



# Incident Management

## Getting Started with Remedyforce Series

Nick Glaser (BMC Software)

Kedar Zavar (Cloudaction)

09 June 2015



## Welcome to the “Getting Started with BMC Remedyforce” Series

Today’s IT departments must drive business growth and innovation, while coping with less resources and increasing complexity. To do this, they require an IT Service Management solution that provides best practices while minimizing costs. BMC Remedyforce is built on Salesforce—the world’s most widely used cloud platform—to deliver complete IT service management functionality with the secure social, mobile, and collaborative capabilities users expect.

With the “Getting Started with Remedyforce” white paper series, our aim is to help you leverage BMC Remedyforce to improve the effectiveness and efficiency of your ITSM operations. Each paper addresses a specific area of interest and provides you with conceptual, functional and technical best practices to make configuration decisions and take action to gain value from your BMC Remedyforce investment.

## Incident Management

A basic function of almost every service delivery organization is the identification and remediation of technical challenges experienced by end users. Addressing these day-to-day requirements is the mainstay of most service delivery organizations. In ITIL terminology, this operational activity is known as Incident Management.

*Incident: An incident is an unplanned interruption to an IT Service or reduction in the quality of an IT service. (Source: ITIL, v3)*

The key goal of Incident management is to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations.

What this means in very real terms is that any organization looking to perform Incident Management must be primarily concerned with ensuring customers who are having difficulty consuming the services provided by the service delivery organization are returned to a working state quickly and efficiently. Service delivery providers must be organized in such a way that they can log incident tickets, resolve them quickly and, when necessary, escalate these tickets to experts in other parts of the IT organization when needed. Additionally, it is expected that IT service providers will utilize both technology and process to identify significant service-threatening events occurring in their environment and take pro-active steps to mitigate the impact of these events on the end-user community before they are even noticed by users and reported as incidents.

Planning and implementation of an effective and efficient Incident Management process is one of the most fundamental and critical exercises for an IT service provider.

### Key Components in BMC Remedyforce:

The following are the key components in BMC Remedyforce that support Incident Management:

- Record Planning
- Statuses
- Templates
- Workflow Automation and Rules
- Communication Management
- Prioritization
- Categorization

In addition to restoring service operations as quickly as possible additional value can be drawn from the Incident Management process. When taken in context with the other facets of the ITIL methodology there is significant value to the business including the ability to detect incidents occurring in the IT environment and respond in an efficient manner, resulting in higher availability of the service; identifying potential service improvements garnered from

contact between the business and the service delivery operations staff; realizing service or training requirements and, perhaps most importantly, aligning IT activities to real-time business priorities.

### Alignability Process Model (APM)

If you are just getting started with Incident Management, and especially if you are planning to leverage BMC's out-of-the-box capabilities, BMC Remedyforce provides a best practices framework via the Alignability Process Mode (APM). The APM describes a set of predefined processes for the delivery and support of services and illustrates how ITIL processes map work to instructions performed in BMC Remedyforce. The model was built to provide an easy-to-use interface that allows for quick access to detailed information regarding the Incident Management process.

