



Incident Management Module

Baseline Configuration Guide

Document Version: 01.00.03 | April 2019

Rsam © 2019. All rights reserved

[Privacy Policy](#) | [Terms of Service](#)

Contents

- About Rsam Baseline Configuration Guides 3
- Baseline Configuration Overview 4
- Incident Management Structure 5
 - Object Type 6
 - Record Categories 6
 - Record Types 6
- Home Page Tabs 7
- Incident Management Workflow 8
 - Workflow Diagram 8
 - Workflow States 10
 - Workflow Roles 11
 - Workflow Buttons 12
- Importing Data 15
 - Importing Incidents 15
- Appendix 1: Auto-Assigning Incidents 16
- Appendix 2: Rsam Documentation 17
 - Incident Management Module Tutorial 17
 - Online Help 17

About Rsam Baseline Configuration Guides

Rsam Baseline Configuration Guides provide you the information needed to understand the pre-defined configurations for each module. These guides should be referenced to gain a better understanding of how the module is configured and can be used out-of-the-box.

Baseline Configuration Overview

This document describes the baseline configuration and structure for the Rsam Incident Management module. The baseline configurations for the Incident Management module allow your users to manage a wide variety of incidents. The pre-configured activities help streamline your program by leveraging a central repository, allowing for data normalization, workflow, and timely reporting in a more automated fashion.

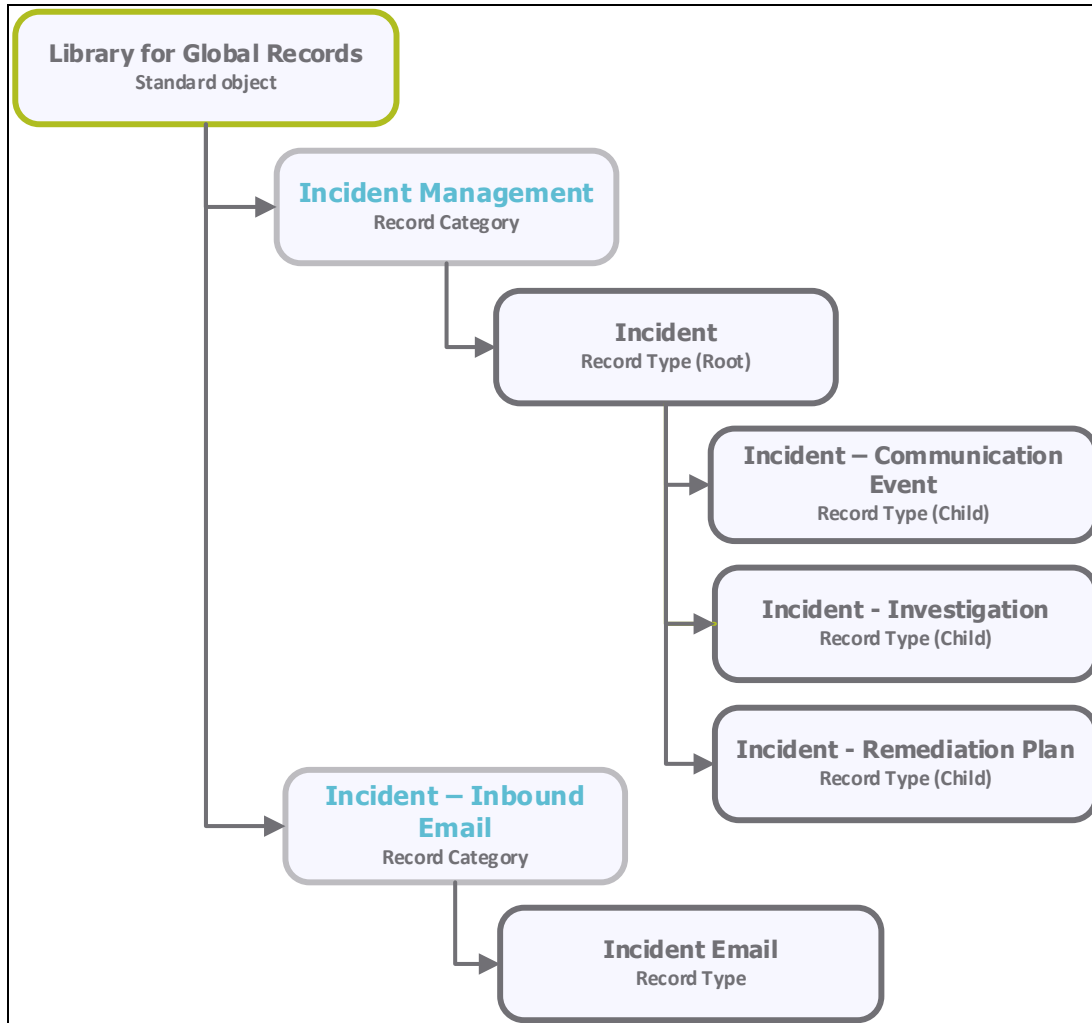
The following is a list of elements that have been configured in the Incident Management module:

