MITRATECH

OpRiskControl Incident Manager Users' Guide

5.5.0

OpRiskControl® Incident Manager

Approval and Publishing History:

OpRiskControl® Incident Manager Users' Guide

Version 5.2.0	Approved and Published	February 2015
Version 5.3.0	Updated, Approved and Published	June 2015
Version 5.4.0	Updated, Approved and Published	March 2016
Version 5.4.1	Updated, Approved and Published	April 2016
Version 5.5.0	Updated, Approved and Published	November 2016

If you need support for OpRiskControl Incident Manager™, please contact the Mitratech support team by sending an email to: support@mitratech.com.

For more information about Mitratech, visit our web site: http://www.mitratech.com.

Contents

1. Introduction

1.1. Welcome

This User Guide contains the information you need to enter and manage information using the Web Browser-enabled OpRiskControl Incident Manager.

1.2. Purpose Of The Software

OpRiskControl Incident Manager simplifies the task of managing general operational Incidents. This software allows you to enter an unlimited number of Incidents by division (or client or project), department, location, asset or type of Incident.

With OpRiskControl Incident Manager you can quickly evaluate the Incidents with the highest impact, and then manage Actions to address the Incident.

1.3. Technical Support

Email support@mitratech.com if you have a problem with this software.

2. Overview

This software is used to manage general organisational Incidents.

It provides a generic framework for establishing the context, identification, analysis, evaluation, action, monitoring and communication of Incidents.

2.1. Functionality

OpRiskControl Incident Manager provides the following functionality:

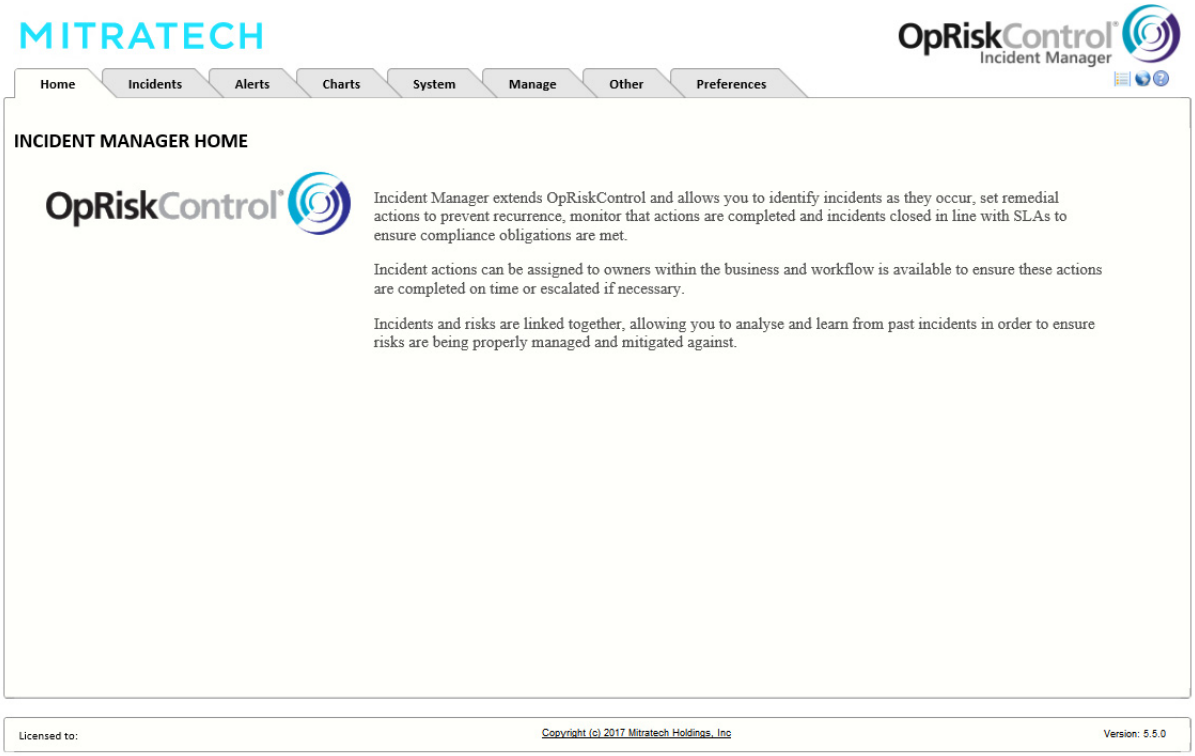
- Incident name, description, the dates an Incident occurred, was reported, recorded, reviewed and closed, the Incident status, type of Incident and more.
- Incident context by department, division, location, asset or user defined code.
- Up to nine levels of Recurrence (most customers use five) and nine levels of Severity (most customers use five) giving greater granularity of Incident rating.
- A record of the names of the users associated with the Incident: Recorded by, Reported by, Contact and the Owner.
- Links to related Risks.
- A link to related documents at both Incident and Action levels.
- Full set of standard reports to review Incident status, assessments, Actions, by location, project, department, division, and so on. Reports show the overall status of the Incident as well as the status of each Action.
- OpRiskControl Incident Manager can give different views of organisation-wide Incidents, and produce reports for various levels of the organisation.
- Create reminders of incomplete Incident reviews.

2.2. About This Guide

This guide describes all the menus and features that are available. However, your system may have some features turned off or you might not have permissions to access all the features. Therefore you might not see everything described in this guide.

2.3. Home Page

When you start OpRiskControl Incident Manager you are presented with the home page. (This home page may be customised by your web site developer.) This page is displayed when Display Home Tab is selected on the *System*, *System Setting*, *Setup* tab.



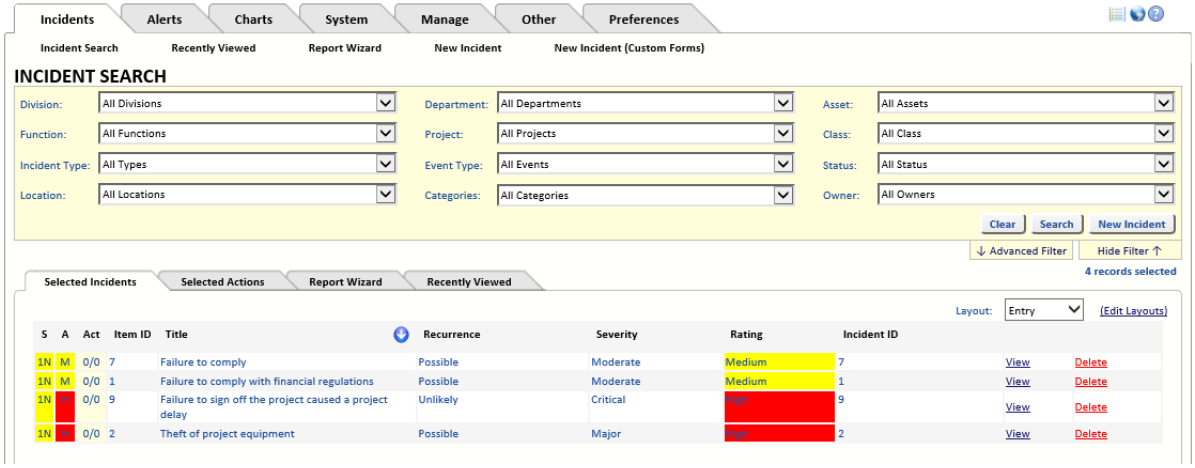
At the top right of the home page there are icons:

- – Opens the online help.
- – Opens the Language Translation page which enables you to translate or rename data items on the currently displayed form and report (this requires user permissions).
- – Opens the last viewed Incident.

3. Incidents

3.1. Incident Search

Incident Search is the main entry point to OpRiskControl Incident Manager.



The search form is automatically populated with your *Search Criteria* preferences (see "Search Criteria" on page 51). You can make changes to the search criteria then click the flashing red *Search* button. You will then be presented with the first page of the search results.

The normal search panel is used to find an Incident by up to twelve search criteria.

If required, configure your *Search Results* preferences (see "Search Results" on page 52) to restrict the number of columns in the search results.

When the search results have been displayed, you can sort a column by clicking on the column header. If you wish to sort the column in the reverse order, click on the column header again.

The number of Incidents per page can be set by selecting the *Preferences* tab, then selecting *Search Results* and *Editing* the *Number of Incidents per page*.

Clicking the *Clear* button performs a search with the *default* criteria. That is, it does not clear all search criteria fields but resets them to the configured defaults (see "Search Criteria" on page 51).

The returned Incidents have a *View* link and a *Delete* link.

Note: When you delete an Incident, all of its Actions are also deleted.

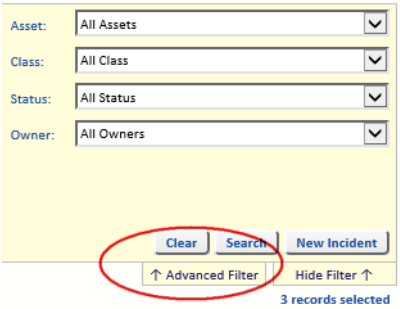
3.1.1. Advanced Incident Search

You can use the ↓ *Advanced Filter* link to show the advanced search area so you can search on a number of extra criteria including:

- *Incident containing text* – Search for a specific word in the Incident descriptions.
- *Action containing text* – Search for a specific word in the Action descriptions.
- *Dates* – Select either *Date Identified, Date Created, Date Reviewed* or *Date of Incident* from the drop-down list. Enter the range of dates for which you want to search. Select *All* to clear the filter for this field.
- *Item ID* – Enter the Incident ID for which you want to search in the text box.
- *Other Ref No.* – Enter the value for *Other Ref No* for which you want to search in the text box.

- *Rating* – Select the field on which you want to search from the drop-down list. Or select *All* to search all the listed fields. When a specific field is selected (for example, *Assessed Rating*), you can then select one of the following:
  - *Equal to* – Search for a specific value for the selected field.
  - *Greater than* – Search for all values greater than the entered value for the field.
  - *Greater than or equal to* – Search for all values greater than or equal to the entered value for the field.
  - *Less than* – Search for all values less than the entered value for the field.
  - *Less than or equal to* – Search for all values less than or equal to the entered value for the field.

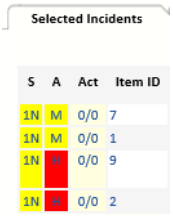
  Next, select the value for which you want to search from the drop-down list. The value in the drop-down list changes according to the field selected.
  - Click ↑ *Advanced Filter* to hide the advanced search area.



You can select from seven standard search results layouts (*Dates*, *Entry*, *Location*, *Other*, *Ownership*, *Review* and *Value*). You can edit those layouts as described in "Search Results" on page 52.

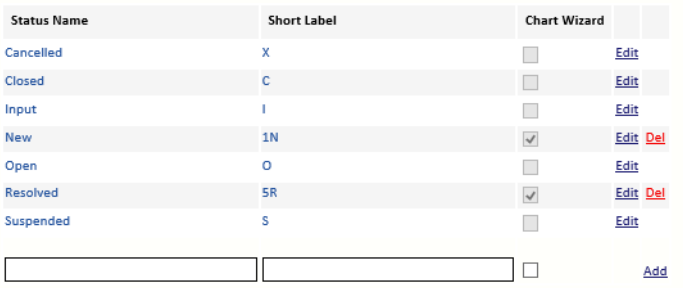
3.1.2. The SA Indicator Columns

The SA columns indicate the status of each Incident without having to *View* each individual Incident.



The short-form columns are used as follows:

- *S* – The Incident status:



Status Name	Short Label	Chart Wizard		
Cancelled	X	☐	Edit	
Closed	C	☐	Edit	
Input	I	☐	Edit	
New	1N	☑	Edit	Del
Open	O	☐	Edit	
Resolved	5R	☑	Edit	Del
Suspended	S	☐	Edit	
		☐	Add	

These can be edited by the System Administrator by selecting the *System* tab then by selecting *System Data* and then by selecting *Incident Status*. Status codes that are essential to the system cannot be deleted.

Other status codes can be added by your System Administrator and can be deleted (unless they have been used in the system). Incidents with non-system status codes are counted in the *Dashboard* under *Other/Active* but the system will not automatically process them in any way.

- *A* – The assessed rating. The Assessed Incident Rating is derived from the Severity and the Recurrence.
- *Act* – The *number of Completed Actions/number of Active Actions*. For example, *1/3* indicates there is one Completed Action and three Active Actions.
- *Item ID* – The unique ID (which was either entered by a user or generated by the system). See "Item ID" on page 10.

3.2. View

Click the *View* link beside an Incident in the Search Results to open the selected Incident for viewing. To edit the selected Incident, select the required tab and then click the *Edit* button. After making the required changes, click *Save* to save the changes or *Cancel* to discard your changes.

Note: If, when you try to edit an Incident, you see *user* is editing this record, the record is currently being edited by another user. You will be allowed to edit the record once the other user has saved their changes, cancelled their edit, or once the record locking period has expired.

3.3. Delete

Click the *Delete* link beside an Incident in the Search Results to delete the selected Incident. A dialog is displayed asking you to confirm you want to delete the Incident and any Action or History associated with it. Click *OK* to delete the Incident and associated Actions and History, or *Cancel* to cancel the deletion.

3.4. Recently Viewed

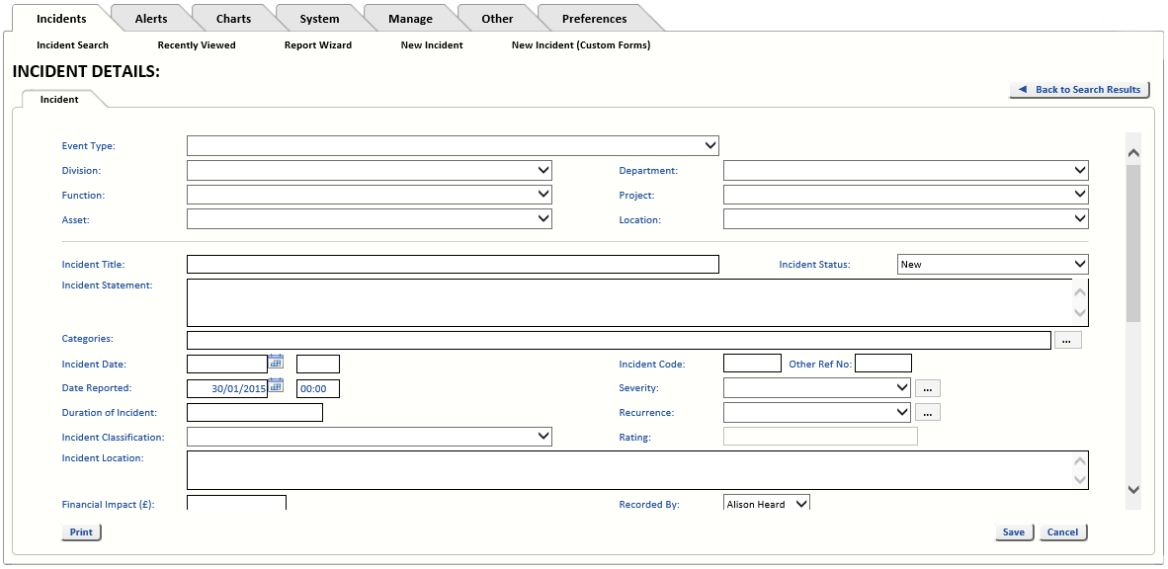
Select the *Recently Viewed* tab to view a list of the last 10 Incidents you have viewed. The first Incident on the page is the last Incident you viewed.

3.5. Report Wizard

See "Report Wizard" on page 33 for a detailed description on the Report Wizard.

3.6. New Incident

The following shows an example of the screen layout.



If the information on this form does not meet your requirements, discuss *Custom Forms* with your System Administrator. *Custom Forms* is an optional module that allows you to create and use different forms for different types of Incident. That means some types of Incidents can be entered in brief while other Incidents may require more detail.

3.6.1. Event Type

Required: Select the *Event Type* from the list. The *Event Type* identifies the Incident that has occurred.

3.6.2. Division

Optional: Select the Division that will own the Incident from the drop-down list. Do not select the Division where the recorder, contact or owner works, but the Division that has agreed to own and, if necessary, manage Actions.

Division is mandatory if RBS is switched on by Division. Please refer to the *OpRiskControl System Administrators' Guide* for more information about RBS.

3.6.3. Department

Optional: Select the Department that has agreed to own the Incident from the drop-down list.

Department is mandatory if RBS is switched on by Department. Please refer to the *OpRiskControl System Administrators' Guide* for more information about RBS.

3.6.4. Function

Optional: Select the Function that will own the Incident from the drop-down list.

Function is not visible unless *Show Additional Enterprise Structure* is selected.

Note For Administrators: On the *System* tab select *System Settings*, then select the *Workflow* tab. The *Show Additional Enterprise Structure* option is in the section with the title *Workflow forms*.

3.6.5. Project

Optional: Select the Project that will own the Incident from the drop-down list.

Project is not visible unless *Show Additional Enterprise Structure* is selected.

Note For Administrators: On the *System* tab select *System Settings*. Then select the *Workflow* tab. The *Show Additional Enterprise Structure* option is in the section with the title *Workflow forms*.

3.6.6. Asset

Required: Select the *Asset* from the list.

People use different terms for the item or area involved in the Incident, such as asset, object, or element. This is the thing that was affected by the Incident.

3.6.7. Location

Required: Select the Location from the drop-down list.

If an Incident is specific to an asset at a specific location, use a street address. If more general, use a city, council, region, state, country or global description.

3.6.8. Incident Title

Required: Enter the Incident *Title*, keeping it short but unique.

This is a short description (up to 100 characters) of the specific Incident, and is used in reports.

3.6.9. Incident Status

When a new Incident is created, its status is set automatically according to the setting for *Default Status for New Incident* which is set by the System Administrator. A new Incident will normally default to either *Open* or *Input*. When a new Incident is automatically set to *Input* it enables an Incident manager to validate the Incident before setting it to *Open* (which means it is active).

To close an Incident, change its status to *Closed* and enter the date closed.

When an Incident is created erroneously, change its status to *Cancelled*. The date closed is not changed in this case.