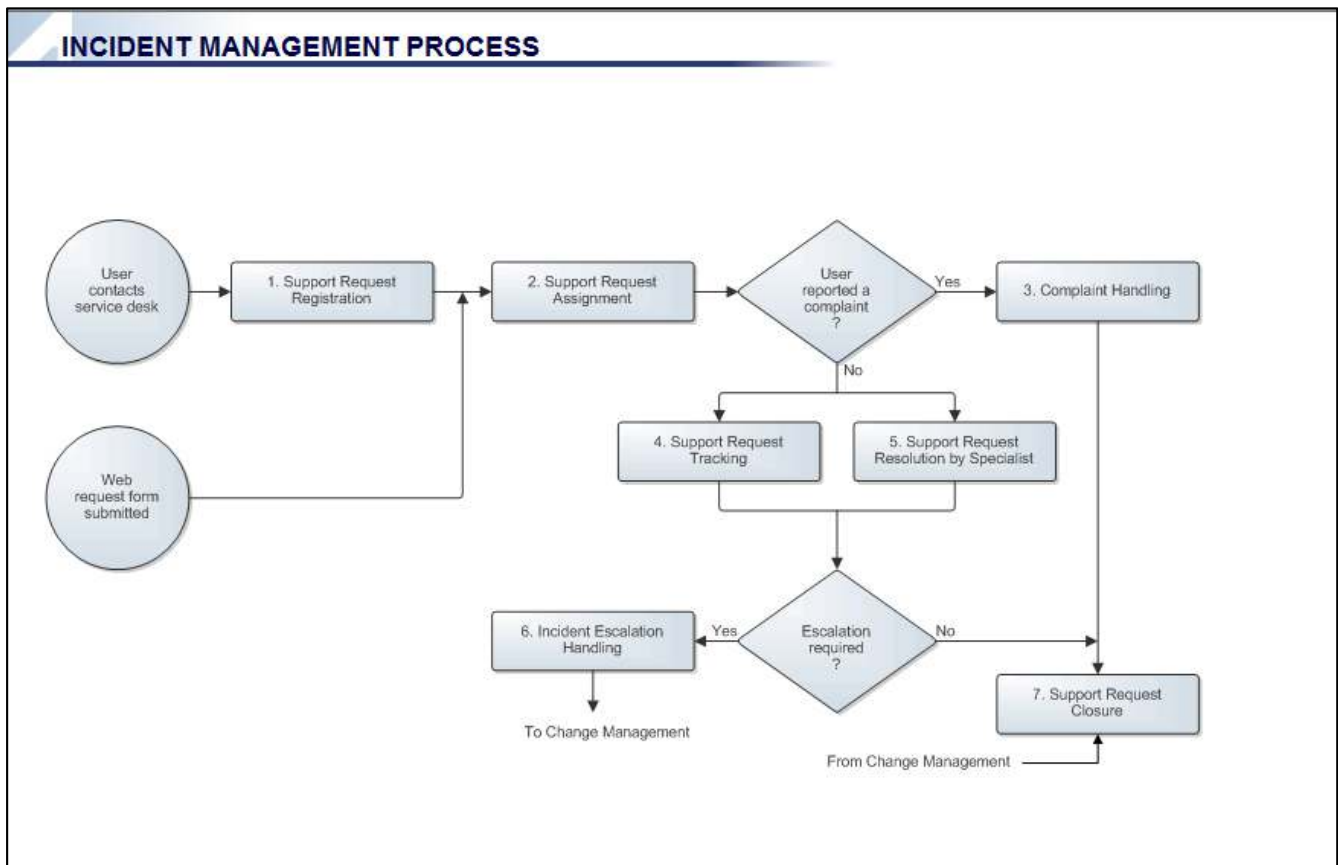


Figure 1 – Incident Management Process Model

For more information about BMC Remedyforce's Alignability Process Model for Incident Management, you can log into BMC Remedyforce and navigate to the Alignability Process Model on the sidebar. If you do not see the sidebar, you can view it by selecting ALT+S. The sidebar will then appear.

### Primary Activities - Incident Management Process:

Please note the flow could be different based on processes but this covers primary activities. Escalations to problem or change request or major incident is not covered in this diagram.

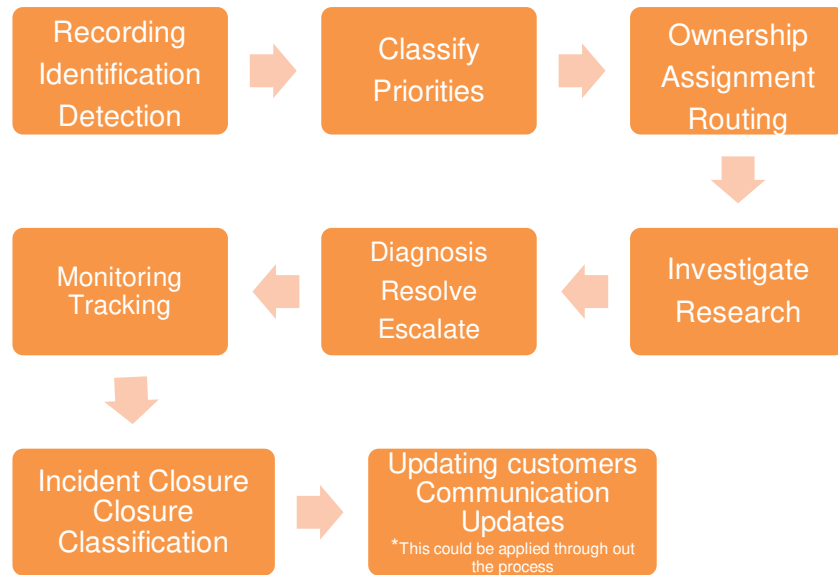


Figure 2 - Primary Activities - Incident Management

## Incident Management – Best Practices

Incident Management is a broad topic which can take many shapes even when following the ITIL framework. There are many strategies that can be used to implement an incident management system therefore it is more profitable to review the common elements of these strategies that allow them to be successful and how those elements can be addressed within the Remedyforce application.

It is strongly recommended that all the elements below be reviewed on a regular basis to ensure their relevance to your organizations goals and their viability in your service delivery environment. Regular review of these elements should become a part of your organizational lifestyle and methodology. To this end, internal committees should be developed and assigned to these elements with the mission of regular assessment and enhancement to the existing configuration elements where useful and necessary.

