instance, fixing an incident causing low level performance also ships valuable service quality improvements.

### **Increase customer satisfaction**

Better problem management leads to fewer incidents, and happier customers. Alternatively, customer patience wears thin when they notice the same incident happening multiple times. Decreasing the occurrence of repeat incidents builds customer trust.

## The problem management process

At Atlassian, we advocate bringing the problem and incident management processes closer together.

When problem management is a heavy, siloed, and separate process, companies can end up creating a dumping ground of problems. This backlog is where problem issues go to die in some teams. It’s best to get problems in front of the teams that can handle and do valuable investigations.

That all being said, it’s good to understand the main steps that contribute to a problem management process. Such as:

1. **Problem detection**- Proactively find problems so they can be fixed, or identify workarounds before future incidents happen.
2. **Categorization and prioritization** - Track and assess known problems to keep teams organized and working on the most relevant and high-value problems.
3. **Investigation and diagnosis** - Identify the underlying contributing causes of the problem and the best course of action for remediation.
4. **Create a known error record**- In ITIL, a known error is “a problem that has a documented root cause and a workaround.” Recording this information leads to less downtime if the problem triggers an incident. This is typically stored in a document called a known error database.
5. **Create a workaround, if necessary** - A workaround is a temporary solution for reducing the impact of problems and keeping them from becoming incidents. These aren’t ideal, but they can limit business impact and avoid a customer-facing incident if the problem can’t be easily identified and eliminated.
6. **Resolve and close the problem**- A closed problem is one that has been eliminated and can no longer cause another incident.

Change Management

Creating a change management plan helps create smoother transitions. You can mandate changes, but if you don’t have a plan for how to implement, monitor, and report on the success of that change, you’re setting yourself up to fail. Regardless of the type of change you want to make, change management gives you more control over the entire process – a process that is typically supporting a costly [implementation plan](https://whatfix.com/blog/implementation-plan/) and investment.

Change management is the process of adapting to, controlling, and implementing change. This process can look different based on the type of change you are conducting. The different levels of change management include the follow:

1. **Organizational Change Management:** How companies conduct transformations, such as altering the organizational hierarchy, introducing new processes, and integrating a new software
2. **Project-Level Change Management:** The strategies and plans that focus on changes to ensure a project achieves the intended goal
3. **Individual Change Management:** Managing the change of an individual person in order to help them grow in their role and/or achieve specific goals

**Benefits Of Change Management**

All changes, big or small, benefit from well-thought-out change management. Change does not come naturally to people or organizations, so without proper management, you’ll likely hit barriers and waste time and money. Change management is the key to successfully implementing changes that stick.

The key benefits of successful change management include:

1. Proactively combat [resistance to change](https://whatfix.com/blog/causes-of-resistance-to-change/)
2. Set clear goals for changes and monitor results
3. Create strategies for implementing change effectively
4. Address and balance multiple aspects of change, such as people, processes, technology, etc.

**Types of Change Management**

You can apply different types of change management, depending on the change you are navigating. Think about how you might approach each of these four types of changes:

1. **Exceptional:** Isolated events that change an individual’s experience but don’t majorly affect multiple aspects of their life. For example, a name change would require some HR paperwork and a new email address but wouldn’t alter the person’s role at work.
2. **Incremental:** Gradual changes that do not require major or sudden shifts, such as upgrading existing technology.
3. **Pendulum:** Sudden swings from one state to another, often switching from one extreme to the opposing view or state. For example, moving from a 100% in-office work environment to a 100% remote team.
4. **Paradigm:** Changes that result in new beliefs or values and become internalized as the new norm. For example, successfully shifting from synchronous communication to a hybrid model that involves both synchronous and [asynchronous communication](https://whatfix.com/blog/remote-team-communication/).

**Steps in the Change Management Process**

The change management process is how you get from Point A (the existing state) to Point B (your desired change). Those are:

1. Determine the reason for the change.
2. Set specific goals for the change.
3. Establish key performance indicators (KPIs) and milestones to monitor progress.
4. Refer to change management models.
5. Create a change management plan and implementation strategy.
6. Designate change leaders.
7. Implement change.
8. Gather feedback.
9. Analyze progress and results.

## Principles of Change Management

Our experience has revealed six key change management principles:

### **1. Create a sense of urgency**

Based on the ‘Enhanced Kotter’s 8-Step Change Model’, this principle focuses on presenting the change as an urgent and exciting opportunity.

### **2. Roll out in phases**

Breaking your initiative into phases helps you avoid overwhelming your team with too much change all at once.