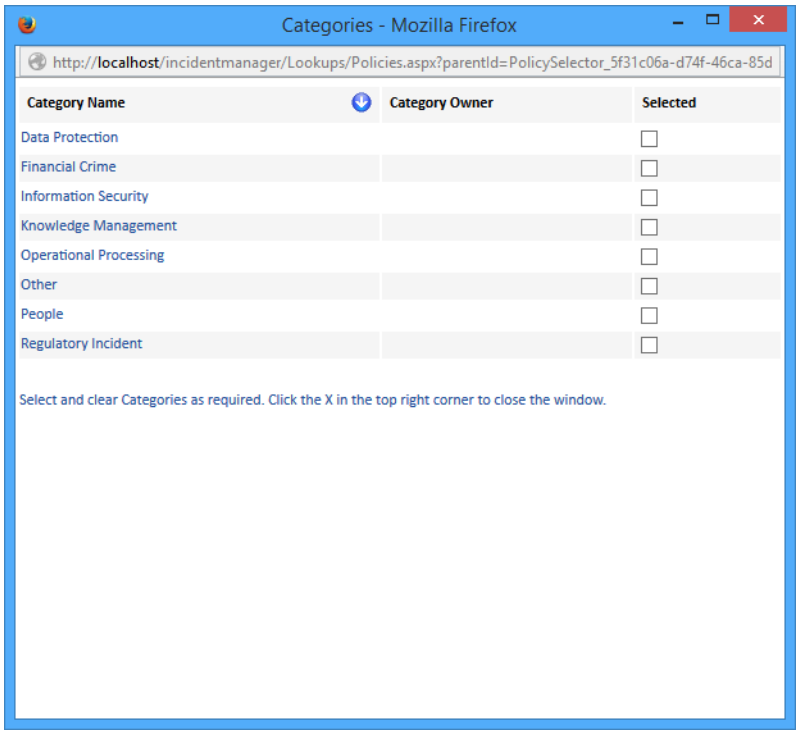
Should the Incident need to be suspended for any reason (for example, the condition cannot logically exist at a point in time but may do later), change the status to *Suspended* so that it is not actively monitored. The date closed is not entered in this case.

3.6.10. Incident Statement

Optional: Enter more details about the Incident.

3.6.11. Categories

Optional: Click on the ellipsis button to open the Category Selector. The list of configured Categories is opened.



Select the Categories you want to add to the Incident and then close the Category Selector window.

3.6.12. Other Ref No

This field can be used, for example, to record an Incident's old reference number when it is imported from a different system.

3.6.13. Incident Date

Required: Enter the date the Incident happened. If required, enter the time the incident happened in the format hh:mm. If no time is entered, 00:00 is used.

3.6.14. Item ID

Automatic: Your System Administrator might have configured the system to have the ID automatically populated (i.e. select the *System* tab then select the *General* tab and select the option *Autogenerate Codes*). If the *Incident ID* is automatically generated, the system uses the database unique ID for the Incident record but does not guarantee sequential allocation of unique ID.

Optional: If your System Administrator has not configured the system to have the ID automatically populated, you can enter an Incident ID in this data field. It is recommended that you enter a unique *Incident ID*. If you enter an Item ID manually, the system does not validate that the ID is unique.

3.6.15. Date Reported

Automatic: The system will enter the date the Incident was recorded. This date can be changed and, if required, a time can also be entered. The time must follow the format hh:mm. When no time is entered, *00:00* is used.

3.6.16. Severity

Required: Select the *Severity*. The descriptions are editable by your System Administrator.

Click ... next to *Severity* to see the definitions for Severity.

3.6.17. Duration Of Incident

Optional: Enter information about how long the Incident lasted.

3.6.18. Recurrence

Required: Select the *Recurrence*. The descriptions can be edited by your System Administrator.

Click ... next to *Recurrence* to see the definitions for Recurrence.

3.6.19. Review Frequency

Optional: The *Review Frequency* defaults to the setting for *Default Review Frequency* in your *Context Profile preferences* but it can be changed. Select the frequency of review, as required.

3.6.20. Rating

Automatic: The *Incident Rating* is the *level of seriousness* and is derived from *Recurrence* and *Severity*. The *Incident Rating* is often shown as *Rating* for short as a column header on search results and reports.

3.6.21. Date Reviewed

Automatic: The date the record was last reviewed (for example, when either the *Recurrence* or *Severity* estimates were changed). On a new record, the date will default to the current date. Optional: When reviewed, and if there is no change to either the *Recurrence* or *Severity*, the date the record was last reviewed can be changed by the user.

3.6.22. Date Next Review

Automatic: The system will add the number of days of the *Review Frequency* to the *Date Reviewed* to determine the date of the next review. The *Date Next Review* drives the automatic alerts via the Notification Manager and the posting of alerts to the *Alerts* page for Incident Reviews. If the review date is due, the message *Due* will appear in red under the *Date Next Review*. If the review date has passed, the message *Overdue* will appear in red under the *Date Next Review*.

3.6.23. Incident Classification

Optional: This field allows the customer to define another dimension of classifying Incidents. Incident Classifications are set up in *Reference Data* and used here.

3.6.24. Incident Location

Optional: Enter where the Incident took place.

3.6.25. Financial Impact

Optional: Enter the value of the financial impact. If used, this field must contain a monetary value, for example 10,000 or 49.99. The currency symbol (e.g. £) is not required.

3.6.26. Recorded By

Required: Select the name of the user who recorded the Incident.

3.6.27. Reported By

Optional: Enter the name of the person who reported the Incident.

3.6.28. Contact

Required: Select the name of the user who is the contact for the Incident.

3.6.29. Reported To

Required: Select who the Incident was reported to.

3.6.30. Owner

Required: Select the Incident owner (the user who has overall responsibility for the Incident) from the list.

3.6.31. Date Closed

Automatic: The date the Incident status was changed to *Closed*.

3.6.32. Closed By

Automatic: The name of the user who changed the Incident status to *Closed*.

3.6.33. Closure Comment

Optional: Enter a comment about how or why the incident was closed.

3.6.34. Description Of Events Prior To Incident

Optional: Enter a description of the events just prior to the Incident happening.

3.6.35. Description Of Event (The Incident)

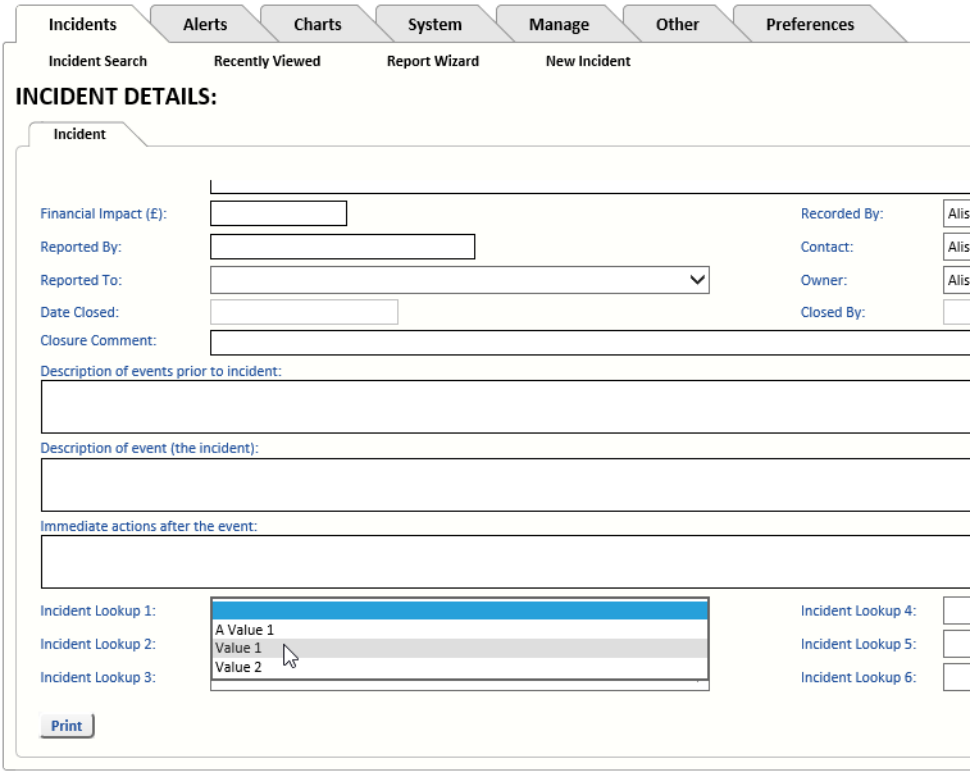
Optional: Enter a description of the Incident.

3.6.36. Immediate Actions After The Event

Optional: Enter a description of the events just after to the Incident happened.

3.6.37. Incident Lookup 1-6

When *Custom Incident Lookups* is selected in the *System Settings* you will see the *Incident Lookup* fields.



Optional: (These Incident Lookup fields might have been renamed.) Select a value from the drop-down list for each field, as required.

Note For Administrators: See *Manage Lookups* in the *OpRiskControl Incident Manager System Administrators' Guide* for more information on Incident Lookup fields.

3.7. Cause Tab

Optional: One or more causes can be added to an Incident.

3.7.1. Cause

Required: To add a Cause for the Incident, select a Cause from the drop-down list.

3.7.2. Cause Description

Required: Enter a description of the Cause of the Incident.

3.7.3. Data Recorded

Optional: By default, today's date is entered for the date the Cause was recorded. Select a date from the calendar or type a date in the text box.

3.7.4. Recorded By

Optional: By default, the name of the user who added the Cause is added as the person who recorded the cause. Select a name from the drop-down list.

3.7.5. Cause Document

Optional: To ink a document to the Cause, click the Browse button and browse to and select the document. The document is added as a link to the Cause. To remove a Cause Document, click the *[Clear]* link.

3.8. Actions Tab

This tab shows the list of Actions related to the Incident. Existing Actions can be edited or new Actions can be created from this page. Actions are described in "Incident Actions" on page 23.

3.9. History Tab

This tab shows the list history events related to the Incident. The History tab is described in "Incident History" on page 31.

3.10. Documents

A tab named *Documents* is provided on the Incident View form so that you can attach multiple documents to each Incident.

You can attach a document using the *Attach Document* button. You can also view a document that has already been attached to the Incident by clicking on the *View* text link. To edit a document's details, click the *Select* text link next to the appropriate document. The *Del* text link removes the document from this page.

The above image shows one document attached to an Incident.

3.10.1. Document Name

Optional: Enter the name (including file path) of any Incident document if the document relates to this specific Incident. You can Browse for the document to capture the path and name.

3.10.2. Created

Optional: Enter the date the document was created, or at least attached to the Incident. The date defaults to the current date.

3.10.3. Author

Optional: Select the author of the document if the author is on the user list, or leave blank.

3.10.4. Revised

Optional: Enter the revised date if the document was revised, or leave blank. If the document details are changed, the system uses the current date by default. However, this can be edited, or left blank.

3.10.5. Version

Optional: Enter the document version number, or leave blank. This is a free format text field and is not validated in any way.

3.10.6. Attached By

Optional: Select the user who revised the document if the user is on the user list, or leave blank.

3.10.7. Security Class

Optional: Enter the document security code, or leave blank. This is a free format text field and is not validated in any way.

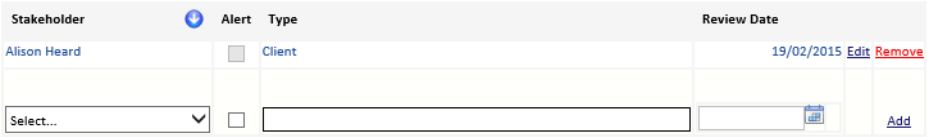
3.10.8. Status

Optional: Enter the document status code, or leave blank. This is a free format text field and is not validated in any way.

3.11. Stakeholders

3.11.1. Stakeholder

Apart from Incident contact, Incident owner and Action owner, additional people might be interested in a particular Incident.



Stakeholders can be selected from the list of users and contacts. If a stakeholder needs to be alerted if anything changes in relation to the Incident, then select *Alert*.

Both *Type* and *Review Date* are optional. A typical Type will be *Reviewer* in free text. If a *Review Date* is set, it will be picked up in the Notification Manager under *Updates and Reminders, Incident Reminders*.

3.11.2. Alerts

Stakeholder alerts requires the Notification Manager. There are two types of alerts:

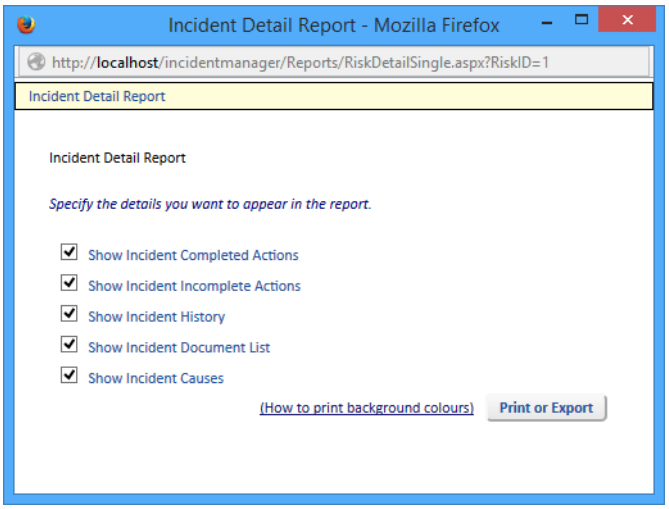
1. A user has been added to the list of stakeholders.
2. The Incident has been updated in some way.

3.12. Incident Form Buttons

When viewing an Incident, the *Incident Form* buttons are available at the bottom of the screen.

3.12.1. Print Button

Click the *Print* button to create an Incident Detail report which contains the selected Incident detail on one form.

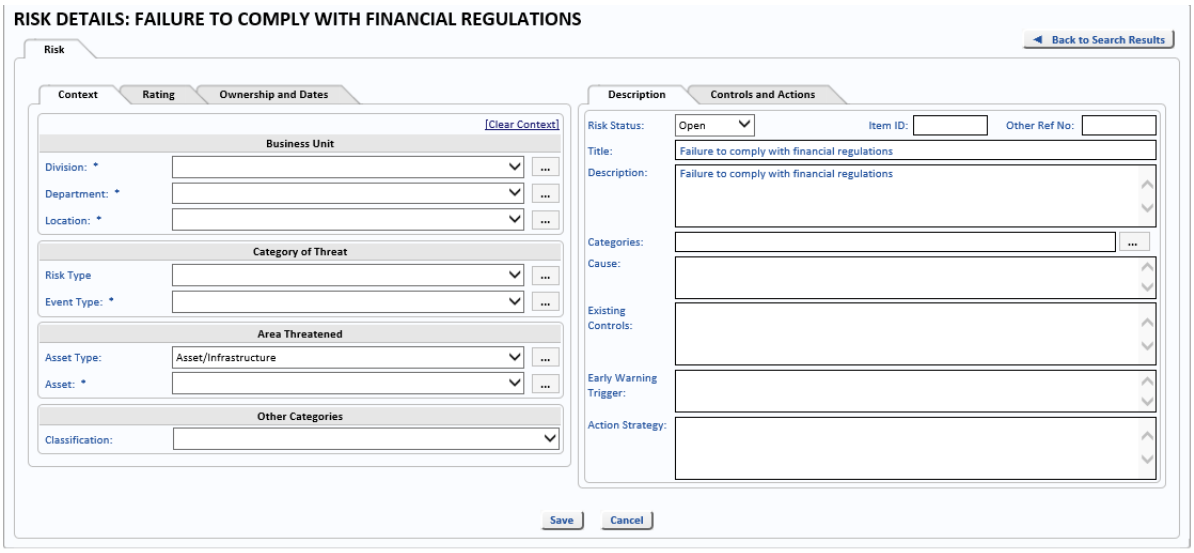


Select the details you want to appear in the Incident Detail report and click *Print or Export*.

The Incident Detail report is displayed in a new browser window. From here you can print the report, if required.

3.12.2. New Risk Button

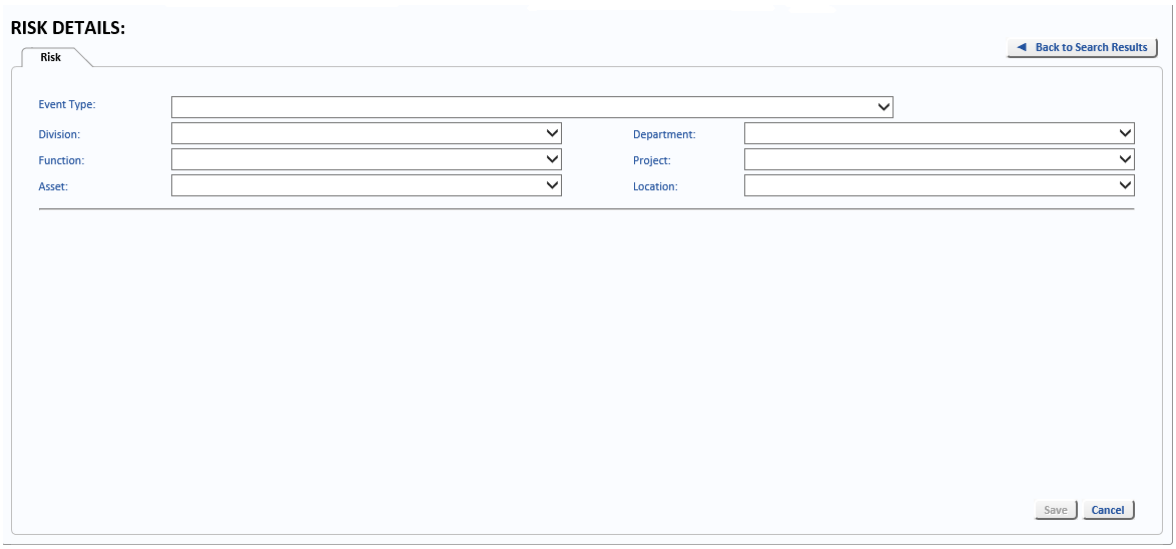
The *New Risk* button enables you to link the current Incident to a newly created tabbed Risk. Click the *New Risk* button to open OpRiskControl Incident Manager with a new Risk. The Incident title is used as the new default title of the new Risk. This can be changed.