### Record Planning:

*Record: A document containing the results or other output from a process or activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an audit report, an incident record or the minutes of a meeting. (Source: ITIL, v3)*

An Incident record is created when a user experiences degradation in their available IT Services. There are various fields and field options that are available when creating an incident record. These fields should allow the IT service provider and their agents to gather as much information as possible when capturing the initial incident.

### Methodology:

While each IT service provider maintains unique requirements for their incident record some general fields can be identified for use in most Incident Management processes: impact, urgency, category, type, item and other fields as a short description field, an affected application or affected hardware field, a closure category, a resolution field and a first call resolution checkbox.

---

In addition to the specific requirements for fields the scope and requirements of the fields must also be determined. This is defined by the scope (which users will have access to any given field) and what the requirements for that field will be (hidden, read-only, optional or mandatory) when utilized by both agents and users.

### Value to the business:

Incident records provide a method of maintaining communication with the user as well as a record of actions performed by IT service provider in support of resolving user incidents. Additionally, incident records help establish relationships between users and incidents as well as incidents shared in the IT environment (multiple users experiencing the same incident). These records also, typically, provide the basis for the majority of all metrics and KPI reporting for the Incident Management process.

As a part of any Incident Management process, it is advisable that an IT service provider develops internal policies, processes and work instructions for the frequency of record updates and documentation standards for service desk agents and all IT personnel involved in the Incident Management process.

### Status Overview:

*Status: The name of a required field in many types of Record. It shows the current stage in the Lifecycle of the associated Configuration Item, Incident, Problem, etc. (Source: ITIL, v3)*

Statuses compose the lifecycle of a record in a process and every process has a lifecycle that contains a beginning, middle and end. By defining its statuses an IT service provider defines its process. Statuses should only mark lifecycle events and should never include a terminal event (e.g. the last status should always be closed or the closed status with a different label). This means that resolution codes should never be a lifecycle event (e.g. no statuses for cancellation, known error, etc.) When possible, statuses should not include specific values that can be related in other record elements (e.g. separate statuses for waiting response, parts, management approval, etc.) Finally, statuses should be visible to users to provide clear understanding of IT service provider activities.

### Status Methodology:

In greater detail, statuses represent the pre-work, active work and post work stages. They identify entry criteria, exit criteria and the phases and gates in-between. Additionally, it is important to identify touch points between an Incident Management process and any other given processes in the IT environment. This includes identify the way points for approvals from stakeholders and management teams.

While each IT service provider maintains unique service offerings and processes some general statuses can be identified for use in most Incident Management processes: an initial state (Request/Open), a working status (Work in Progress), a status for actions within the user scope (Pending – Customer), a status for actions within the service provider scope (Pending – IT), a status for the resolution of the incident (Resolved) and a status for the final state (Closed).

Additional statuses may be required or added as needed. These may include statuses to identify transitions between Incident Management and other processes or customer responses through a self-service portal.

### Value to the business:

Statuses are utilized by the Incident Management process to establish response and resolution times for Service Level Agreements. A *Work in Progress* status allows for SLA reporting requirements for response time. A *Pending Customer* status allows a clock-stop on SLAs. A *Pending IT* status allows for a pending status that does not have a clock-stop to track time that IT is responsible for actions on its end that may not be a working status. Finally, *Resolved* status allows for a quality assurance check by the customer to ensure that work has been performed to the customer's satisfaction. The *Resolved* status also allows IT to place responsibility on the customer to communicate with the IT service provider.

### Templates:

A template is a pre-populated incident record. Typically, templates are based on frequently occurring incidents.

---

---

### Methodology:

Leveraging existing data for reported incidents provides the best method for determining what templates are most suited to your environment and customer needs. By examining the most frequently reported incidents to the service desk a profile can be developed for the most commonly reported incidents. Typically, the top five most frequently reported incidents can then be created as templates for use by agents. Fields such as impact, urgency and routing assignments can be populated as well as possible scripts for agents to use to capture additional data (in the notes or description field). Repetition of this methodology on a regular basis will allow you to continue to identify and develop templates for your service delivery organization which remain relevant as your organization continues to grow and mature.

### Value to the business:

Templates provide value in multiple ways to both the service provider and the end user. Templates allow service providers to address incidents more quickly by reducing the amount of information an agent needs to populate in the record and routing them automatically to the appropriate resource for action. Templates also provide greater ease-of-use to customers reporting incidents through the self-service portal and can capture more useful data to the agent triaging the ticket by capturing information through questions pre-populated into the record. Finally, templates ensure greater consistency when being populated by either an agent or a customer as they gather uniform data from any source.