### **3. Address resistance**

By explaining the WIIFM for each person or department affected by the initiative, you can get ahead of the inevitable internal resistance and help your employees [adapt to change](https://whatfix.com/blog/adapt-to-change/).

### **4. Use a variety of training methods**

Not everyone learns in the same way, so it’s important to provide guidance through a variety of [training methods](https://whatfix.com/blog/employee-training-methods/) and [types of employee training](https://whatfix.com/blog/types-employee-training-programs/) formats.

### **5. Establish change leaders**

Without internal buy-in, your initiative is over before it even begins. [Change leaders](https://whatfix.com/blog/change-leadership/) help motivate the entire team to push forward with the transformation.

## Examples of Change Management

Change management can be applied to various industries and functions — anytime you make a significant change to how things work within an organization, you’ll need to manage that change. Here are some examples across industries and functions.

### **Change Management Examples By Industry**

* **Retail** – [Takealot uses Whatfix to automate self-training for sellers](https://whatfix.com/resources/case-study/how-emarketplace-takealot-automate-self-training-for-their-sellers/)
* **Healthcare** –[Internet Brands use Whatfix to drive product adoption](https://whatfix.com/resources/case-study/internet-brands-driving-product-adoption/)
* **IT** – Wipro enables sales representatives with Whatfix
* **Medical Devices** – Centense switches from paper to an electronic quality management solution
* **Grocery Stores** – Local Roots NYC quadruples delivery fleet during COVID-19 shutdowns

### **Change Management Examples By Business Function**

* **Sales** – [Sophos uses Whatfix to drive change management on Salesforce](https://whatfix.com/resources/case-study/how-sophos-drives-salesforce-change-management/)
* **HR** – [ManpowerGroup streamlines HR platform adoption with Whatfix interactive guidance](https://whatfix.com/resources/case-studies/mpg_seamlessly_transition_recruiters_to_bullhorn/)
* **Onboarding** – [PlanetHS decreases internal support tickets with Whatfix onboarding assistance](https://whatfix.com/resources/case-study/planeths-reduces-training-and-onboarding-effort/)
* **Customer Training** – [Corrigo uses Whatfix to reduce customer training costs](https://whatfix.com/resources/case-study/corrigo-reduces-customer-training-costs/)
* **Payroll** – Tricor group uses RPA to save 3,000+ hours in payroll services each year

Release Management

Release management refers to the process of planning, designing, scheduling, testing, deploying, and controlling software releases. It ensures that release teams efficiently deliver the applications and upgrades required by the business while maintaining the integrity of the existing production environment.

In the competitive, dynamic, and fluid world of business and IT, half-baked releases are the last thing you need. The modern enterprise is a truly dynamic environment; and not all these changes are happening at the same pace. IT organizations need a way to orchestrate these myriad changes. That’s where [release control](https://www.microfocus.com/products/release-control/overview) and [deployment automation](https://www.microfocus.com/products/deployment-automation/overview) come in to play. They help ease the transition to continuous delivery; and work through the Digital Transformation one release at a time. This is the new normal of IT.

### What is Release the Management Process?

The specific steps of release management will vary depending on the unique dynamics of each organization or application. Nevertheless, the following sequence is the most common.

#### Request

Release management starts with requests for new features or changes to existing functions. There’s no guarantee that all requests made will eventually translate into a new release. Each request is evaluated for its rationale, feasibility, and whether there’s a way to fulfill it by reconfiguring the application version already in production.

#### Plan

This is the most important step in a release’s evolution. It’s here that the release’s structure is defined. A robust plan ensures the release team stays on track and that requirements are satisfied. Create or reuse a workflow or checklist that can be referred to by stakeholders throughout the release process. The workflow should detail not just scope and milestones but responsibilities.

#### Design and Build

This is the programming phase where the requirements are converted to code. The release is designed and built into executable software.

#### Testing

Once the release is deemed ready for testing, it’s deployed to a test environment where it’s subjected to non-functional and functional testing (including user acceptance testing or UAT). If bugs are found, it’s sent back to developers for tweaking then subjected to testing again. This iterative process continues until the release is cleared for production deployment by both the development team and the product owner.

#### Deployment

The release is implemented in the live environment and made available to users. Deployment is more than just installing the release. It entails educating users on the changes and training them on how to operate the system in the context of the new features.

### What are Release Management Success Indicators?

For a release to be deemed successful, it must attain the following objectives:

* It’s deployed on time.
* It’s deployed within budget.
* It has little to no impact on current users.
* It satisfies the needs of current and new users, technological advances and/or competitive demands.