Enter the values for the Risk. Please refer to the *OpRiskControl Users' Guide* for more information about creating Risks.

3.12.3. New Custom Risk Button

The *New Custom Risk* button enables you to link the current Incident to a newly created custom Risk. Click the *New Custom Risk* button to open OpRiskControl Incident Manager with a new Risk using a Custom form.

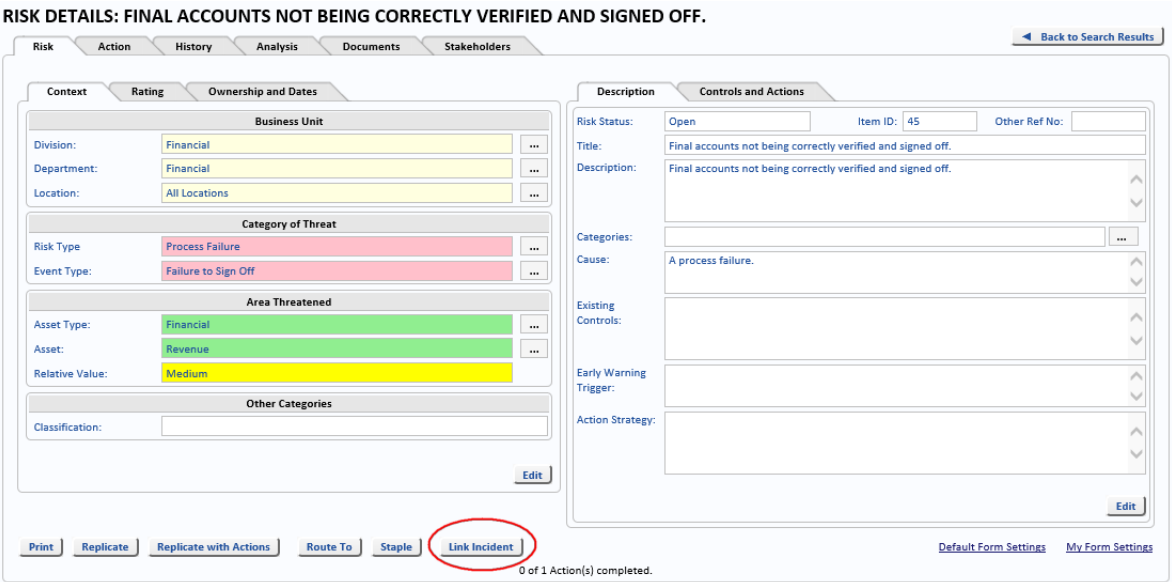


Select the *Event Type* to display the remaining Risk fields. Enter the values for the Risk. Please refer to the *OpRiskControl Users' Guide* for more information about creating Risks.

3.12.4. Link To Risk Button

The *Link to Risk* button enables you to link the current Incident to a Risk which already exists in OpRiskControl. Click the *Link to Risk* button to open OpRiskControl Incident Manager on the search results page. Select the Risk you want to link the Incident to and click the *View* link text to open the Risk.

Click the *Link Incident* button to link the selected Risk to the Incident.



The *Link Incidents* button is replaced with the *Incidents* button. Click the *Incidents* button to show the Incidents which are linked to the selected Risk.

3.12.4.1. Incident

The title of the Incident linked to the Risk.

3.12.4.2. Date

The date the Incident occurred.

3.12.4.3. Event Type

The Event Type assigned to the Incident.

3.12.4.4. Reported

The date the Incident was reported.

3.12.4.5. View

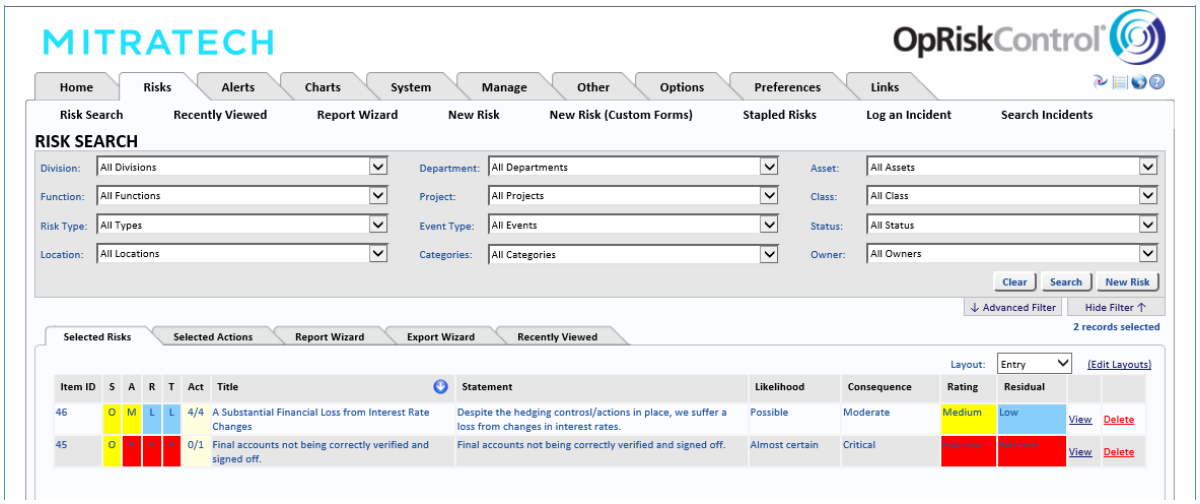
Click the *View* text to view the Incident.

3.12.4.6. Unlink

Click the Unlink text to unlink the Incident from the Risk. A confirmation dialog is displayed asking you to confirm you want to unlink the Incident from the Risk. Click *OK* to unlink or *Cancel* to close the dialog without unlinking the Incident from the Risk.

3.12.5. Links Button

The *Links* button enables you to view all the Risks which are currently linked to the selected Incident. Click the *Links* button to open OpRiskControl's *Risk Search* page. Only the Risks which are linked to the selected Incident are displayed.



3.12.6. Replicate Button

You can create a new Incident by copying an existing Incident. You will then need to change *Title* before you can save the Incident. The new Incident will have the same settings as the original with the exception of the following:

- The name of the User who copied the Incident appears in the *Recorded By* field.
- The *Item ID* is automatically created when *Autogenerate Codes* is selected on the *System* tab and the copied Incident is *Saved*.

Note For Administrators: Select the *System* tab, then select *System Settings* and select the *General* tab. The *Autogenerate Codes option* is on this page.

- *Actions* are not copied and therefore there will be no Actions associated with the copied Incident.
- *Links* are not copied and therefore there will be no Risks associated with the copied Incident.

Edit the copied Incident as required and *Save* the Incident.

When *Show Additional Enterprise Structure* is selected, you can copy (*Replicate*) an Incident to another Function or Initiative.

Note For Administrators: On the *System* tab select *System Settings*. Then select the *Workflow* tab. The *Show Additional Enterprise Structure* option is in the section with the title *Workflow forms*.

3.12.7. Route To

Work is routed to specific people (or User Groups) via the *Route To* button on the main Incident form.

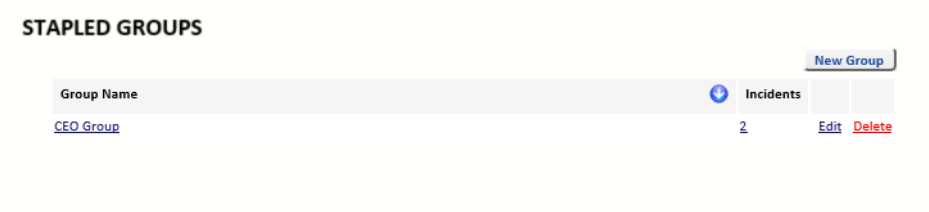
This buttons allows work (on Incident, Action or control) to be routed to another user regardless of whether they are currently associated with the work. It also allows different parcels of work to be routed to different people (e.g. for approval of two different treatments), or the same parcel of work to be routed to multiple people (e.g. for optional review and comment).

3.12.8. Staple Button

Incidents are created by division, department, location, and so on, or by Incident rating level. However, sometimes you might want to manage a group of Incidents regardless of their home business unit or their Incident ratings.

If, for example, the members of the Board of Directors have nominated a number of things they want attended to before the next board meeting, you are able to create *Stapled* Groups. You then staple any relevant Incident to that Stapled Group and manage them as a group regardless of their home business unit.

Before Incidents can be stapled, *Activate Incident Stapling* must be selected in *System Settings*. Also, a Stapled Group needs to be created by selecting the *Incidents* tab, then select *Stapled Incidents* and click the *New Group* button.



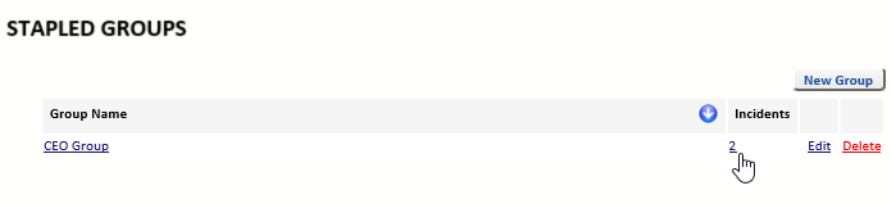
After a Stapled Group is created, an Incident can be associated with it via the *Staple* button at the bottom of the Incident form in View mode.

The list of Incidents which have been Stapled together can be viewed by clicking the number in the *Incidents* column for the appropriate Stapled Group.

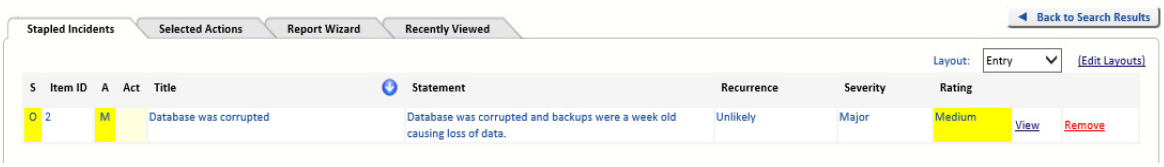
Note For Administrators: On the *Incidents* tab, select *Stapled Incidents* to edit and create Stapled Groups.

If an Incident has already been Stapled, the button at the bottom of the view form will change from *Staple* to *Stapled*.

To remove an Incident from a Staple Group, select Stapled Incidents from the Incidents tab, click on the number of Incidents in the Stapled Group.



The Incidents which have been Stapled to that group are listed. Click *Remove* to remove the Incident from the Stapled Group.



In the *Incident Search Results* and *Reports* (Incident List, Actions Status, Executive Incident Summary) if the *Stapled* column is included in the Report it is displayed as *SG* (for *Stapled Group*). Stapled Incidents have a tick in the *SG* column.

3.12.9. Standard Button

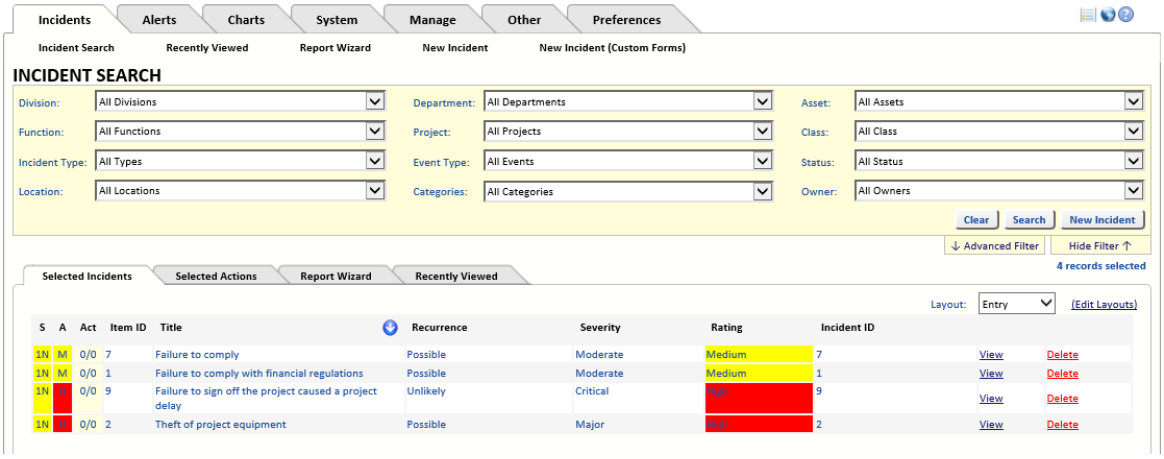
The *Standard* button is displayed in Incident View mode if the current linked Incident Event has an associated standard. Standards are configured in the Reference Data, and optionally associated with Incident Events in the Reference Data.

Note For Administrators: Please refer to the *OpRiskControl System Administrators' Guide* for more information about configuring a Standard for an Incident Event.

4. Search Incidents

4.1. Search Criteria

The list of Incidents can be searched.



The Incident Search can be filtered by the following fields:

- Event Type
- Division
- Department
- Asset
- Location
- Dates

4.2. Search Results

The search results are displayed with the following default columns. To change the way the search results are displayed, click *Edit Layout*. Move any columns you want hidden to the list on the left. Move any columns you want displayed to the list on the right.

The default *Entry* Layout columns are described below.

S – the Status – either *O* (Open), *I* (Input), *1N* (New), *5R* (Resolved), *S* (Suspended), *X* (Cancelled) or *C* (Closed).

Item ID – The unique Incident identifier.

Act – the number of complete Actions/the total number of Actions.

Title – The title of the Incident.

Statement – The statement provided for the Incident.

Recurrence – The value set for the Recurrence of the Incident.

Severity – The value set for the severity of the Incident.

Rating – The Rating calculated using the values for Recurrence and Severity.

Reviewed – The date the Incident was last reviewed.

View – Click to view the selected Incident

Delete – Click to delete the selected Incident.

5. Incident Actions

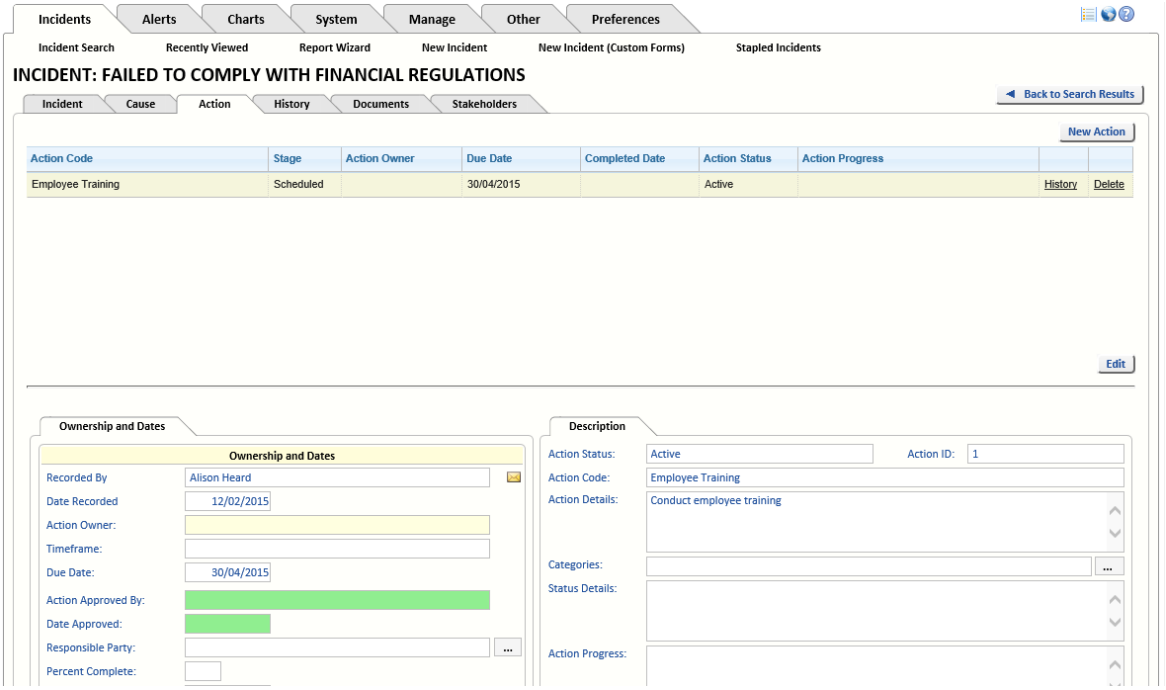
5.1. Introduction

OpRiskControl Incident Manager users are able to record Actions to mitigate an Incident.

You can add as many Actions to an Incident as required. Only the Action name and description are mandatory.

5.2. Action Search

When an Incident is displayed and you click the *Action* tab, you will see a list of Actions that have been attached to the Incident. If you wish to add an Action, click the *New Action* button.



The Action grid includes the following columns:

- *Action Code* – The Action Code used to create the Action.
- Stage – The *Stage* is determined automatically, based on the status of the Incident and of the Action:
  - When the Incident has not been accepted and the Incident status is *Input*, the Action is *In Progress*.
  - When the Incident status is *Open* and the Action has a *Completed Date* or the Action is an *existing control*, the Action is *Completed*.
  - When the Incident status is *Open* and the Action has neither a *Due Date* nor a *Completed Date*, the Action is *In Progress*.
  - When the Incident status is *Open* and the Action has a *Due Date* but does not have a *Completed Date*, the Action is *Scheduled*.
  - When the Incident status is *New*, *Closed*, *Cancelled* or *Suspended*, the Action is *Non Active*.
- *Action Owner* – The user who was assigned as the Action Owner.
- *Due Date* – The date selected for the Due Date.
- *Completed Date* – The date the Action was completed.
- *Action Status* – The current status of the Action (for example: *Active*, *Cancelled*, *Closed*, *Completed* or *Suspended*).

- *Action Progress* – Displays the current entry in the Action Progress field for this Action. The *Action Progress* field can be used to record how effective the control has been at mitigating the Incident.

The following links are available for each Action:

- *History* – Displays the Action History for the selected Action.
- *Delete* – Deletes the selected Action.