### Workflow Automation and Validation Rules:

Automated workflow allows data populated in an incident record to guide, through a series of rules or specified elements, that record through a process workflow with minimal intervention from an agent. An example of this would be automatic assignment of a record to a specific queue based on the categorization of the incident.

A validation rule will ensure that information is validated based on other information within the record. Agents or customers are required to populate certain data in the incident record form.

### Methodology:

Frequently, when planning for workflow automation, service delivery organizations will have workflow data captured in process documentation and work instruction developed to inform agents on the manual methods for driving a business workflow. These documents should be gathered and triaged by the service delivery team management. The workflows which are easiest to achieve, such as assignment based on categorization, and those which are most frequently utilized, end user onboarding, end user off boarding, simple permissions access, should be prioritized for inclusion into the tool. It is best to shoot for the processes which cover the majority of your service delivery business rather than the minor or rare exceptions. Focus on the processes and instruction that is most relevant to your day-to-day activity. Processes which are not well defined have multiple if/then situations or a large number of required approvals.

However, for validation rules the management team responsible for development of the service delivery tool must establish what elements of the incident record form are critical from both the perspective of an agent and a customer. These two requirements may differ slightly as internal service delivery agents will have an understanding of the organizational requirements that end users do not; for example impact and urgency statements.

End users should be required to provide enough data so that service delivery agents are able to act on that data to properly triage the end user's incident. Service delivery agents should be required to supplement end user supplied data within the service delivery organization's standards (assigning the proper categorization, impact, urgency, setting the proper status, etc.)

### Value to the business:

Automated workflow reduces error in the service delivery environment by creating an automated, repeatable process. Human error is taken out of the equation ensuring that no step is either intentionally or accidentally omitted. This provides a solid foundation for audit requirements. Additionally, automation functionality reduces agent workload by removing tedious manual routing and management of records. Reduction of administrative overhead will allow your agents to focus on more involved efforts when dealing with customer incidents.

Validation rules allow your service delivery organization to obtain actionable data from both agents and customers to ensure that features such as workflow automation, communication, routing, reporting, and customer service. Without actionable and relevant data no service delivery organization will be able to effectively address the needs of the customer or the internal organizational requirements.

---

### Communications Management (Single Point of Contact):

*Single Point of Contact: Providing a single consistent way to communicate with an organization or business unit. For example, a single point of contact for an IT service provider is usually called a service desk (Source: ITIL, v3)*

Communication within the operational aspects of an IT service provider is a critical element when attempting to mitigate, prevent or resolve incidents within an IT environment. Specifically, the core elements of communications being who receives the message, when does that party receive the message and what information is included in the communication. These parties can include users, agents, internal IT department and other individuals or teams involved with Incident Management.

Communication strategies may also involve messages related to projects, exceptions, emergencies or to new or customized processes. Often times one of the challenges, IT service providers face is trying to strike the right balance between too much communication and too little communication.

#### Methodology:

Using the factors above, a matrices or similar tool can be utilized to determine that the right information is passed at the right time to the right party while maintaining a balance of neither communicating too much or too little with the required parties.

Additionally, it is advisable that an IT service provider develops internal policies, processes and work instruction for the frequency of communication updates and non-response for service desk agents and all IT personnel involved in the Incident Management process.

Finally, communication may include operational meetings which occur on a regular schedule with a set agenda. These meetings should focus on the operations of day-to-day activities and the Incident Management process with the intent of disseminating information amongst the various groups responsible for Incident Management within the IT environment.

#### Value to the business:

Efficient and effective communication with regards to IT services and the Incident Management process allows for incidents to be addressed, resolved, prevented and mitigated in a timely fashion.

### Prioritization Overview:

*Priority: A category for the relative importance of an incident, based on impact and urgency. (Source: ITIL, v3)*

Prioritization allows both the organization and the individual agent to set an order of operations for activity. Prioritization is often determined by two separate factors known as Impact and Urgency. These two quantifiable elements take incident prioritization from a subjective assessment to a more objective measurement of the impact of an incident or incidents to an IT environment.

Prioritization is a dynamic function that may change over the lifecycle of an incident and, consequently, may need to be altered to reflect these changes. While initial prioritization of an incident is important, it is also important that the final state of the incident's priority accurately reflect the true values for impact and urgency for accurate reporting against Service Level Agreements.

For a more in-depth discussion of the utilization and value of Prioritization please refer to the [BMC white paper on Priority, Impact and Urgency](#).

### Categorization Overview:

*Categorization: A named group of things that have something in common. Categories are used to group similar things together, usually to three or four levels of granularity. (Source: ITIL, v3)*

Categorizing incidents allows two important functions to occur in an Incident Management process: the routing of incidents to the part of the IT organization responsible for their resolution and the easy reporting of relevant data to the appropriate level of management.