- Structure
- Home Page Tabs
- Incident Management Workflow
- Data Import

The information on the elements mentioned above will provide a baseline understanding before you leverage the *Incident Management Step-by-Step Tutorial* or begin to tailor the module to meet your unique requirements.

Incident Management Structure

All incidents in the Incident Management module are stored in the object type, Library for Global Records.



Object Type

The following object type has been pre-configured in this module.

Object Type	Usage
Library for Global Records	A standard library object under which all the incident records are stored.

Record Categories

The following record categories have been pre-configured in this module.

Record Category Type	Usage
INC: Incident Management	A category type that includes the Incident record type and its child record types: Communication Event, Investigation, and Remediation Plan.
IND: Incident - Inbound Email	A category type that includes the Incident Email record type.

Record Types

The following record type has been pre-configured in this module.

Record Type	Usage
INC: Incident	This is a root-level record that contains all the incident-related information. This record can have multiple child records or record types.
INC: Incident – Investigation	This is a child-level record of an incident record (one-to-many). The investigation record tracks investigative actions and allows a user to attach supporting documentation.
INC: Incident - Communication Event	This is a child-level record of an incident record (one-to-many). The communication record allows a user to track communication (Phone, Email, and so on) with another party and to attach evidence of that communication event.
INC: Incident - Remediation Plan	This is a child-level record of an incident record (one-to-many). This record allows a user to track plans, dates, assignment, and evidence.
INC: Incident - Email	Incidents coming into Rsam from Email Listener are originally created as record of this type. Then they are automatically converted to an Incident record.

Home Page Tabs

The Baseline Configuration of the Incident Management module contains several Home Page tabs. These tabs can be configured for various roles and then can be assigned to your users to complete their tasks. The following Home Page tabs are available in the Incident Management module.

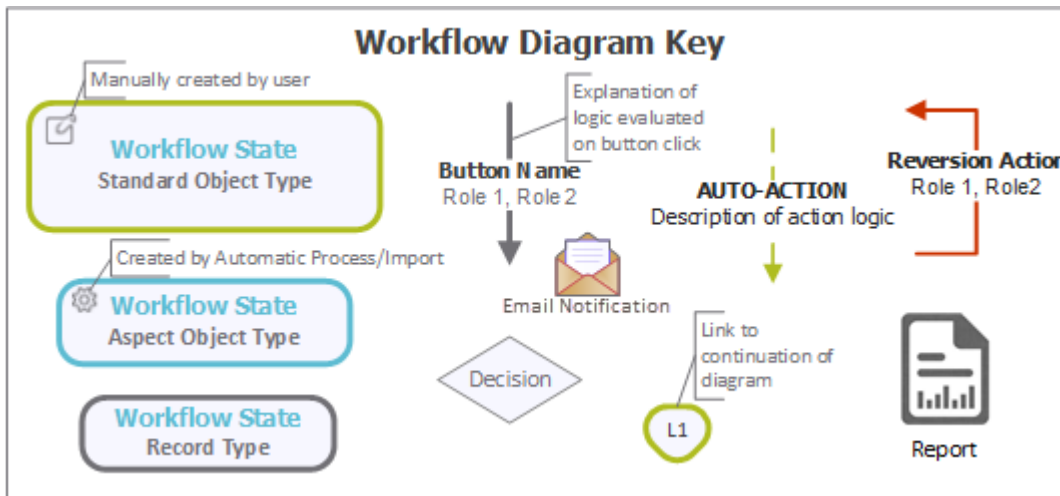
Home Page Tab	Description
INC: Incident Management (grouping tab)	Allows quick access to the subtabs available in the Incident Management module.
INC: Incident Management Home	This is a standard Home Page tab that allows the users to view a list of incident records by categories, create a new incident record, and view various dashboard charts.
INC: Incident Navigator	This is a record navigator that allows the users to view incidents grouped by various attributes such as workflow state, status, and so on).