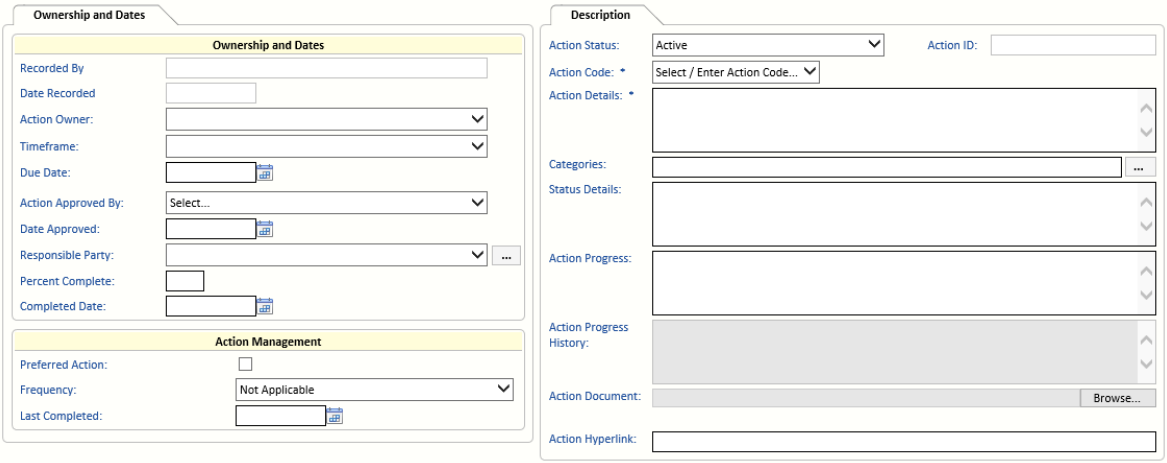
There is an *Edit* button below the Action grid. Click the *Edit* button and then click on any field in the Action grid you want to edit. Either a text box or a drop-down list is displayed, allowing you to change the selected field.

Note: When *editing* the Action Grid, the columns may be different from those displayed when *viewing* the Action grid. All the changes made to the Action grid in *Edit* mode are saved as you make them.

5.3. New Action

While viewing an existing Incident, select the *Action* tab and click the *New Action* button.

This section describes the items on the standard Action Form. If you are using a Custom Form, the fields displayed will differ.



5.4. Ownership And Dates

5.4.1. Recorded By

Automatic: The user who records the Action is entered automatically.

5.4.2. Date Recorded

Automatic: The system will enter the date the Action was recorded and it cannot be altered.

5.4.3. Action Owner

Optional: Select the Action owner (user who has overall responsibility for the Action) from the list.

It is highly desirable to allocate an Action owner as soon as possible. It is optional here only to allow time for the Action to be approved, and until approved the ultimate Action owner is not responsible for progressing the Action. An Action owner can be external to your company.

5.4.4. Timeframe

Optional: Select the time frame. Action time frames can be project phases, and they can be included in the *Action Status Report* and *Work Schedule Report*. The *Work Schedule Report* can also be sorted by *Timeframe*.

5.4.5. Due Date

Optional: Enter the date by which the Action should be completed. Although this field is optional, any Actions with a *Due Date* will be omitted from Action *Due Date* reports, and will not have automatically created Alerts.

5.4.6. Action Approved By

Optional: This field has been provided for enhanced workflow management, and is under RBS control so that only those with approval permissions can approve an Action.

Please refer to the *OpRiskControl System Administrators' Guide* for more information about RBS.

5.4.7. Date Approved

Optional: This field has been provided for enhanced workflow management, and is under RBS control so that only those with approval permissions can enter the date. If the details of the user who approved the Action are removed, the date is cleared from the record.

Please refer to the *OpRiskControl System Administrators' Guide* for more information about RBS.

5.4.8. Responsible Party

Optional: Select the party responsible for this Action (for example, a government agency, another party, or a contractor).

5.4.9. Percent Complete

Optional: Enter the percentage of the Action that has been completed.

5.4.10. Completed Date

Optional: Enter the date on which the Action was completed. Although this field is optional, any Actions without a *Completed Date* will be included on any Action *Due Date* reports, and will automatically create Alerts if the due date has passed.

5.5. Action Management

5.5.1. Preferred Action

Optional: This field is for documentation purposes only. It is not involved in any automated calculation.

5.5.2. Frequency

Optional: Select the frequency if the Action is to be a recurring action – for example, an annual inspection. It is the number of days the process *Activate Recurring Actions* uses to put recurring controls back on the 'to do' list, to make them Due again. The system will then put the recurring control back on the to-do list a number of days (as specified in system settings with the option *Recurring Action Reset (Day)*) before they are due to be completed again.

Incident Manager normally stores Actions that occur once. However, the system supports recurring Actions. The system must be able to reset the *Due Date*, clear out the *Completed Date*, and not lose track of what has been done before. The reset must not compromise Actions due and overdue Alerts, but it will distort Dashboard Action counts in that recurring Actions will be subtracted from *Completed* and added to *Approved*. Users need to be aware that recurring Actions get put back in the queue and counted as such.

The Job Scheduler updates Recurring Actions daily.

5.5.3. Last Completed

Automatic: This field is automatically populated with the date of the last *Completed Date* so that when recurring Actions are put back on the list of jobs to be done (according to the *Frequency* and when the *Completed Date* is cleaned out), there is a *Last Completed* date for tracking purposes. Completed Actions are also logged to the History page. Note that recurring Actions are put back on the list to be completed when *Activate Recurring Actions* is run.

5.6. Description

5.6.1. Action Status

Mandatory: The status will default to *Open* but can be set to *Closed*, *Cancelled*, *Completed* or *Suspended*.

A *Suspended* Action is one that is not currently active. For example, when your CCTV system has failed and needs to be fixed, or your insurance company has declined to renew your insurance and you are uninsured for fire and burglary, the Action Status could be set to *Suspended*.

A *Closed* Action is one that may have worked in the past but is not considered effective or at least not cost-effective. If you want to keep the Action for later reference, *Close* the Action. If the Action is not required for future reference, *Delete* it.

A *Cancelled* Action is one you were thinking of using but changed your mind (perhaps due to cost or complexity). If you want to keep the Action for later reference, *cancel* the Action. If the Action is not required for future reference, *Delete* it.

Control over what is shown on the screen and in reports is managed from the Action List preferences.

Action Status is a user selectable item while *Stage* is determined automatically. *Status* and *Stage* are selectable items (select the *Preferences* tab and then select *Action List*).

5.6.2. Action ID

The *Action ID* is automatically generated. The system uses the database unique ID for the Action record but does not guarantee sequential allocation of unique IDs.

5.6.3. Action Code

Required: Select an Action Code from the drop-down list. If a suitable code does not exist, select *Other* from the list and create your own.

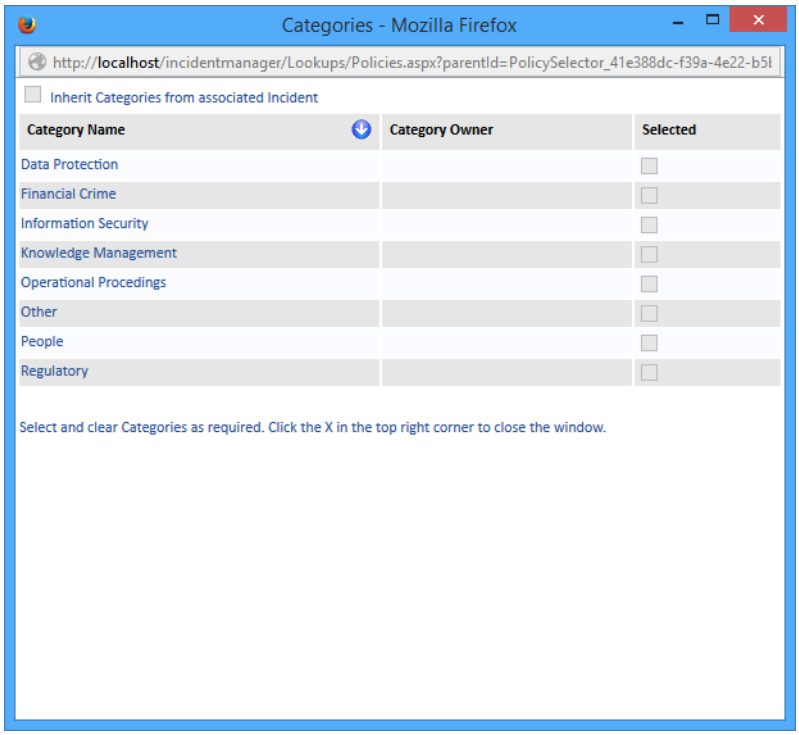
Note: When *editing* the *Action Code* field, you will be editing the *Action Code* for the selected Action only (by typing it in the *Action Code* field). This edited *Action Code* will not be available when creating new Actions.

5.6.4. Action Details

Required: The Action detail is defaulted from the available Action types, but you can alter or overtype this specific instance of the Action without affecting the available Action types.

5.6.5. Categories

Optional: Click on the ellipsis button to open the Category Selector. The list of configured Categories is opened.



To make the Action inherit the Categories of the parent Incident, select the option *Inherit Categories from associated Incident* and then close the Category Selector window.

To set Categories for the Action, clear the option *Inherit Categories from associated Incident,* select the Categories you want to add to the Action and then close the Category Selector window.

Note: By default, when an Action is created for an Incident which already has Categories configured, the Action inherits the parent Incident's Categories.

5.6.6. Status Details

Optional: The status detail is entered. This relates to the current situation relating to progress in implementing the Action. This field can be selected and included on reports.

5.6.7. Action Progress

Optional: The *Action Progress* field can be used to record how effective the control has been at mitigating the Incident. Each new entry overwrites the previous entry. Each entry is written to the *Action Progress History* field (see below).

5.6.8. Action Progress History

Read Only: The *Action Progress History* field is automatically updated when the *Action Progress* field is changed. The new entry for *Action Progress* is added to the *Action Progress History* field with a date stamp.

5.6.9. Action Document

Optional: Enter the name (including file path) of any Action document if the document relates to this specific Action. You can *Browse* for the document to capture the path and name, and *Open* the document using the buttons provided. If the Action Code was set up with an Action document, this field will inherit that document name.

5.6.10. Action Hyperlink

Optional: Enter the hyperlink (web link) of any information if the information relates to this specific Action. If the Action code was set up with an Action hyperlink, this field will inherit that URL.

5.7. Lookup

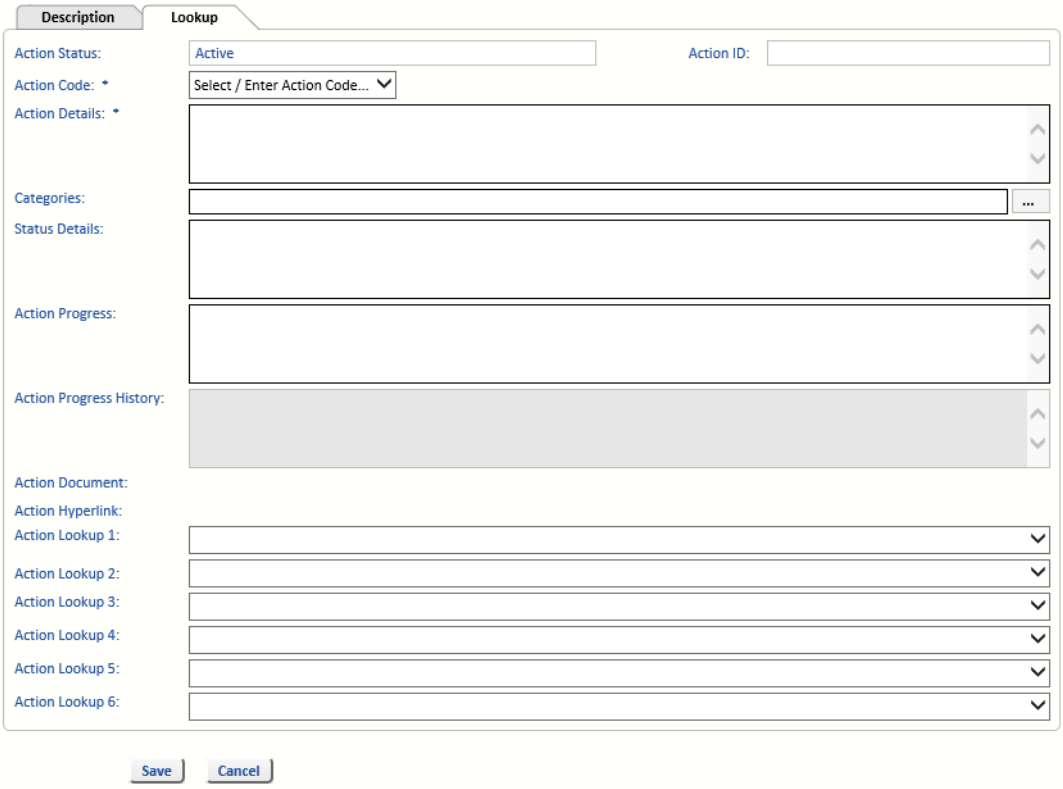
When *Custom Action Lookups* is selected in the *System Settings* you will see the *Lookup* tab. The following fields on the *Lookup* tab are the same as the fields on the *Description* tab.

- Action Status
- Action ID
- Action Code
- Action Details
- categories
- Status Details
- Action Progress
- Action Progress History
- Action Document
- Action Hyperlink

Please see "Description" on page 26 for descriptions of these fields.

5.7.1. Action Lookup 1-6

The *Action Lookup* fields are displayed below the *Description* tab fields.



Optional: (These Action Lookup fields might have been renamed.) Select a value from the drop-down list for each field, as required.

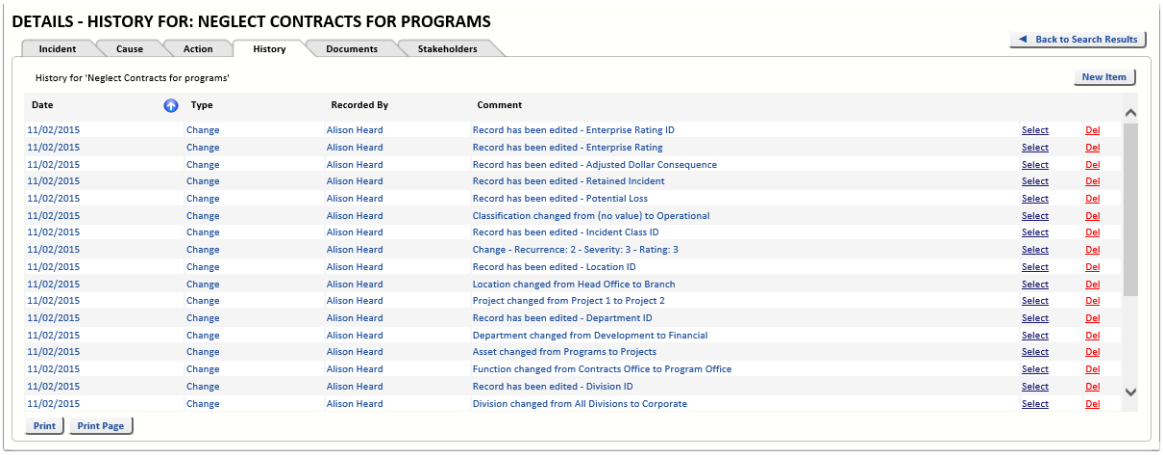
Note For Administrators: See *Manage Lookups* in the *OpRiskControl Incident Manager System Administrators' Guide* for more information on Action Lookup fields.

6. Incident History

6.1. History At The Incident Level

Users of Incident Manager are able to record notes about an Incident using the Incident History form. In addition, many records are written automatically to the Incident history file as specified on the *System Settings* page. Apart from the history file, all changes are written to an Audit file in case forensic analysis is required.

Whenever an Incident is reviewed, a record is written to the history file showing the new Recurrence, Severity and Incident rating. This will happen if either the Recurrence or Severity or Incident review date is changed. The automatic record will use the current date, a history type of *Change*, and the current Incident recorder's name.



To add a new history item click *New Item* and complete the fields.

To edit an existing history event, click *Select* next to the history item and edit the fields.

6.1.1. Date

Required: Enter the date the comment was entered. It should default to the current date, but can be altered and back-dated (subject to organisational standards).

6.1.2. History Type

Required: Select the history type from the list. There are example history types already created, but if you need different history types, ask your System Administrator to set them up for you.

6.1.3. Follow Up

Optional: If there is to be a follow-up, enter the date due. This field is interrogated by the Alert Reminders program.

6.1.4. Recorded By

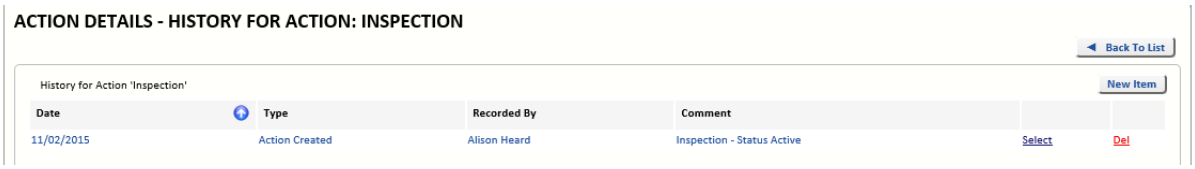
Required: Select the comment recorder (user who records the comment) from the *User* list.

6.1.5. Comment

Required: Enter any appropriate comment. There is space for 255 characters.

6.2. History At The Action Level

History about Actions, can be logged with the Action that it relates to, and/or with the Incident it relates to. Select an Action from the Action grid and click the *History* link.



The amount of Action History which is logged (and where it is logged – on the Incident *History* tab, or by clicking the *History* link as described above, or both places) is determined by the settings on the *History* tab.

Note For Administrators: Select the *System* tab, then select *System Settings* and select *History*.

7. Report Wizard

7.1. Introduction

Many Incident reports are provided. However, users can access the data via other report writers such as Crystal Reports. It is imperative that the user does not employ any tool that is able to update data in the database as this might compromise the database integrity. All report tools must use *read-only* access.

You can display reports on the screen (rather than send them to a printer) and, where possible, *drill-down*. When you have displayed a report in the Report Wizard, and want to see more details of any Incident or Action listed in the report, you can click on the row to open up the form that manages the Incident or Action.