Categorization is, typically, the most difficult aspect to develop due to the unique nature of all IT Service Providers and the customers who consume their services.

For a more in-depth discussion of the utilization and value of Categorization please refer to the [BMC White Paper: Categorization](#).

### Incident vs. Service Request

As we are discussing Incident management, it's important to understand the difference between Incident and service request. We will not cover this in detail however this should give you an overview. Please see [BMC White Paper: Service Request Management](#)

Incident	Service Request
An incident is an unplanned interruption to an IT Service or reduction in the quality of an IT service. (Source: ITIL, v3)	A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service (Source: ITIL, v3)
Service disrupted	Request
Not planned	Planned
Something is broken, requires fix	Need something (standard IT service)
Example - Printer not working	Example - New Hire Request ,password reset

Table 1 - Incident vs. Service Request



## Incident Management – Application in BMC Remedyforce

Remedyforce supports Incident creation from below methods giving great flexibility.

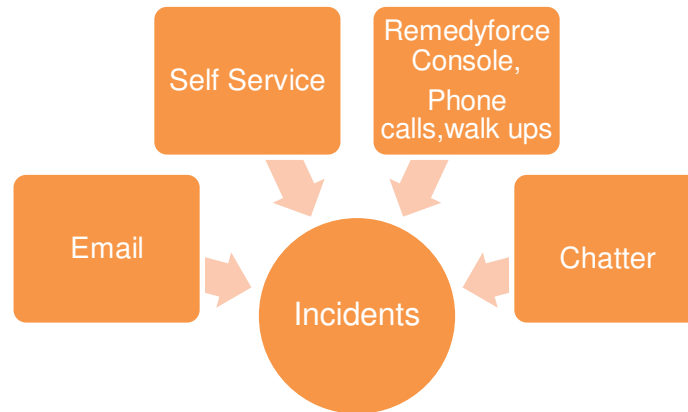


Figure 3 - Incident Creation Methods in Remedyforce

### Record Planning Overview:

BMC Remedyforce allows you to configure your incident record. Customers can leverage several established fields, add fields required to meet your individual organizational requirements or even remove fields to collect pertinent data. Customers can leverage multiple field types (for a list of custom field types available on the Salesforce platform visit Salesforce Help: [Custom Field Types](#)) to meet their data collection requirements. Additionally, these fields can be leveraged to display data from other objects in the database such as information on a Configuration Management Database (CMDB) configuration item (CI) through relationships established between the objects.

BMC Remedyforce can leverage several of these field types to meet whatever unique requirements are necessary for your service delivery organization.

### Out-of-the-box, BMC Remedyforce supports:

- Client ID
- Account
- Category
- Description
- Resolution
- Impact
- Urgency
- Priority
- Status
- Opened Date
- Responded Date
- Due Date
- Closed Date
- Service
- Service Offering
- Configuration Item
- Outage End
- Staff
- Owner