Incident Management Workflow

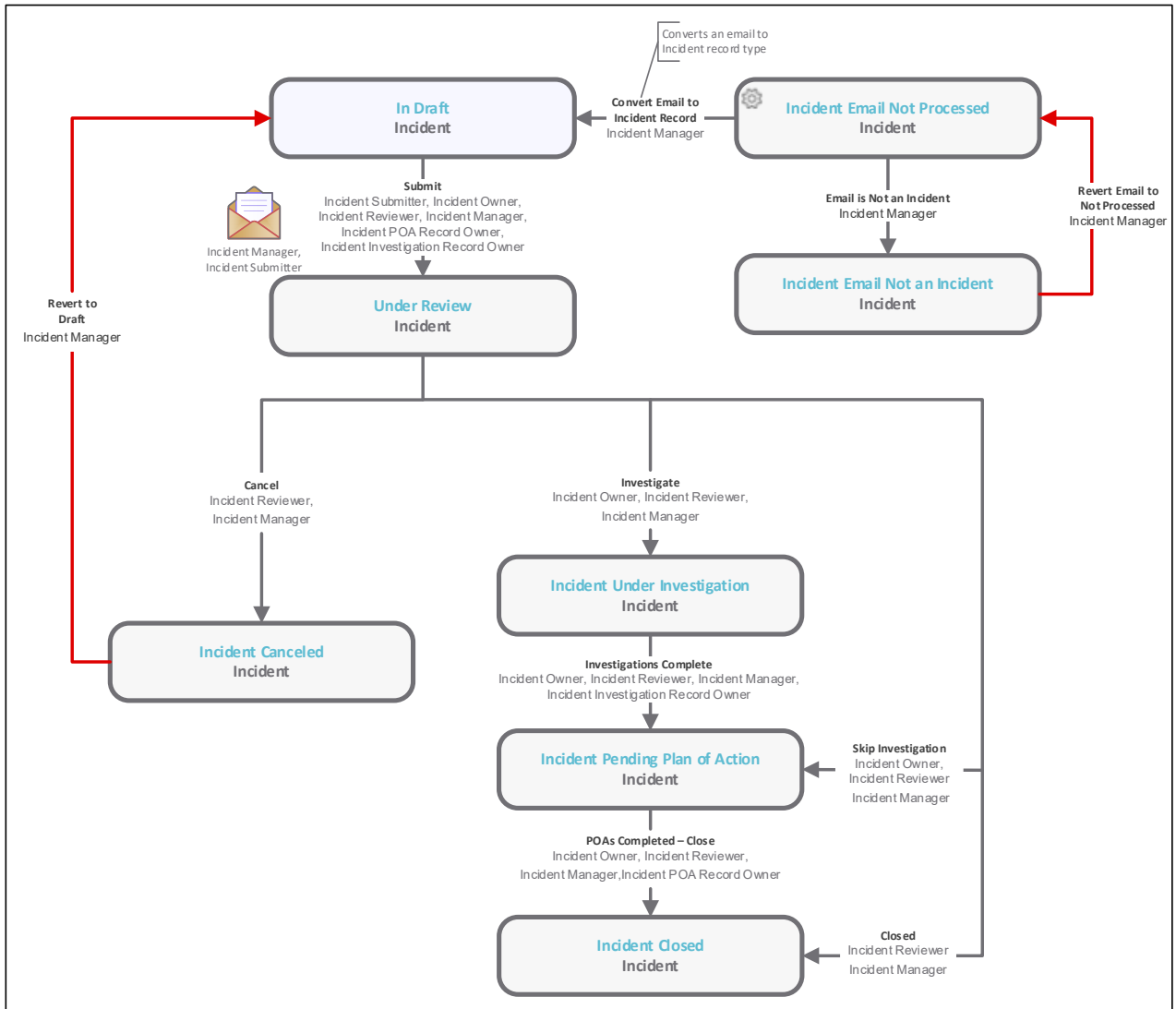
This section covers the workflow diagram, workflow states, workflow buttons, and workflow roles associated with the baseline Incident Management workflow.