There are a number of ways to print reports. You can specify, select, view and print the list of Incidents using the Report Wizard or from various points in the system. The Report Wizard contains reports based upon the Incidents selected using the search screen.

7.2. Incident Search And Display

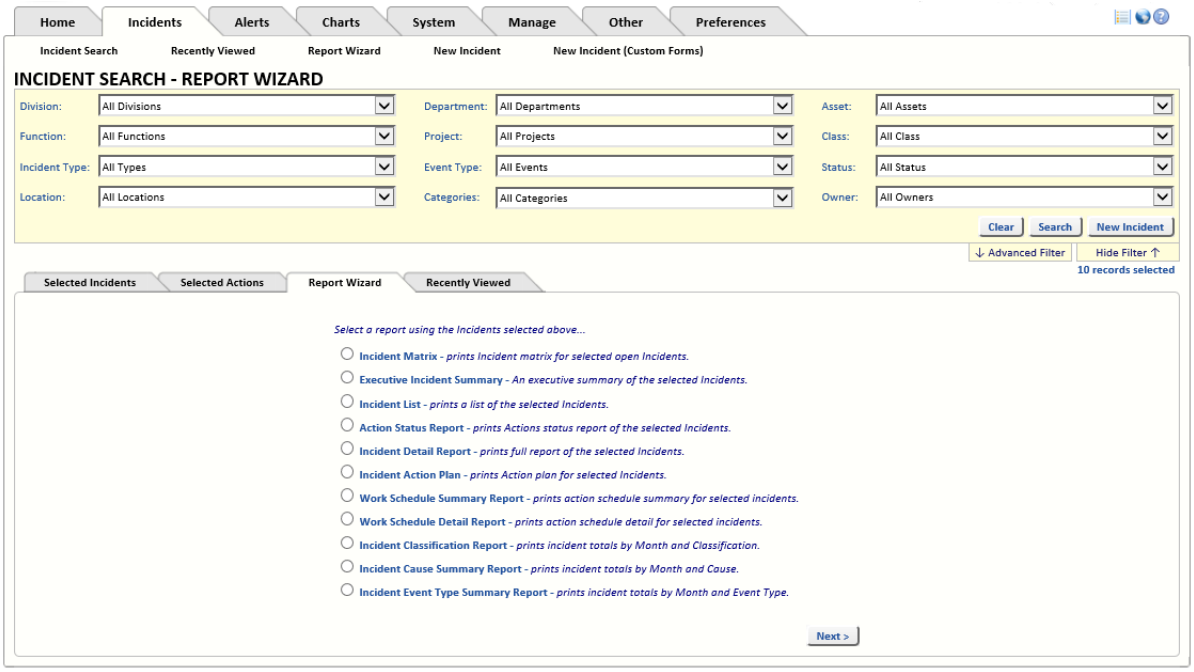
Determine the data you want displayed on the screen via the search filter. Then decide which columns you want displayed on the screen via the search layouts. Finally, you can set the order you want the data displayed on the screen by clicking on the column headings.

After displaying the records, you can:

- Print as displayed (you may need to select landscape mode to fit all columns on the page).
- Print to a PDF driver (pseudo printer) so you can distribute the report to others in PDF format.
- Use the Report Wizard to get pre-formatted reports (recommended).

7.3. Report Wizard

After filtering your data, select Report Wizard and then select the report format.



7.4. Report Wizard Overview

Most reports start with a page where you select the columns you want included and the order of the columns in the report.

The next page (if any) will normally allow you to enter a sort order. In some reports, you can also select how you want to group the report, but be careful that the grouping of a report will take more time to process and requires ample server memory. If the report is not displayed in about a minute, check with your IT support to make sure the server has at least 4 GB of memory.

Some reports that drill down to the Action level will also give you a third page where you can select the columns related to the Actions. Sorting and grouping is not available at this level.

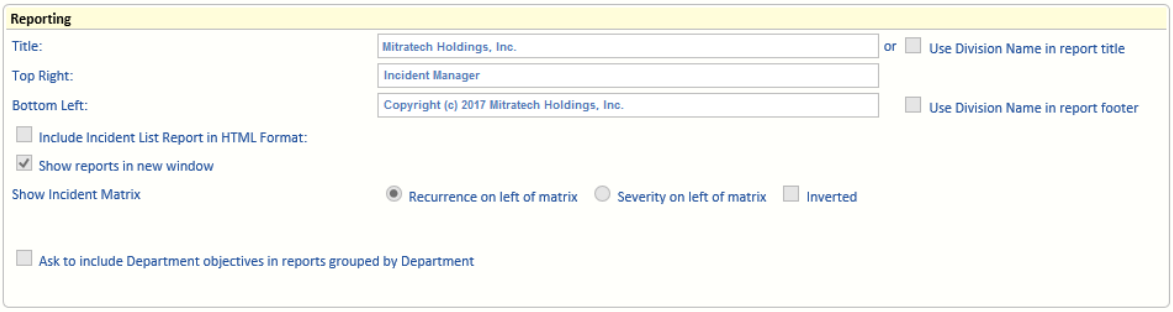
When you get to the last page (just before printing) a System Administrator should see the following options on two reports (Executive Incident Summary Report and Action Status Report). The *Group by Incident* button allows duplicate Incidents to be hidden in the reports.

If you have administrator privileges, you will see the *Set Report Defaults* button. This button makes the currently selected options the default options for the selected report.

The *Back* button takes you back one page.

The *Report List* button takes you back to the Report Wizard page.

If you have an active pop-up blocker on your browser and do not want to change it, ask your System Administrator to clear the option *Show reports in new window* in System Settings. Then all reports will be displayed in the same window rather than being displayed in a new window.

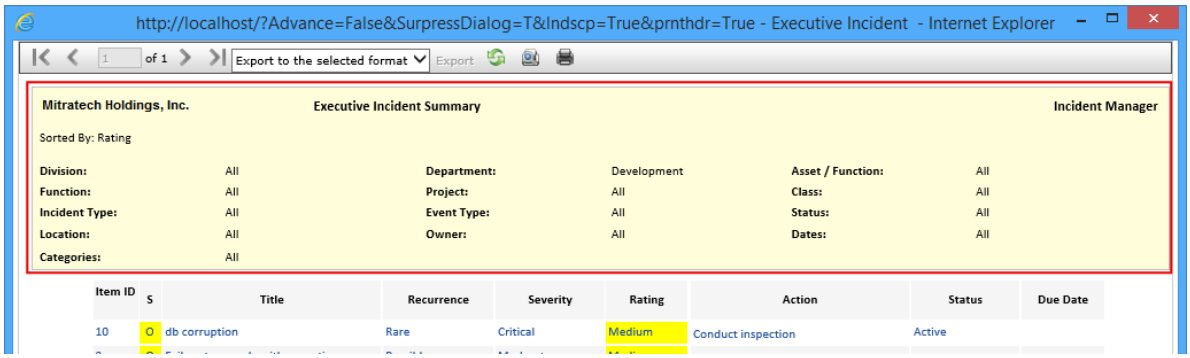


If you are grouping reports by Department and you want to append Department objectives to the Department name, ask the System Administrator to select the *Ask to include Department objectives in reports grouped by Department* option. You will then be given the option to select the option *Append objectives to group name* when grouping by Department.

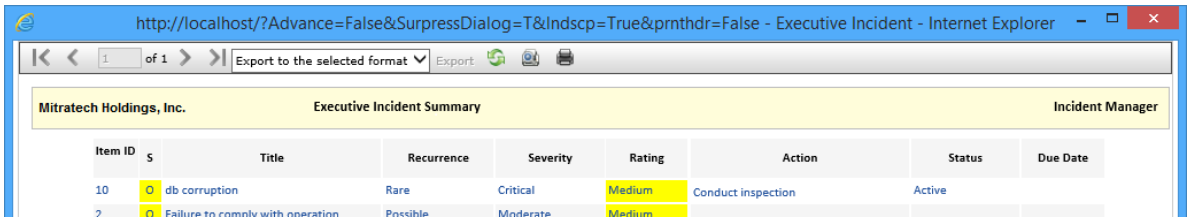
When *Print in landscape* is selected, the printer will default to landscape mode. This option is not available on all Reports.

The *Save Report Template* button is displayed only if you have permissions to save the report for others to select and use. Only the *Incident List Report* has this option. See "Template Reporting" on page 43.

When *Print criteria in header* is selected, the report includes your selection criteria in the header of the report.



When this option is cleared, the criteria are not shown.



This is useful later when you are trying to remember how you filtered the report.

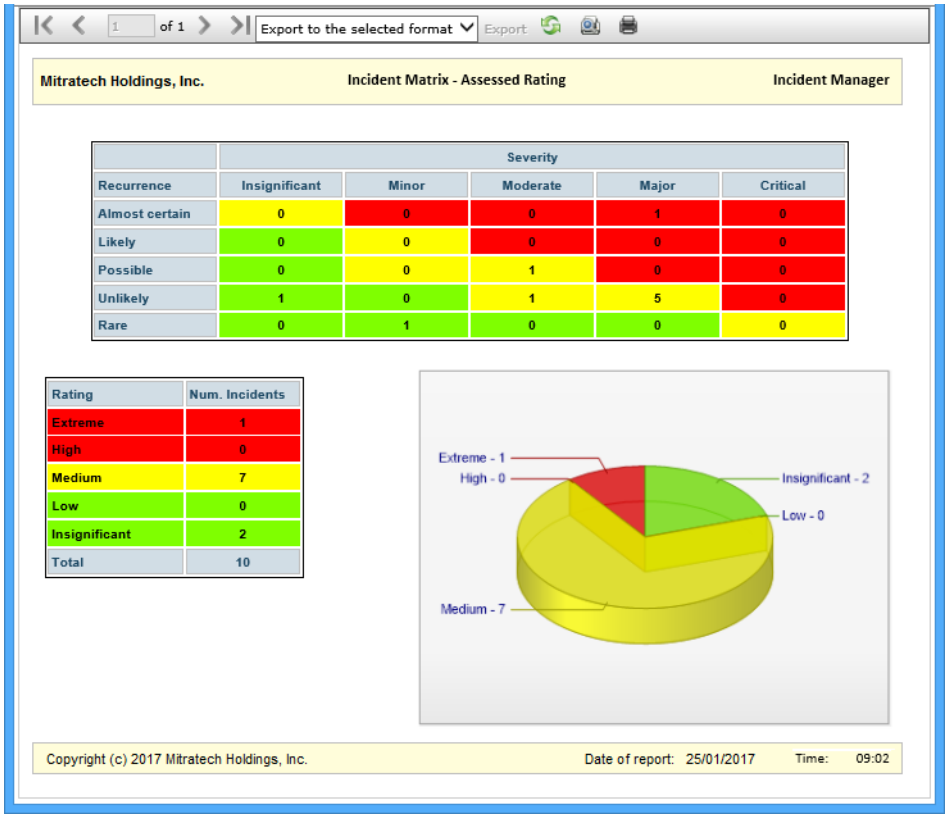
7.5. Incident Matrix

The Incident Matrix is displayed for the selected records (not necessarily for all records). It will exclude Incidents that do not have a status of *Open*.

If your system is configured to show Severity on the left of the Incident Matrix, then you will see a tick-box that you can enable to print the Severity values with the Incident Matrix.

Be mindful that if you configure to show Severity on the left of the Incident Matrix, the matrix will arrange (and look) differently to having Recurrence on the left of the matrix.

When you click the *Print or Export* button, you see the Incident Matrix.



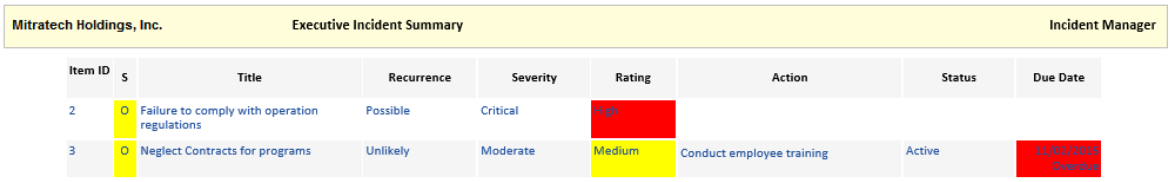
	Severity				
Recurrence	Insignificant	Minor	Moderate	Major	Critical
Almost certain	0	0	0	1	0
Likely	0	0	0	0	0
Possible	0	0	1	0	0
Unlikely	1	0	1	5	0
Rare	0	1	0	0	0

Rating	Num. Incidents
Extreme	1
High	0
Medium	7
Low	0
Insignificant	2
Total	10

The Incident matrix is displayed with Recurrence levels down the left and Severity levels across the top giving the Incident counts at the intersections. There is also a small table at the bottom on the left giving the counts for each rating level, and a pie chart that gives the break-up visually.

7.6. Executive Incident Summary Report

The *Executive Incident Summary Report* gives a quick snapshot of what requires attention. Anything in red needs immediate attention or is overdue.

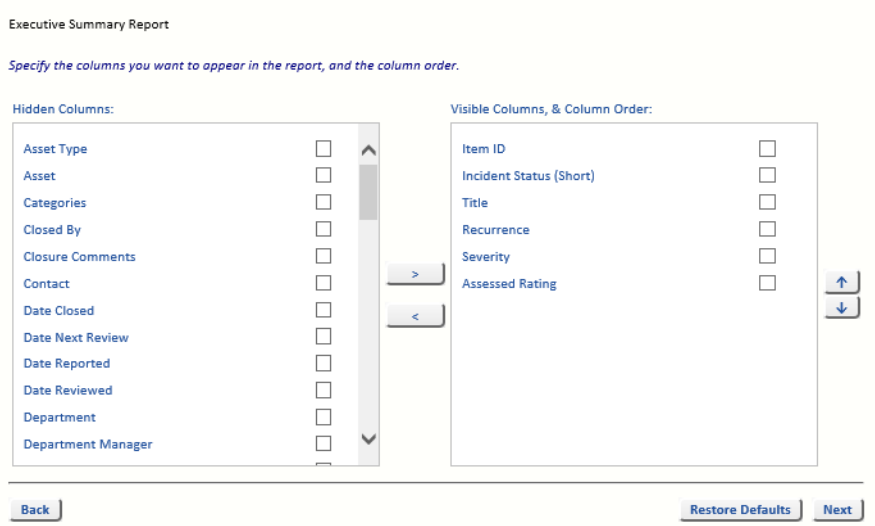


Item ID	S	Title	Recurrence	Severity	Rating	Action	Status	Due Date
2	O	Failure to comply with operation regulations	Possible	Critical	High			
3	O	Neglect Contracts for programs	Unlikely	Moderate	Medium	Conduct employee training	Active	31/07/2013 Overdue

This is the report most popular with senior executives.

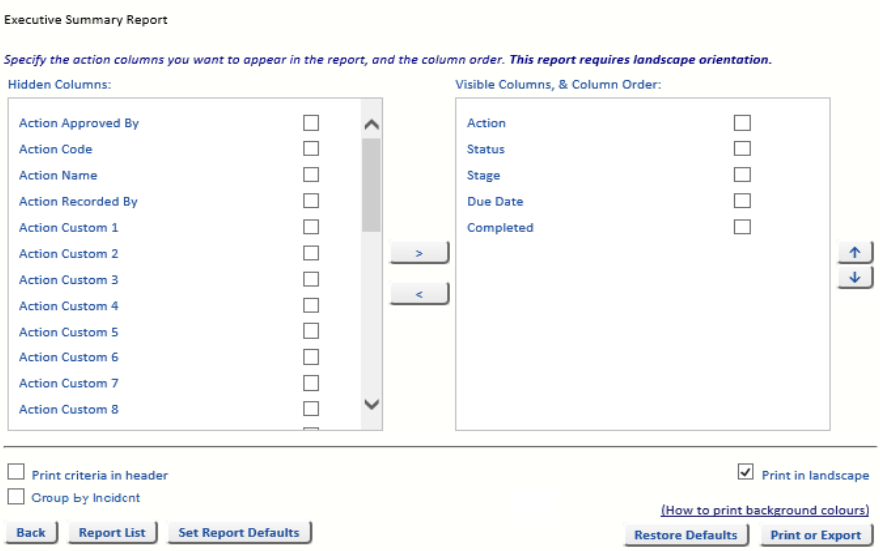
7.6.1. Executive Incident Summary Selections

Select the Incident columns you wish to see on the left side of the Executive Incident Summary Report.



At this point you may determine the order (left to right) of the selected columns.

Then after selecting the report order, select the Action columns you wish to see on the right side of the report.

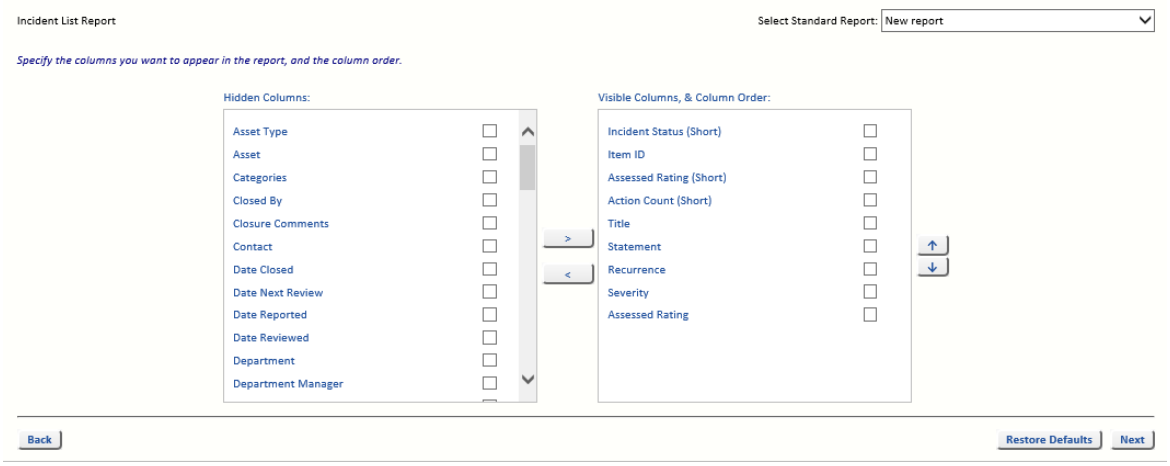


At this point you may determine the order (left to right) of the Action columns.