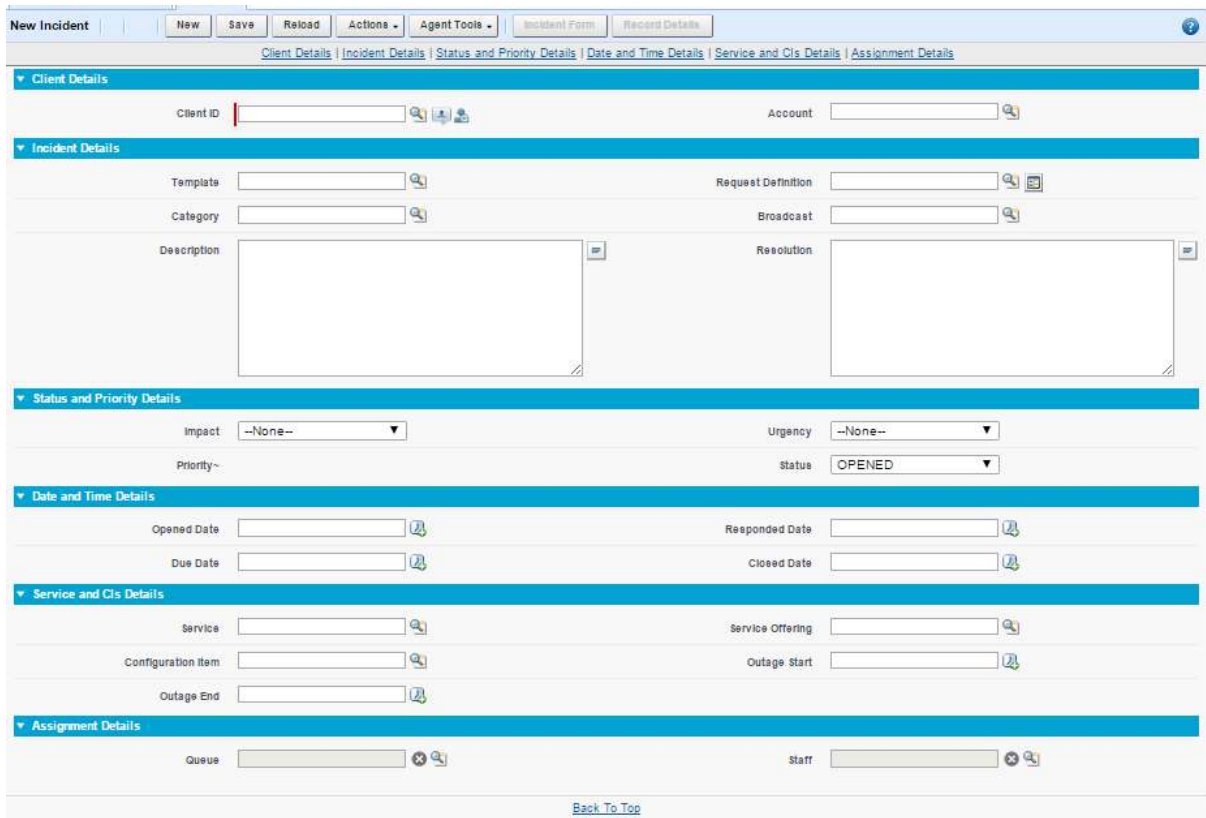


Figure 2 – BMC Remedyforce Incident Form

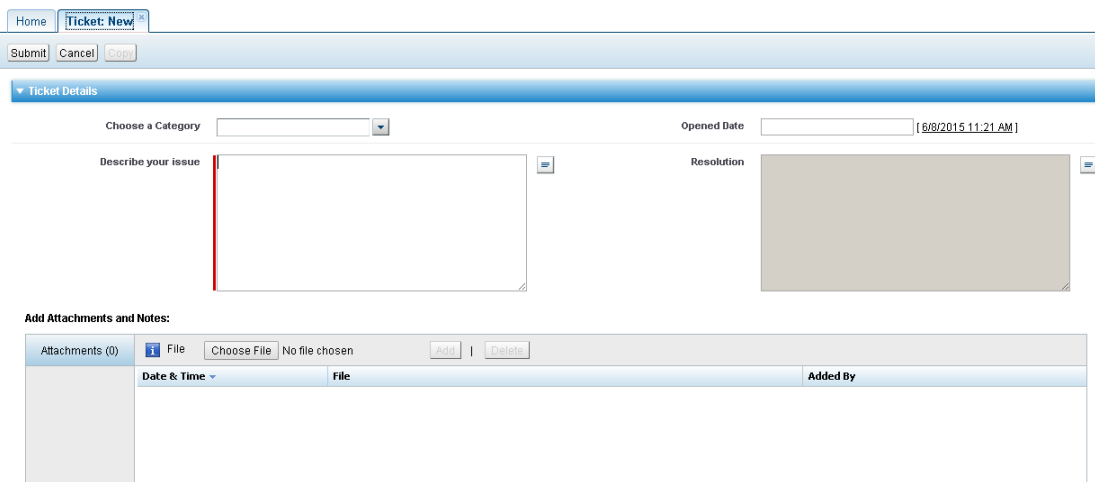


Figure 3 – BMC Remedyforce Self-service Form

---

### Status Overview:

The status of a record tracks its progress from opening to closure. BMC Remedyforce provides two default states: Open and Closed. However, you can track more stages by creating status records and assigning descriptions that accurately describe each stage.

*Although you can create multiple status records to assign to the Open and Closed states, you can designate only one state as the default for any given status.*

You can also configure out-of-the-box or custom status records as work status only if they apply to the Incidents object and are assigned to the Open state. The work clock for incident records calculates only the time for which an open incident is assigned to a work status. The Work Status setting enables you to track the total time for which staff members have actively worked on an incident during the business hours of an organization. For example, you can configure the Opened or In Progress status records as work status. In this case, the time spent on an incident in the Opened or In Progress status is considered in the total work time. However, the work clock does not calculate the time spent on that incident in any other status, such as Waiting for Reply or Approval Requested.

### Templates:

To help ensure accuracy and completeness, BMC recommends that you use a template to create records. Templates help you to configure commonly used workflow, ensure consistency in the way information is captured, increase productivity and efficiency, and reduce errors. Using templates, you can prepopulate fields on a form, which reduces the need to enter commonly used data, or create records to provide an automated workflow process.

Depending on the requirements of your staff members, you can create templates for commonly occurring incidents, tasks, change requests, service requests, and releases. Additionally, templates can be leveraged by end users through the Self-Service portal.