Workflow Diagram

Before proceeding to the workflow, it is recommended that you familiarize yourself with the following Rsam workflow diagram key.



The following diagram shows the baseline Incident Management workflow.



Workflow States

The following is a list of states associated with the baseline Incident Management workflow.

Workflow State	Description
INC: In Draft	An incident that is created automatically enters this state. In this state, an owner is assigned to the incident. After performing the necessary steps, the incident owner submits the workflow to the Under Review state.
INC: Under Review	In this state, an incident is reviewed and analyzed thoroughly. Depending on the outcome of analysis, the incident is submitted for further investigation or to seek an approval on the remediation action plan, or it can be closed straightaway if proper measures are in place or cancelled if no proper evidence is available.
INC: Incident Under Investigation	An incident enters this state from the Under Review state when it is required to investigate the root cause of incident. In this state, a remediation plan is created and proposed.
INC: Incident Pending Plan of Action	An incident can enter this state from either the Under Review state or Incident Under Investigation state. In this state, the remediation plan is approved and then the incident is closed.
INC: Incident Closed	An incident enters this state from either the Under Review state or Incident Pending Plan of Action state after that incident has been mitigated and necessary measures to avoid its recurrence has been taken.
INC: Incident Cancelled	An incident enters this state from the Under Review, Under Investigation, or Pending Plan of Action state due to some of the reasons, such as the incident has zero effect on the organization or has no proper evidence that needs further action.
INC: Incident Email Not Processed	This state flags records created by Email Listener that have been not analyzed to verify whether they are related to an incident.
INC: Incident Email Not an Incident	This state flags records created by Email Listener that do not qualify as an incident.

Workflow Roles

The following is a list of workflow roles that perform tasks associated with the states in the baseline Incident Management workflow.

Note: Sample users for each of these roles are optionally provided with the baseline module installation package.

Role	Account ID	Description
INC: Incident Submitter	r_incident_submitter	This role is assigned to a user that submits incidents.
INC: Incident Owner	r_incident_owner	This role is assigned to a user that has the responsibility to mitigate the effect of incidents and resolve them completely by adopting appropriate measures. This role allows a user to create, view, update, and delete incidents records, and view email records.
INC: Incident Reviewer	r_incident_reviewer	This role is assigned to the user that needs to review incident records. A user with this role reviews and approves a remediation plan and helps an incident owner to resolve and close an incident case. This role allows a user to create, view, update, and delete incidents records.
INC: Incident Manager	r_incident_manager	This role is assigned to the user that needs to assign incidents to users. A user with role can create, view, update, and delete incident records, and create, view, and update email records. Typically, this role allows a user to perform all the tasks in each state.
INC: Incident POA Record Owner	None	This role is assigned to a user who has to work on a specific portion of an incident. This role has read-only access to some tabs, and create, read, and update access to the Communication, Time Entries, and Remediation tabs.
INC: Incident Investigation Record Owner	None	

In addition to the above roles, the Rsam installation package includes an administrative role, **U: Object Administrator**, as well as a sample user for that role, **r_admin**. This user has access to all record types, object types, workflow states, and workflow buttons across all Rsam baseline modules. Rsam Administrators should take necessary precautions to restrict standard users from accessing Rsam with this administrative role.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Incident Management workflow.