7.7. Incident List Report

Incident List Report is the quickest and easiest way to get a list of selected records. It allows you to select the columns in the printed list, the sort column and the sort order, and the number of Incidents to print.

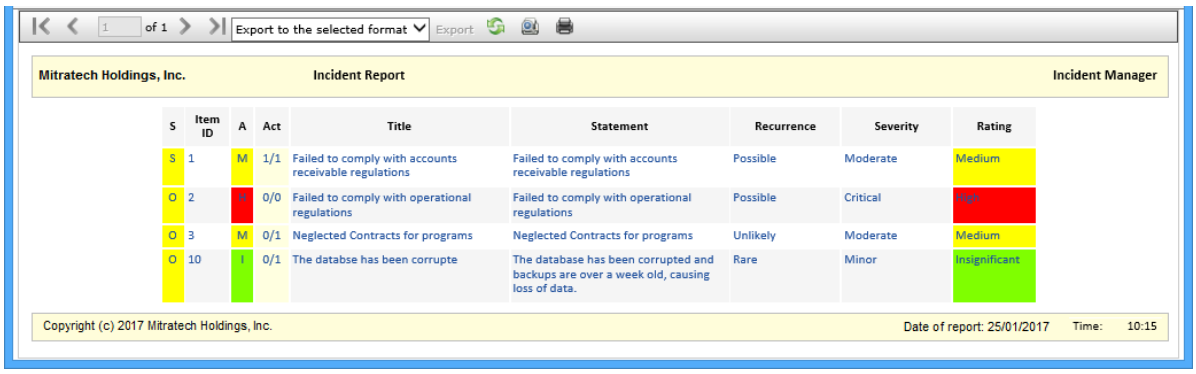
With Select Standard Report set to *New report*.



Select the columns you wish to print, and the order (left to right) of the columns.

Select the grouping and sort order in which you wish to print the information. If required, limit the number of incidents to be printed. By selecting the number of records to print, you will be able to print a top Incident report by whichever sort column you specify.

When you click *Print or Export* you will see the following style of display.



S	Item ID	A	Act	Title	Statement	Recurrence	Severity	Rating
S	1	M	1/1	Failed to comply with accounts receivable regulations	Failed to comply with accounts receivable regulations	Possible	Moderate	Medium
O	2	H	0/0	Failed to comply with operational regulations	Failed to comply with operational regulations	Possible	Critical	High
O	3	M	0/1	Neglected Contracts for programs	Neglected Contracts for programs	Unlikely	Moderate	Medium
O	10	I	0/1	The databse has been corrupte	The database has been corrupted and backups are over a week old, causing loss of data.	Rare	Minor	Insignificant

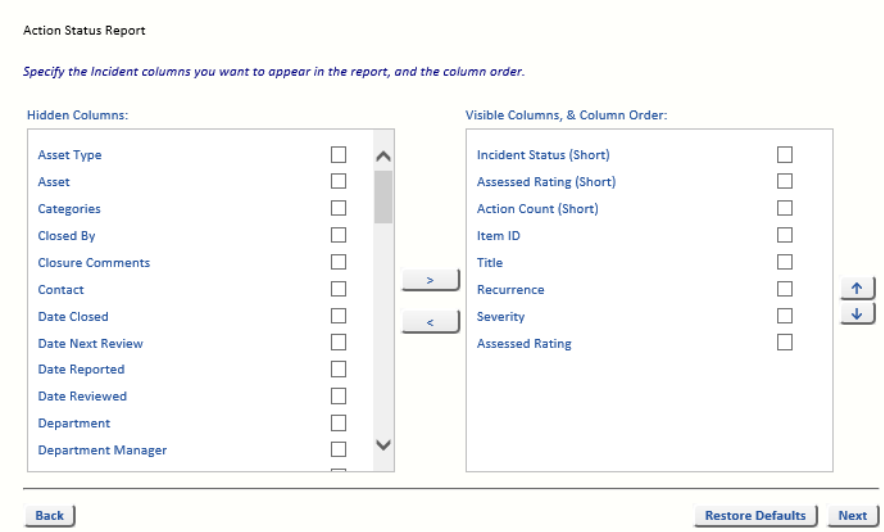
The export options are in the drop-down list:

- Acrobat (PDF file)
- CSV (comma delimited)
- Excel 97-2003 Workbook (.xls)
- Excel Workbook (.xlsx)
- Rich Text Format
- Word Document

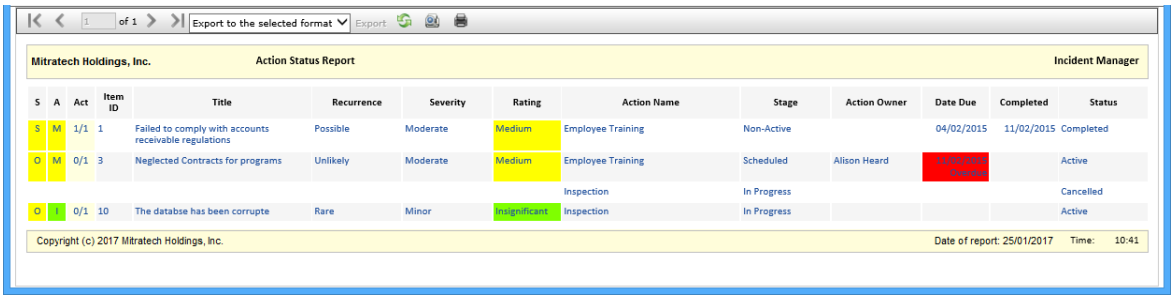
To get back to the menu system you will need to use the browser's *Back* button.

7.8. Action Status Report

The Action Status Report has the same two forms as the Incident List Report to select the Incident columns, report grouping and sort order. In addition, a third form allows you to select the Action columns that will be seen on the report.



The report may look like this depending on the selections made.

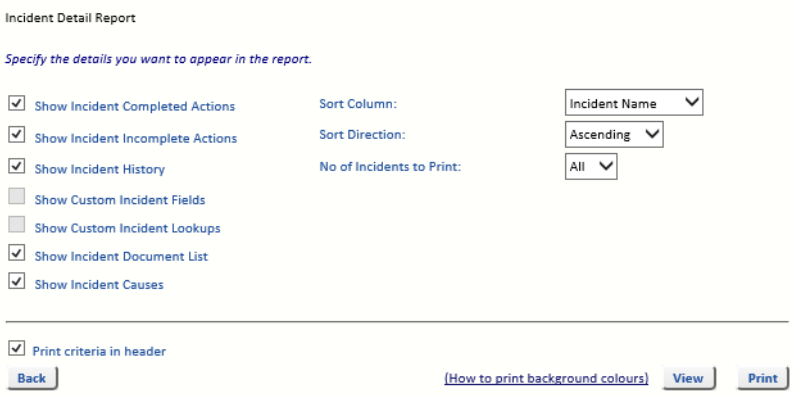


The Action Status Report has an option to print all Incidents even if they do not have Actions.

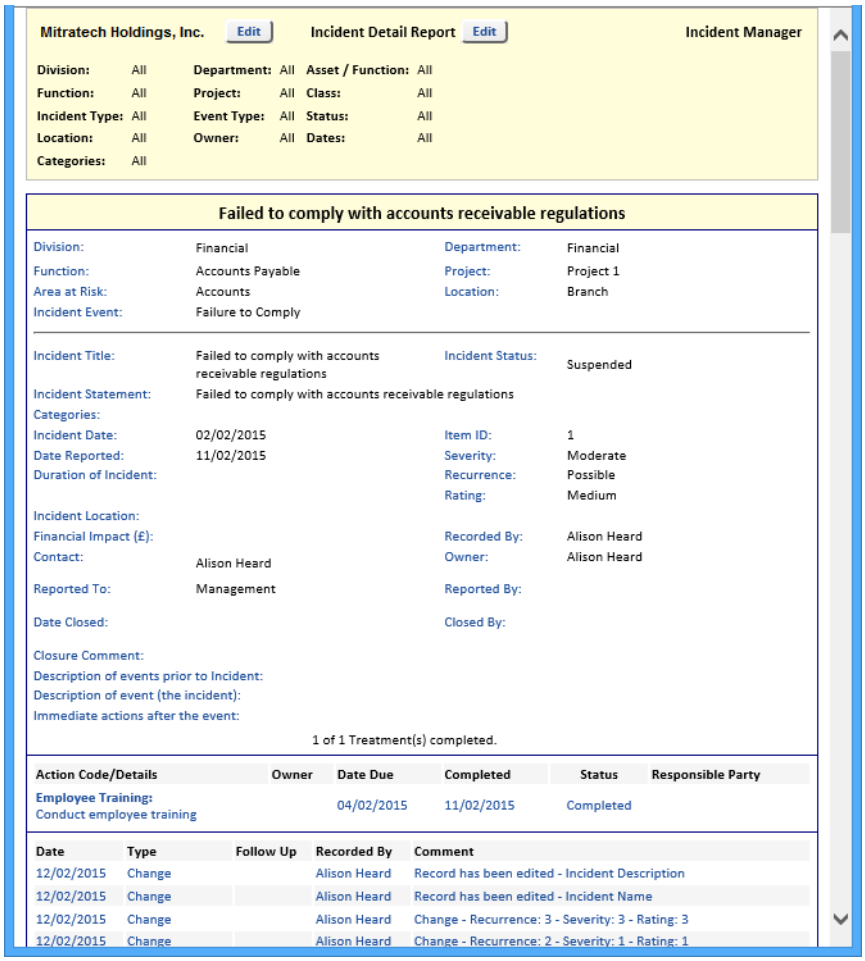
The Action Status Report column settings are separate to the column settings for the Action List at the top of the Action data entry page.

7.9. Incident Detail Report

The Incident Detail Report will print all details for selected Incidents. It allows you to select the sections of the report and the sort column, the sort order and the number of records to print.



By selecting the number of records to print, you will be able to print a detailed report of the top Incidents sorted by whichever column you select.



Mitratech Holdings, Inc. Edit Incident Detail Report Edit Incident Manager

Division:	All	Department:	All	Asset / Function:	All
Function:	All	Project:	All	Class:	All
Incident Type:	All	Event Type:	All	Status:	All
Location:	All	Owner:	All	Dates:	All
Categories:	All				

Failed to comply with accounts receivable regulations

Division:	Financial	Department:	Financial
Function:	Accounts Payable	Project:	Project 1
Area at Risk:	Accounts	Location:	Branch
Incident Event:	Failure to Comply		
Incident Title:	Failed to comply with accounts receivable regulations	Incident Status:	Suspended
Incident Statement:	Failed to comply with accounts receivable regulations		
Categories:			
Incident Date:	02/02/2015	Item ID:	1
Date Reported:	11/02/2015	Severity:	Moderate
Duration of Incident:		Recurrence:	Possible
		Rating:	Medium
Incident Location:			
Financial Impact (£):		Recorded By:	Alison Heard
Contact:	Alison Heard	Owner:	Alison Heard
Reported To:	Management	Reported By:	
Date Closed:		Closed By:	
Closure Comment:			
Description of events prior to Incident:			
Description of event (the incident):			
Immediate actions after the event:			

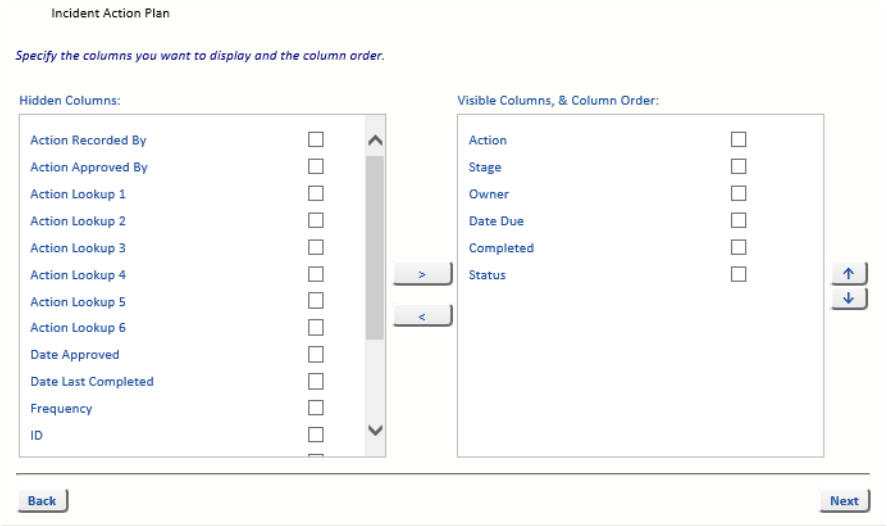
1 of 1 Treatment(s) completed.

Action Code/Details	Owner	Date Due	Completed	Status	Responsible Party
Employee Training: Conduct employee training		04/02/2015	11/02/2015	Completed	

Date	Type	Follow Up	Recorded By	Comment
12/02/2015	Change		Alison Heard	Record has been edited - Incident Description
12/02/2015	Change		Alison Heard	Record has been edited - Incident Name
12/02/2015	Change		Alison Heard	Change - Recurrence: 3 - Severity: 3 - Rating: 3
12/02/2015	Change		Alison Heard	Change - Recurrence: 2 - Severity: 1 - Rating: 1

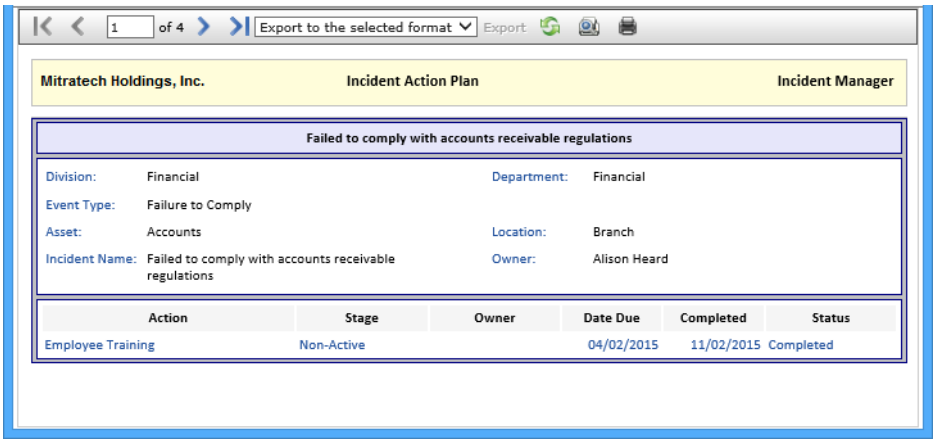
7.10. Incident Action Plan

The Incident Action Plan will print summary information for selected Incidents and the planned Actions for those Incidents. It allows you to select the sort column, the sort order, and the number of Incidents to print. This may be the best report to take to a management meeting when discussing budgets or Incident management activities.



By selecting the number of records to print, you will be able to print an Incident management plan for the top Incidents by whichever sort column you select.

The report shows the Actions for the Incidents.

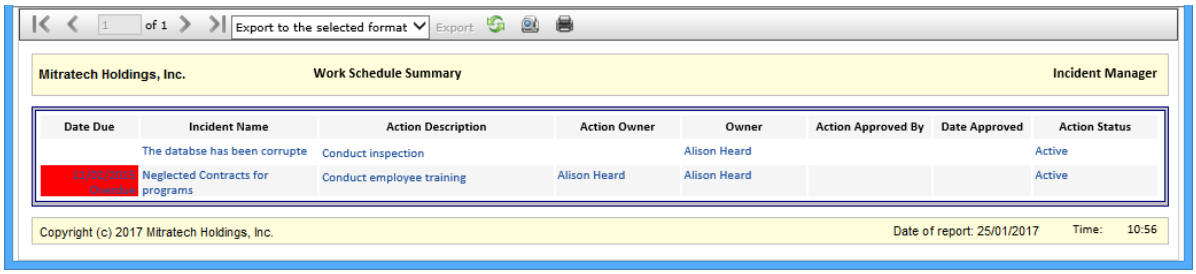


7.11. Work Schedule Reports

The Work Schedule reports will print summary or details of Actions for selected Incidents. It allows you to select the Action sort column, the sort order and the number of records to print.

This is the report that a workgroup manager would print to determine how to schedule Incident Actions.

An example Work Schedule Summary report.



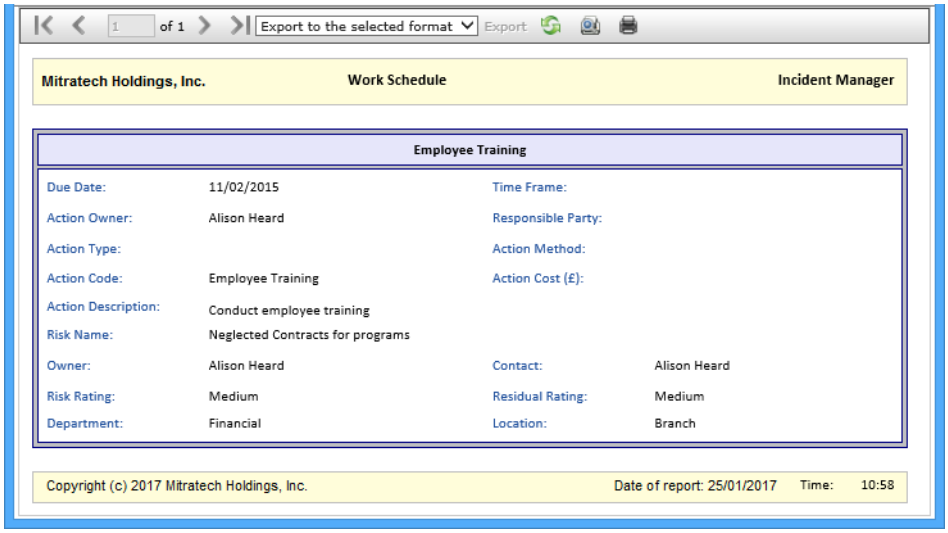
1 of 1 Export to the selected format Export

Mitratech Holdings, Inc. Work Schedule Summary Incident Manager

Date Due	Incident Name	Action Description	Action Owner	Owner	Action Approved By	Date Approved	Action Status
	The databse has been corrupte	Conduct inspection		Alison Heard			Active
11/01/2015 Overdue	Neglected Contracts for programs	Conduct employee training	Alison Heard	Alison Heard			Active

Copyright (c) 2017 Mitratech Holdings, Inc. Date of report: 25/01/2017 Time: 10:56

An example Work Schedule report.