Use "System Template" checkbox to hide automation templates which are used in workflows or service request etc. The system templates are not shown in the Template lookup in the BMC Remedyforce Salesforce page layout. This way it keeps the template list clean.

### Workflow Automation and Rules:

BMC Remedyforce has created out-of-the-box workflows that are available for you to use. You must activate these workflows to use them. For more information, see [Salesforce Help: Creating Workflow Rules](#). The following table describes the out-of-the-box workflows.

Out-of-the-box Workflow Automation and Rules in BMC Remedyforce Include:

- Apply template to BMC Server Automation created incident
- Apply template to End User Experience Management created incident
- Notify incident owner when change request linked to incident is closed
- Notify incident owner when each linked task is closed
- Notify incident owner when final task linked to incident is closed
- Notify staff of incident due in 1 hour
- Notify staff of incident nearing due date
- Notify staff when no action has occurred for 24 hours
- Notify the assigned staff member when an incident has been marked for follow up
- Notify the assigned staff member when an incident is created and assigned to the staff member
- Notify the assigned staff member when an incident is reassigned to the staff member
- Notify the assigned staff member when an incident is reopened
- Notify the client when an incident is closed
- Notify the client when an incident is created
- Notify the client when an incident is reopened
- Open Incident from email
- Update the incident's status through email

---

### Communications Management (Single Point of Contact):

Communication management has three main components within BMC Remedyforce:

- Email Templates
- Email Alerts
- Workflow Rules

Each of these elements contributes to successful management of communication between both agents and end users within BMC Remedyforce. Email templates dictate what information is provided to either the agent or end user. The Workflow automation and rules dictate when and to whom that information is disseminated. Email templates may be configured to include data from the incident record, custom logos and signatures or for notifications about agreement milestones.

BMC recommends that you first clone and then edit the out-of-the-box email templates. If you receive an error message when cloning a BMC Remedyforce out-of-the-box email template, see [Resolving an error with cloning a BMC Remedyforce email template](#).

The out-of-the-box email template is available in your organization at Remedyforce Administration > Configure Email > Email Templates.

You can customize the fields that are used in the templates to display the information of your choice in the email message. You can include the fields that are available for the objects. Select the object in the Related to Type field while creating an email template. Use the API Names field to obtain the values of these fields in the email templates. To see a list of fields available for an object, navigate to Setup > Create > Objects or Remedyforce Administration > Manage Objects > Create and Edit Objects. The list of fields that you can use in an email template is displayed in the Custom Fields & Relationships section.

### Prioritization Overview:

Within the BMC Remedyforce application, priority has its own Custom Object in the database which is leveraged by multiple other objects in the database (Incident, Problem, Change, Release and Task). Impact and urgency values are also therefore utilized by multiple objects in Salesforce database.

This means that BMC Remedyforce can use priority to leverage workflows to alert an appropriate group within a service delivery organization, escalate a ticket, and allow association with a particular Service Level Agreement, or many other functions. If a particular category is associated with a business service or area deemed critical to the organization, the priority of the ticket can be elevated by BMC Remedyforce through automation. This can be useful when receiving ticket information from an automated source such as monitoring or asset management software.

### Categorization Overview:

Within the BMC Remedyforce application categorization has its own Custom Object in the database which is leveraged by multiple other Objects in the database (Incident, Problem, Change, Release and Task). This means that categories can be utilized across all ITSM process and can leverage elements of the taxonomy. This gives your organization a great deal of flexibility when establishing a category structure and taxonomy.

This structure inside of the database also allows for Customer facing categorization to be incorporated as well. The ability for BMC Remedyforce to utilize workflows to automatically route or re-categorize tickets means that end-users can select from a more “customer friendly” taxonomy which can automatically be re-categorized by a workflow trigger to fit into an appropriate structure for an IT organization. Workflows can also automatically route tickets to the appropriate support group based on categorization.

Categorization can also help prioritize a ticket. If a particular category is associated with a business service or area deemed critical to the organization, the urgency of the Category can be configured so that the priority of the ticket can be elevated by BMC Remedyforce through automation. This can be especially useful when receiving ticket information from an automated source such as monitoring or asset management software, allowing for rapid notification of responsible parties, tracking of the duration of the outage and faster resolution times.

---

Some other areas to consider for planning include:

### **Making fields required for Staff or end users:**

It is important to make sure that you have enforce certain rules so that you can get required reporting as well as the process is followed. For example resolution is required before closing incident as simple validation rule can take care of this. Some fields could be marked as required on the forms based on layouts making them required on field sets.