Button	Available to	Notification	Description
INC: Revert to Draft	Incident Manager	No	Available in the Incident Under Investigation, Incident Pending Plan of Action, Incident Closed, Incident Cancelled, and Under Review states to move the incident record workflow to the In Draft state.
INC: Submit	Incident Submitter Incident Reviewer Incident Manager Incident POA Record Owner Incident Investigation Record Owner	Yes	Available in the In Draft state to move the incident record workflow to the Under Review state.
INC: Investigate	Incident Owner Incident Reviewer Incident Manager	No	Available in the Under Review state to move the incident record workflow to the Incident Under Investigation state for investigation purpose.
INC: Skip Investigation	Incident Owner Incident Reviewer Incident Manager	No	Available in the Under Review state to move the incident record workflow to the Incident Pending Plan of Action state for skipping the investigation step.
INC: Closed	Incident Reviewer Incident Manager	No	Available in the Under Review state to move the incident record workflow to the Incident Closed state.
INC: Cancel	Incident Reviewer Incident Manager	No	Available in the Under Review, Incident Under Investigation, and Incident Pending Plan of Action states to move the incident record workflow to the Incident Cancelled state.

Button	Available to	Notification	Description
INC: Investigations Complete	Incident Owner Incident Reviewer Incident Manager, Incident Investigation Record Owner	No	Available in the Incident Under Investigation state to move the incident workflow to the Incident Pending Plan of Action state.
INC: POAs completed – Close	Incident Owner Incident Reviewer Incident Manager Incident POA Record Owner	No	Available in the Incident Pending Plan of Action state to move the incident record workflow to the Incident Closed state.
INC: Email is not an incident	Incident Manager	No	Available in the email records that are created by Email Listener. Clicking this button moves an email record workflow to the Incident Email not an Incident state.
INC: Convert email to incident record	Incident Manager	No	Available in the email records that are created by Email Listener. Clicking this button converts a specific email record into an incident record type and places it in the In Draft state.
INC: Revert Email to Not Processed	Incident Manager	No	Available in the Incident Email not an Incident state. Clicking this button transitions the email record workflow to the Incident Email Not Processed state.
INC: AUTO: Incident Email (new)	N/A	Yes	This workflow button is used when automatically creating an incident from an email. This button is associated with the handler— INC: Notification - New Incoming Incident Email . During a record import, this button will automatically notify the <i>Incident Manager</i> of a new Incident being created.
INC: AUTO: Incident - Investigation - On Record Create	N/A	No	This button is used to automatically populate specific fields used in creation of new investigations. The fields that are automatically populated can be changed from the handler— INC: Auto Populate Initial Incident Investigation Fields .

Button	Available to	Notification	Description
INC: AUTO: Incident - On Record Create	N/A	No	This button is used to automatically populate specific fields used in creation of new incidents. The fields that are automatically populated can be changed from the handler— INC: Auto Populate Initial Incident Fields.

Importing Data

Default import maps have been created for the baseline record categories to help you import incidents with little to no configuration required in your Rsam instance.

Importing Incidents

Incident records can be imported using the *Incident Email Message* map. This map allows you to automatically import incident-related emails and converts them to incident records.

Appendix 1: Auto-Assigning Incidents

In addition to assigning the owners to incidents manually, Rsam provides you the ability to automatically assign owners to individual incidents based on a specific keyword imported from the Email Listener. This method is commonly used for technologies by the team responsible for addressing incidents on those technologies. For example, Java, Adobe, Apache, and SQL are some of the most common technologies that are assigned using this method.

Note that managing your Rsam instance with a large number of individually assigned incidents can affect the overall performance of your Rsam instance. It is recommended to assign the owners at the object level or the level above the object. Otherwise, consider upgrading your system requirements. For more information, refer the *Rsam Performance Guide*.

Appendix 2: Rsam Documentation

Incident Management Module Tutorial

For a detailed walk-through of the Incident Management Module user experience, refer the *Incident Management Module Step-by-Step Tutorial*. You should have received the *Incident Management Module Step-by-Step Tutorial* along with the Incident Management Module instance. If not, contact your Rsam Customer Representative to obtain an electronic copy of the *Incident Management Module Step-by-Step Tutorial*.

Online Help

This document provides an overview of the Incident Management Module configuration. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Enter **Username** as *r_admin* and **Password** as *password*.
2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.