1 of 1 Export to the selected format Export

Mitratech Holdings, Inc. Work Schedule Incident Manager

Employee Training

Due Date:	11/02/2015	Time Frame:	
Action Owner:	Alison Heard	Responsible Party:	
Action Type:		Action Method:	
Action Code:	Employee Training	Action Cost (£):	
Action Description:	Conduct employee training		
Risk Name:	Neglected Contracts for programs		
Owner:	Alison Heard	Contact:	Alison Heard
Risk Rating:	Medium	Residual Rating:	Medium
Department:	Financial	Location:	Branch

Copyright (c) 2017 Mitratech Holdings, Inc. Date of report: 25/01/2017 Time: 10:58

As the Incidents themselves can be filtered by Division, Department, Area/Function, Location and Incident Owner, and then the Actions can be sorted by Action Owner, Responsible Party, Due Date, Action Type, Action Method, a workgroup manager will have a powerful tool with which to schedule Incident Actions.

Note: Work Schedule reports provide data on *Open* Incidents.

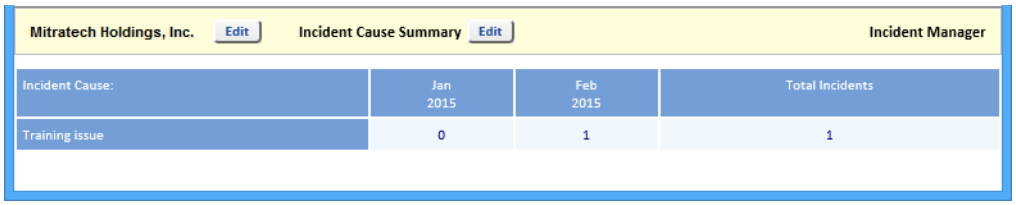
7.12. Classification/Cause/Event Type Reports

The *Incident Classification Report* shows the number of Incidents raised for each Classification for each month for the selected date range.

The *Incident Cause Summary Report* shows the number of Incidents raised for *All Causes*, or for just the selected Cause for each month for the selected date range.

The *Incident Event Type Summary Report* shows the number of Incidents raised for each Event Type for each month for the selected date range.

The *Incident Classification Report*, *Incident Cause Summary Report* and *Incident Event Type Summary Report* all use a similar format.



7.13. Template Reporting

If the user (normally the Incident Coordinator) has the appropriate permissions, they will be able to save the Incident List Report as a Report Template.

If the user clicks *Save Report Template* a dialog is opened and they can then name the report for later use.

The report template may later be selected by any user.

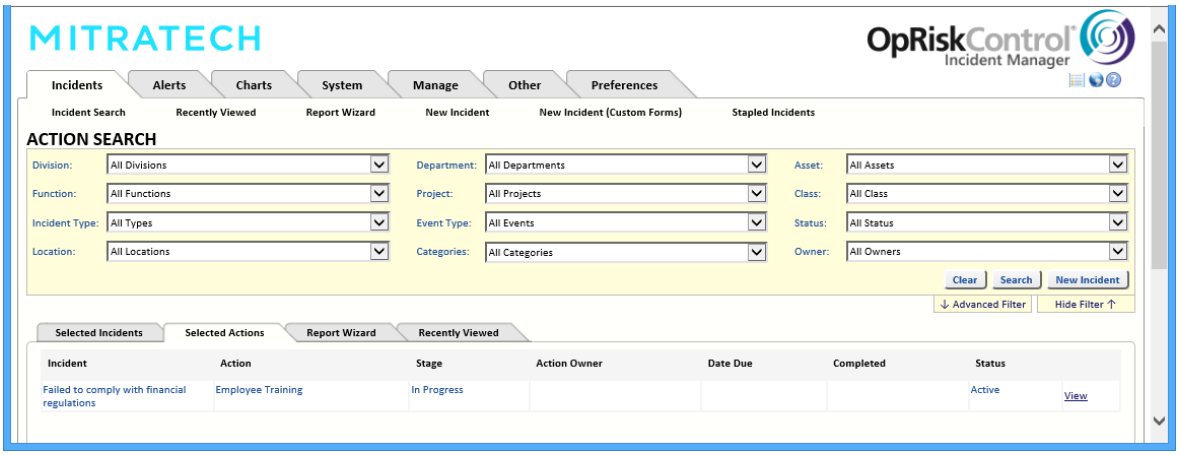
There are multiple stages to producing a report, and they are:

1. The report filter (what data to include).
2. The report layout (report type).
3. The report columns.
4. The report grouping.
5. The report sorting.

With OpRiskControl Incident Manager report templates, the only thing that can be changed by a user is the report filter. The rest of the report is fixed.

7.14. Selected Actions

Whenever a search is performed for Incidents, the Actions that relate to those Incidents are available on the *Selected Actions* tab.



Likewise, if an advanced text search is performed for a keyword in Actions and the results are displayed on the *Selected Actions* tab, the Incidents that relate to those Actions is available on the *Selected Incidents* tab.

8. Alerts

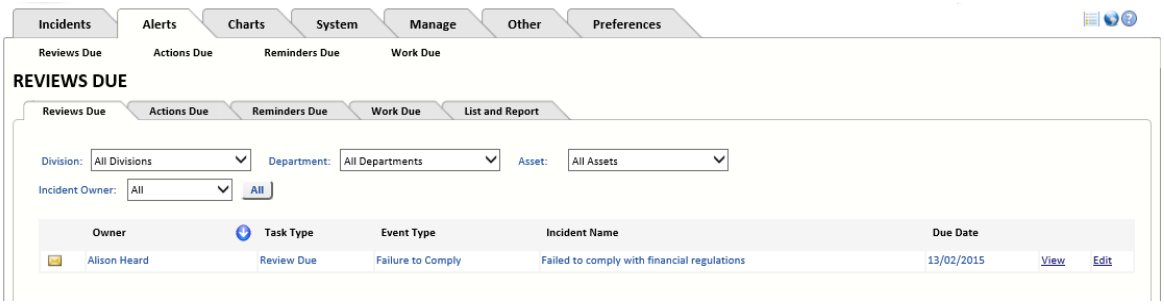
8.1. Introduction

Select *Alerts* from the main menu, and then select one of the following forms:

- Reviews Due
- Actions Due (or recurring controls due)
- Reminders Due
- Compliance Due (if Compliance Interface is being used). The Compliance Interface is an optional module, and details are available if requested.
- Work Due
- List and Report

8.2. Incident Reviews Due

Incident *Reviews Due* will create a list of every Incident (for the selected Incident *Owner*) which is expected to have been reviewed by the Incident Review Due alert date. The Incident Review Due alert date is derived by adding the review frequency (e.g. Month = 30 days) to the last review date and subtracting a configured review alert period (normally 7 days).

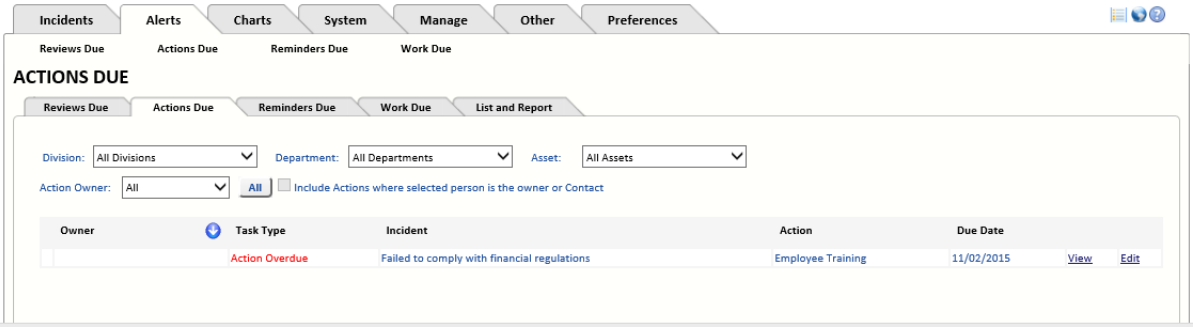


If any Incident review due date has passed, the words *Review Overdue* will be displayed in red. You can email the Incident owner listed for any Incident.

You may also filter by division, department and area at Incident.

8.3. Actions Due

Actions Due will create a list of every Incident (for the selected Incident Action Owner), which is expected to have been completed by the Action Due alert date. The Action Due alert date is derived by subtracting a configured Action alert period (normally 30 days) from the Action Due date.



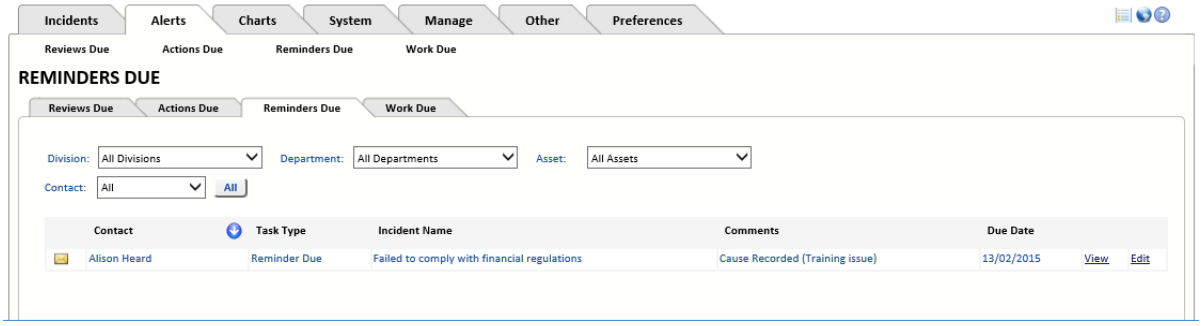
If any Action Due date has passed, the words *Action Overdue* will be displayed in red. You can email the Action owner listed for any Incident. In the above example it is quite evident why some Actions have not been completed as they have not been allocated an Action owner.

You may also filter by division, department and area at Incident.

You may find there are overdue Actions because no owner has been allocated to the Action.

8.4. Reminders Due

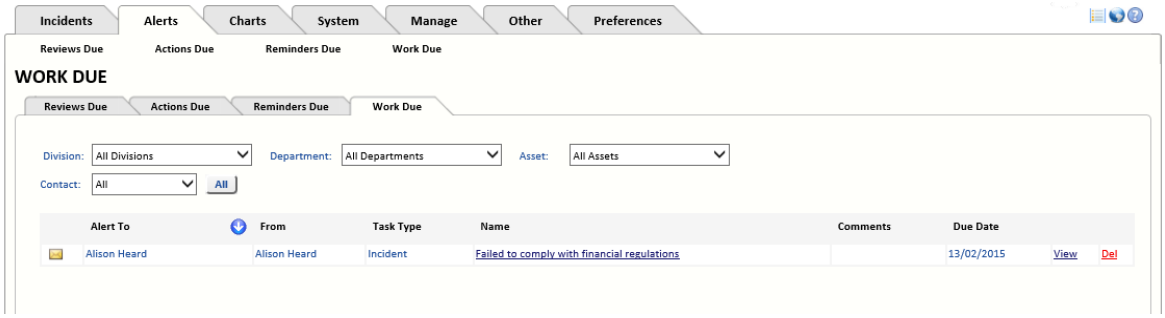
Reminders Due will create a list of every escalation reminder (set on the Incident History tab) that is due. The alert date is derived by subtracting a configured alert period (normally 1-3 days). from the Escalation Follow-up date.



You may filter by Contact, Division, Department and Asset.

8.5. Work Due

If anyone has routed work to the selected *Owner*, it is listed on this page.



Work is routed to specific people (or User Groups) via the *Route To* button on the main Incident form.

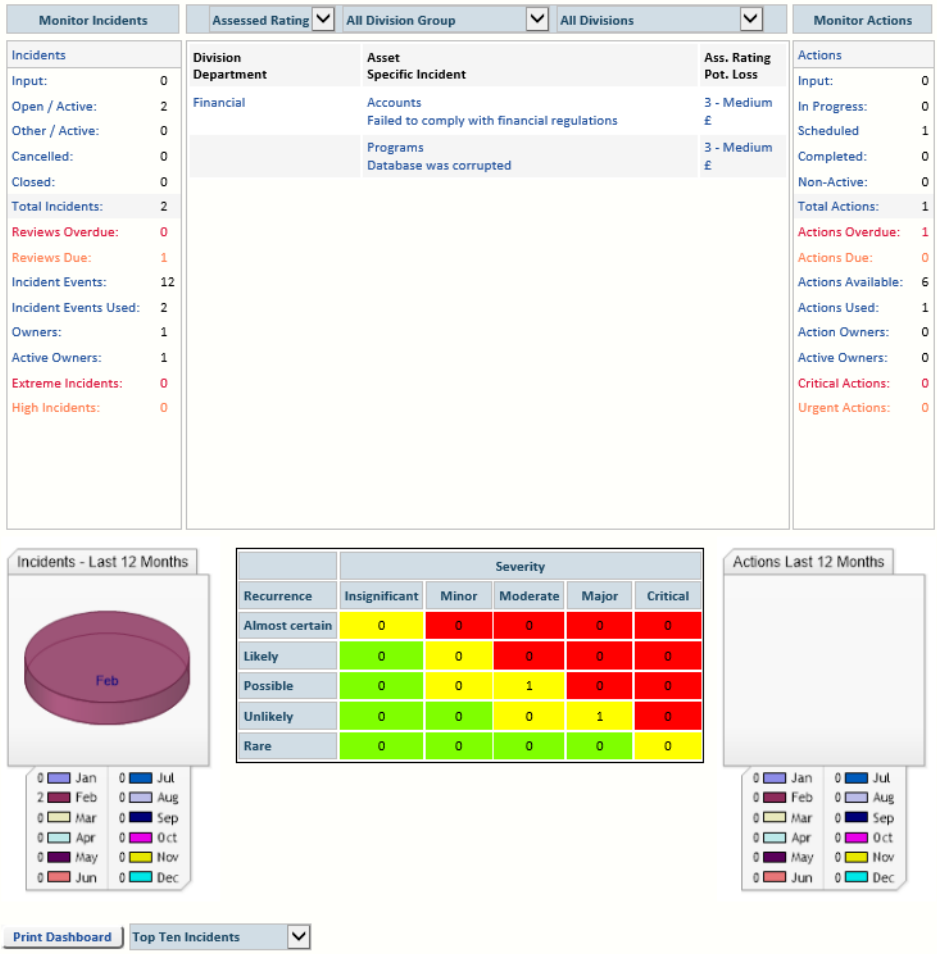
9. Charts

The Charts menu on the main menu includes any charting modules that have been purchased for your installation. The Incident Dashboard is provided with all systems.

9.1. Incident Dashboard

The Incident Dashboard provides insight into the effectiveness of the Incident management effort enterprise wide. The dashboard contains four areas of information:

- Incident counts.
- Action counts.
- Current top Incidents.
- Incident matrix.



The Dashboard normally shows Incidents, counts and statistics for the whole enterprise, but it can be filtered by Division or Division Group.

The *Monitor Incidents* section on the left shows Incident counts and the *Monitor Actions* section (which includes controls and Actions) on the right shows Action statistics. The explanation of these counts follows.

9.1.1. Monitor Incidents

- *Input* – Incidents that have been entered but not formally accepted into the system.
- *Open/Active* – Incidents that are currently active.
- *Other/Active* – Incidents which have been assigned non-system status codes are listed here.

- *Cancelled* – Incidents that may not now be required (e.g. duplicate Incident).
- *Closed* – Incidents that do not exist now.
- *Total Incidents* – Incidents that exist in the system regardless of status.
- *Reviews Overdue* – Incidents where the review date has passed.
- *Reviews Due* – Incidents where the review date is approaching (within the time band configured in System Settings).
- *Incident Events* – Potential Incident Events set up in the system.
- *Incident Events Used* – The number of Incident Events that have associated Incidents.
- *Owners* – The number of people (and/or roles) that own Incidents.
- *Active Owners* – The number of people (and/or roles) that own Incidents that are currently open/active.
- *Extreme Incidents* – The number of Incidents that are currently rated at the highest level.
- *High Incidents* – The number of Incidents that are currently rated at the second highest level.

9.1.2. Monitor Actions

- *Input* – Actions associated with Incidents that have not formally been accepted into the system.
- *In Progress* – Actions associated with Incidents that are open/active and neither the Action *Due Date* nor the Action *Date Completed* has been entered.
- *Scheduled* – Actions which have been assigned a *Due Date*.
- *Completed* – Actions associated with Incidents that are open/active and the Action *Date Completed* has been entered.
- *Non-Active* – Actions associated with Incidents that are not open/active.
- *Total Actions* – Actions that exist in the system regardless of status.
- *Actions Overdue* – Actions where the due date has passed.
- *Actions Due* – Actions where the due date is approaching (within the time band set up in System Settings).
- *Standard Actions* – The number of *Action Codes* in the system.
- *Action Used* – The number of Action types which includes ad hoc Actions and standard mitigations set up in the system. The count may be more than Actions Available due to ad hoc Actions.
- *Action Owners* – The number of people (and/or roles) that own Actions.
- *Active Owners* – The numbers of people (and/or roles) that own Actions that are currently open/active.
- *Critical Actions* – The number of Actions that are associated with Incidents that are currently rated at the highest level.
- *Urgent Actions* – The number of Actions that are associated with Incidents that are currently rated at the second highest level.

9.1.3. Pie Charts

If your installation has a charting license then you will be able to see a small chart on either side of the Incident matrix as follows:

The left chart will show *Incidents entered by month* for the last 12 months and the right chart shows *Actions completed by month* for the last 12 months.

9.2. Chart Wizard

The Chart Wizard selects the chart to be used with various information. There are chart criteria based on average values and chart criteria based on total values.