### **Using Actions/Notes Incident details:**

Activity log plays important role. Staff should add/use Remedyforce actions to document the activity. This way all communication is documented on the Incident record and if the record moved from one queue to another queue or if staff is away everything in once place. Promote use of public and private notes (actions) to help communication and updates.

### **Incident and Configuration Item and CI explorer:**

Incident may have impact on service or CI. Remedyforce gives ability to imports Configuration items and link them to accounts or clients. If the user is reporting issue relate to impacted CI staff can easily link CIs for that client to Incident. They can also use CI explorer to see relationship and other records. Helping in reporting as well as diagnosis. S

### **Tasks and Incident management:**

A task is a unit of work that must be completed as a step in resolving an incident. You can create a task from an existing incident or directly using the Task page. Task could be used to distribute the work across teams internally keeping the primary ownership with specific team. They also help in fulfilment process. You can also control execution order of dependent tasks. For example, one of your clients calls a staff member to report that the common printer is not working. The staff member checks the printer and finds that the printer cartridge needs to be replaced. Additionally, the printer paper is getting over and would need to be purchased. The staff member creates an incident to record the issue of the printer not working. Next, the staff member creates the following tasks that must be completed to resolve the incident:

Task 1: Purchase the printer cartridge.

Task 2: Replace the faulty printer cartridge with the new printer cartridge.

Task 3: Purchase the printer paper.

Task 4: Refill the printer paper in the printer.

### **Incident and Knowledge management:**

Remedyforce has powerful knowledge management module with "smart search mechanism". The knowledge articles could be internal or external (available for client's vs staff). Helps staff to resolve issue, build knowledge base, receive feedback. Make sure that you roll out the "self-help" option to reduce the incident count.

### **Incident and Service Level agreements:**

If companies plan to rollout service level management with Incident management consideration factors like statuses and Priorities (foundation data) etc. would be important. For more information see the Remedyforce help document: [BMC Remedyforce SLA](#)

### **Surveys:**

Feedback on service is crucial to improve services and to gauge how the helpdesk is doing.

Remedyforce provides out of box survey functionality. For more information see the Remedyforce help document: [BMC Remedyforce Surveys](#)

### **Reporting and Quick views:**

Remedyforce is shipped with great reports around time tracking and average resolution time, first call resolution and other great reports list is available in the Remedyforce help document: [BMC Remedyforce Report List](#)

Use of quick views with reporting gives lot of flexibility. Here is a list of out of box quick views: [BMC Remedyforce - Out of Box QuickViews](#)

---

### Incident Management – Configuration Steps

#### Record Planning Overview:

Please reference the Salesforce publicly available information on form field creation and configuration available at Salesforce Help: [About Custom Fields](#).

#### Status Overview:

Please reference the BMC publicly available information on status creation and configuration available at Remedyforce Help: [Creating Status Records](#).

#### Templates:

Please reference the BMC publicly available information on template creation and configuration available at Remedyforce Help: [Creating Templates](#).

#### Workflow Automation and Rules

Please reference the Salesforce publicly available information on Workflow rule creation and configuration available at Salesforce Help: [Managing Workflow Rules](#).

#### Communications Management (Single Point of Contact):

Communications Management is achieved by a combination of workflow rules and email templates. You can get additional information from the link above for Salesforce on "Managing Workflow Rules." Please reference the BMC publicly available information on email template creation and configuration available at Remedyforce Help: [Creating an Email Template](#).

#### Prioritization Overview:

Please reference the BMC white paper for more details at: [BMC White Paper: Impact, Urgency & Priority](#).

Please reference the BMC publicly available information on priority creation and configuration available at Remedyforce Help: [Creating Priorities](#).

#### Categorization Overview:

Please reference the BMC white paper on categorization at [BMC White Paper: Categorization](#).

Please reference the BMC publicly available information on category creation and configuration available at Remedyforce Help: [Creating Categories](#).

---

## In Summary

BMC Remedyforce Incident Management enables your agents and end users the ability to submit and administer incidents and enables your service delivery team to quickly and efficiently resolve those incidents. This capability can provide value by improving employee productivity, reducing administrative overhead, empowering your agents and increasing both employee and customer satisfaction. We encourage you to check out our very active user community to get involved with additional discussion on this topic or engage with our product teams to recommend feature enhancements to the solution. Please visit us at: [bmc.com/communities](http://bmc.com/communities).

BMC delivers software solutions that help IT transform digital enterprises for the ultimate competitive business advantage. We have worked with thousands of leading companies to create and deliver powerful IT management services. From mainframe to cloud to mobile, we pair high-speed digital innovation with robust IT industrialization—allowing our customers to provide amazing user experiences with optimized IT performance, cost, compliance, and productivity. We believe that technology is the heart of every business, and that IT drives business to the digital age.

**BMC – Bring IT to Life.**

