# Incident

The **Incident module** of **ACMS** is for managing incidents. Existing paper-based investigation processes can be replicated electronically using this module.

Key features include:

- Log incidents, set due dates for investigations, and allocate to the appropriate investigators
- Attach incidents to people
- Collect and upload evidence
- Enter the sequence of events on a timeline
- Choose causes from the RSSB cause set or build your own
- Make recommendations and record outcomes, such as, action taken and development plans
- · Generate Investigation reports using to your own company standard
- Manage the approvals cycle for investigations

#### On this page:

- Incident and Investigations Workbench
- Causes
- Incident Categories
- Incident Properties
- Incident Types
- Investigation Types
- Investigation Remits
- Investigators
- Post-Incident Decision (PID)
- Candidate Dashboard Tab
- My Page Tabs
- Reports and Dashboards

# Incident and Investigations Workbench

All incidents and investigations can be viewed using the Incident and Investigations Workbench. The workbench has two views:

- The Incident view, which allows the user to search on the basis of the type, status date and location of incident.
- The Investigations view, which allows the user to search on the basis of the status, due date and content of the investigation.



Once an incident or investigation is selected, the user can move to the detail screen, which has tabs for all the different stages of an investigation.



#### Causes

An important part of an investigation is determining the causes of an incident. Train operating companies use different causation models according to their own standards.

Causes on ACMS are modelled using 'cause sets'. A cause set that represents the RSSB standard is provided by default. This can be used directly, edited to match a custom standard, or abandoned in favour of a completely different custom set.

Cause sets are a tree of related causes with guidance notes, that help the investigator choose the most appropriate causes for an investigation. Cause sets can have as many items and nested levels as required, and the guidance notes are completely customisable.

# **Incident Categories**

Companies need to manage different categories of incident and produce reports and statistics based on these categories. Typically, TOCs use these categories:

- Operational
- Occupational

Incident categories are configurable.

#### **Incident Properties**

Incident properties are used to capture the data about an incident, in a way that allows for granular searching and reporting. Incident properties can be recorded, against the incident as a whole, or against individuals involved in the incident. There are many default properties available in **ACMS**, examples of properties recorded against incidents as a whole are:

- Journey Direction
- Platform
- Journey Start Time
- Weather

Examples of properties recorded against individuals are:

- Fatigue Index
- Time on since last break
- · Alcohol and Drugs test results

If these properties do not meet the need, then there is also a facility to add custom properties.

## **Incident Types**

Incident types allow an organisation to configure a name for a specific type of incident, such as a 'Fail to Call' or 'Platform Incident' and dictate what pieces of information (incident properties) should be collected for that type of incident. Incident Types belong to Incident Categories.

The Incident Type Admin screen is a matrix of tick-boxes, allowing selection of all the different incident properties, for each incident type. It also allows for the selection of a default 'Investigation Type' for each one.

#### **Investigation Types**

Investigation types allow the modelling of different investigation processes for different incident types. So, for example, a minor incident might need only 7 days to be completed and require a simple report, whereas a major incident might need much longer and require a more complex report.

Custom report templates can be created on a per Investigation Type basis.

## **Investigation Remits**

Investigation remits can be created and issued by ACMS using a combination of pre-defined, boilerplate text, and custom information.

## Investigators

Only authorised investigators have permission to edit investigations. There are four levels of authorisation on ACMS as follows:

- Investigator an Investigator can contribute evidence on an investigation. They can only see the investigations to which they are allocated.
- Lead Investigator a Lead Investigator has the same privileges as an Investigator, plus they can also lead an investigation which gives them
  the ability to submit the investigation for approval and add other investigators. They can only see the investigations to which they are
  allocated.
- Approver (also known as Designated Competent Person) an Approver can approve (or reject) investigations. They can see all investigations.
- Investigations Admin (also known as Chief Investigator) an Investigations Admin can do everything, including log new incidents, and start
  investigations.

This allows granular control of who can modify what.

## **Post-Incident Decision (PID)**

A Post-Incident Decision (PID) can be set against a candidate in the system. This is simply a marker, which gives an indication of the recommended course of action for this person, should they have an incident. There are three levels of PID (LOW, MEDIUM and HIGH).

The names for these levels are customisable.

#### **Candidate Dashboard Tab**

When the Incident module is activated a tab appears on the candidate dashboard that enables users with appropriate security privileges to find all the incident data relevant to a particular candidate.

#### My Page Tabs

When the Incident module is activated a tab also appears on 'My Page' so that candidates can see their own incident data.

## **Reports and Dashboards**

There are many standard reports associated with the Incident Module. These include, but are not limited to:

- Incident Summary Report: this shows all incidents
- Incident Property Report: this shows all incidents that have data for the given property
- Investigation Status Report: this shows a red, amber or green status for investigations, depending on when they are due to be completed
- . Overdue Investigation Report: this shows all overdue investigations
- Recommendations Reports: this shows all recommendations

There are also individual reports, for just one person, available from the candidate dashboard:

- CDP History Report: this details all the competence development plans for this person
- Incapacity History Report: this details all the incapacities (periods off role for medical reasons) involving this person
- Incident History Report: this details all the incidents involving this person

These are often useful as contributing evidence in an investigation.

Custom reporting and bespoke dashboards are available.