The Chart Wizard uses the same filter as the *Incident Search except that only Open Incidents are shown*, and remembers selections from one program to the other. When the filter is changed, you need to click the *Search* button, and when that is done, the number of Open records is displayed on the right side of the form.

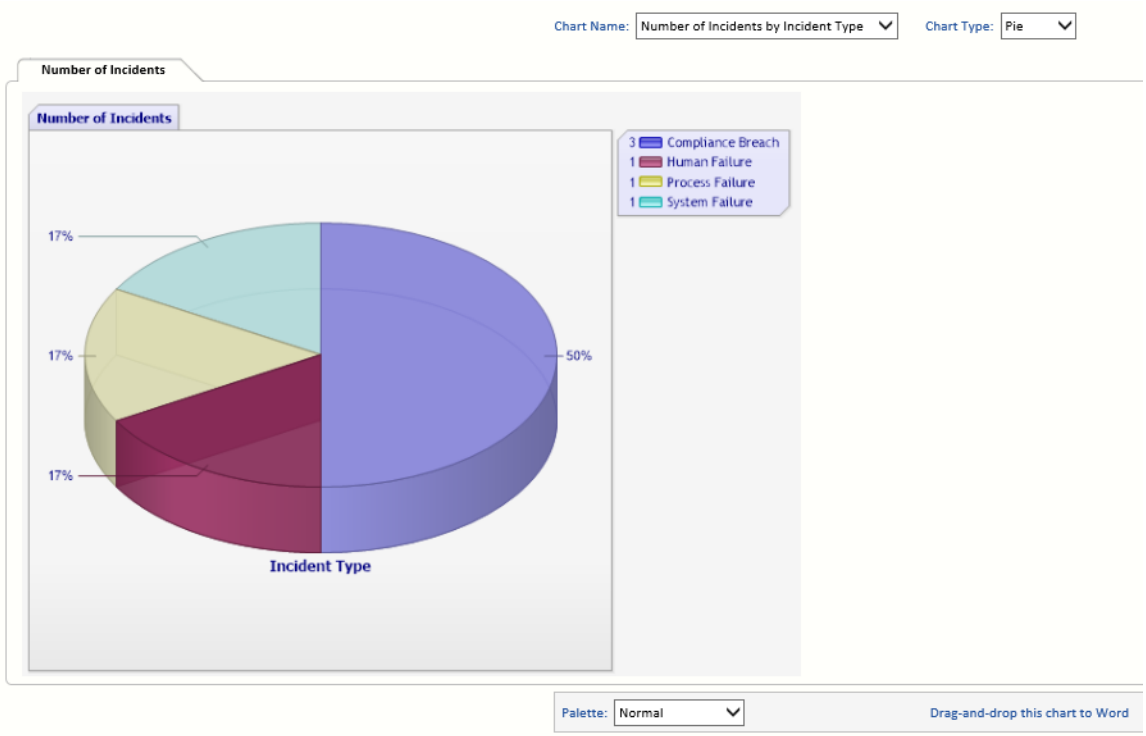
Chart options depend on the chart type. The toolbar above the chart allows you to customise the chart by selecting:

Chart Name – select the type of information displayed in the chart:

- Number of Incidents by:
- Asset/Area.
- Cause Code.
- Department.
- Division.
- Event Type.
- Function.
- Incident Group.
- Incident Type.
- Location.
- Project.

Chart Type – select the type of chart (*Column*, *Bar* or *Pie)*.

The toolbar below the chart allows you to manage the presentation, not the data that is displayed. You may change the palette, and, depending on the type of chart, select the sort sequence.

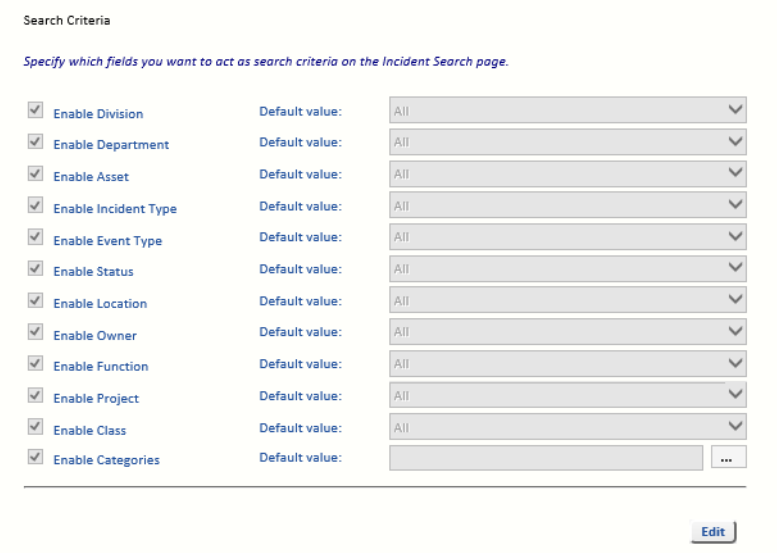


10. Preferences

Preferences may be changed at two levels. The System Administrator may change system wide preferences (on the *System* tab select *System Settings*), or users may change their personal preferences from the *Preferences* menu.

10.1. Search Criteria

Select the *Preference* tab then select *Search Criteria*. Select the criteria you want to be set by default when searching for Incidents. Users do not have to use the default search criteria and can change the criteria used when they search for Incidents.

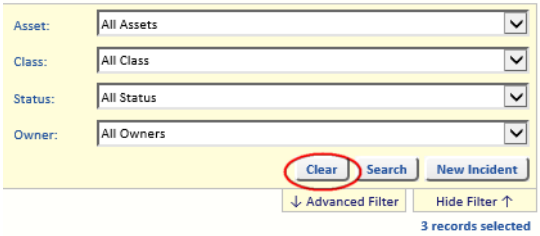


The criteria are normally set to *All* initially (except Categories, which is blank), but if you are working on a specific area, then you might want to configure the default values to show just the Incidents in which you may be interested. One criterion you might want to set here is the Incident *Status* to *Open* so that only open Incidents are displayed by default.

To edit a default value, click edit and select the required default value from the drop-down list. To edit the default value for Categories, click the ellipsis button (...) and select the required Categories from the list. Close the Category Selector window by clicking the *x* in the top right corner. The selected Categories are displayed.

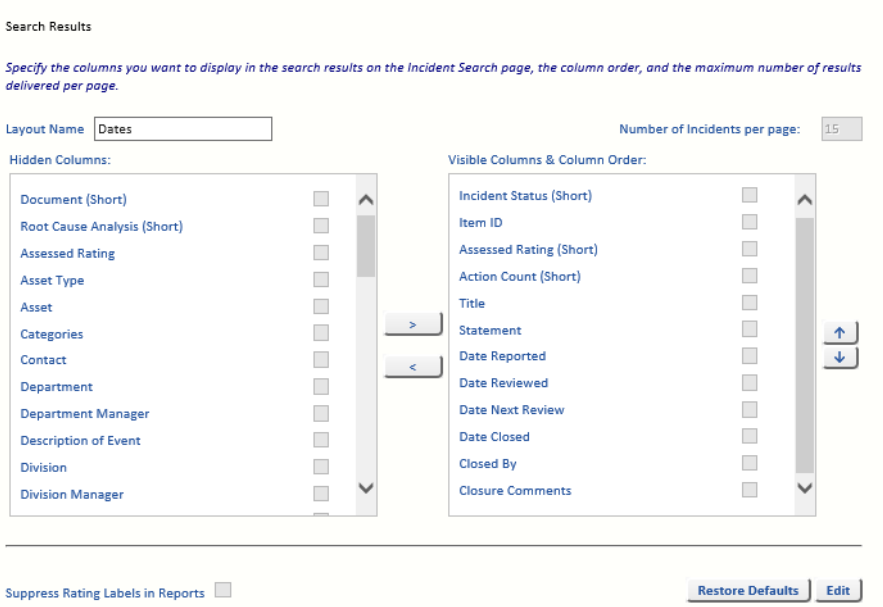
Click *Save* to save the changes, or *Cancel* to discard the changes.

The new defaults are displayed on the Incident Search page after the *Clear* button is clicked.



10.2. Search Results

From the *Preferences* tab, select *Search Results*. This page displays the available layouts which can be selected on the *Incident Search* results page.



To change any settings, first click the *Edit* button to enter Edit mode.

The *Search Results* preferences page allows you to configure the layouts you may select when you do an Incident search. The initial settings for the layouts are:

All layouts will normally have the following columns:

- The 2 SART columns (Status, Assessed).
- The *Act* column (meaning Actions) shows the number of Actions completed/number of Actions active.

Click the *Edit* button to enter Edit mode. You can then select a layout to edit.

10.2.1. Entry Layout

The default layout is the *Entry* layout and this layout has the following defaults:

- Item ID
- The 2 SART columns (Status, Assessed).
- The *Act* column (meaning Actions) shows the number of Actions completed/number of Actions active.
- Incident Name
- Description
- Recurrence
- Severity
- Assessed Rating
- Residual

10.2.2. Other Layouts

Other layouts default to different aspect such as:

- Dates
- Location

- Ownership
- Review
- Value
- Other

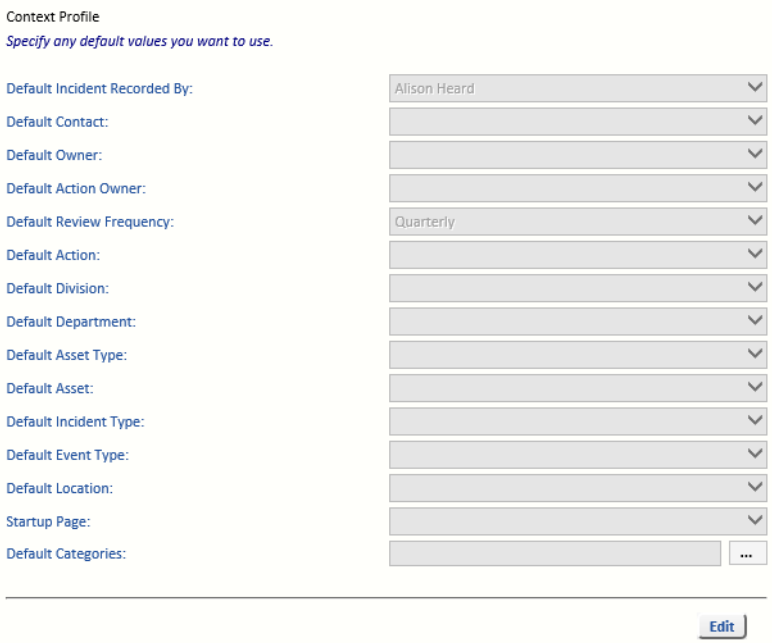
Although you cannot *Edit* the *Layout Name*, you can change the columns you want to be displayed and the order of the columns on the screen. Click the *Edit* button and select a layout from the *Layout Name* drop-down list. You can now make changes to the selected layout.

You can hide or reveal columns by selecting the tick-box of the column you want to move and then by using the < or > buttons. Alternatively, select the *Incidents* tab then select *Incident Search*. The *Search Results* page is displayed and the layout can be changed by selecting a *Layout* from the drop-down list. The *Edit Layouts* link then allows you to edit the currently selected *Layout*.

Note: In *View* mode, and with the relevant layout displayed in *Layout Name*, you may *Restore Defaults*.

10.3. Context Profile

Select the *Preferences* tab then select *Context Profile*.



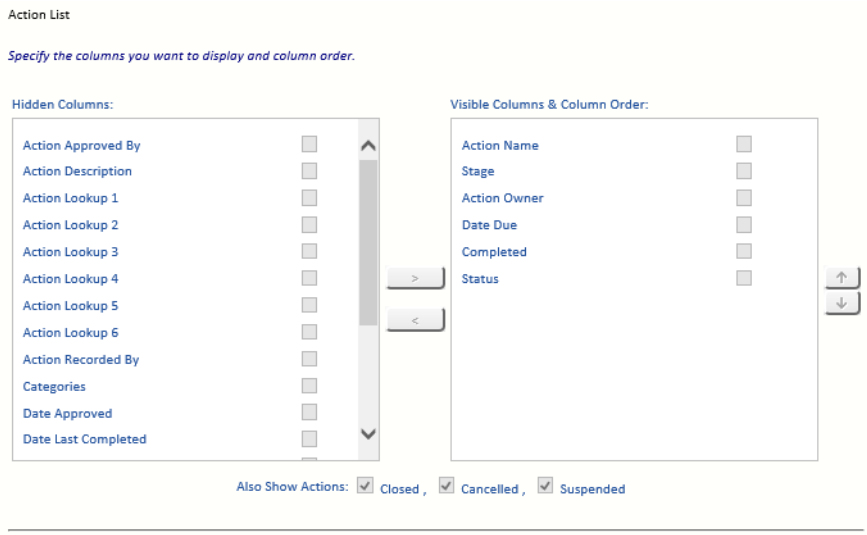
The *Context Profile* ensures your data entry may be as quick and effortless as possible. If you are focusing on, for example, construction workforce safety for steelworkers and are entering a batch of Incidents for a new project, you could set the division to *City Works*, the department to *Civil Engineering*, the area at Incident to *Construction* and the location to the building address. Then, while you enter Incidents relevant to that area, these fields would be populated automatically. You might then set the Incident contact as *Business Unit Manager* and the Incident owner and Action owner as *Project Manager*, and the review frequency to, for example, *Quarterly*.

Even though fields default to the values set here, they may be changed on the Incident as it is being created or at any time later.

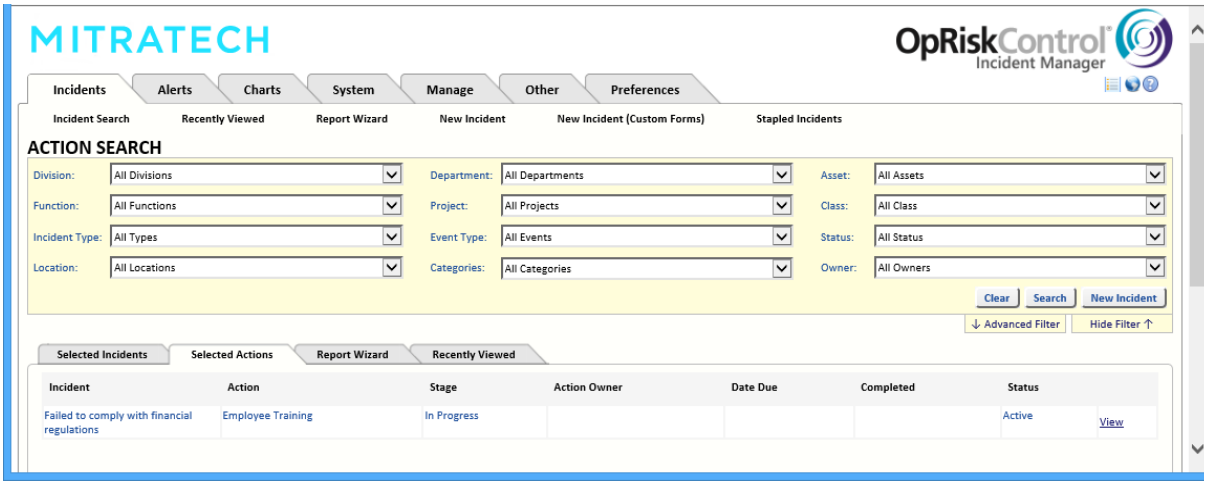
The system sets your name in the *Recorded By* field, because that allows the system to automatically log who creates Incident records or makes changes in the system.

10.4. Action List

Select the *Preferences* tab then select *Action List*.



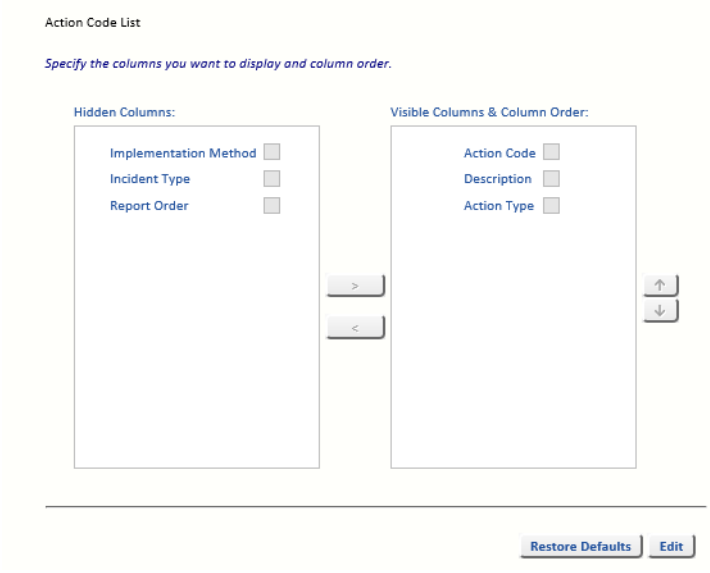
The Action list form allows you to specify the columns you want to see in the list of Selected Actions (on the *Incidents* tab, select *Incident Search* and then select the *Selected Actions* tab).



The *Status* column is controlled by system users, while the Stage column is determined by the system.

10.5. Action Code List

Select the *Preferences* tab and then select *Action Code List*.



The *Action Code List* page allows you to specify the columns you want to see in the list of Action codes displayed on the *Action Codes* summary page. Select the *Manage* tab, then select *Reference Data* and select *Action Code* to see a summary (displaying just the columns selected above) of the *Action Codes*.

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

MITRATECH

www.mitratech.com

5001 Plaza on the Lake, Suite 111, Austin, TX 78746
Tel: US (512) 382-7322. Email: support@mitratech.com

6575 West Loop South, 3rd Floor, Bellaire, TX 77401
Tel: US (888) 272-4699

460 Norristown Road, 3rd Floor, Blue Bell, PA 19422
Tel: US (610) 729-1100

430 Bath Road, Slough, Berkshire, SL1 6BB
Tel: UK +44 (0)1628 600900

1 Kingdom Street, Paddington, London, W2 6BL, UK

432 St. Kilda Road, Melbourne, Victoria 3004
Tel: Australia +61 (0)3 9521 7077