- Alerts Management –

Alerts V1

FOR RISKMAN VERSION 2503

Last reviewed March 2025

CONTENTS

INTRODUCTION

This reference guide is aimed at Administrators/Managers who will be responsible for creating and managing Alerts within RiskMan. Alerts can be created for all Registers that are activated within your RiskMan e.g. Incidents, Feedback, Risk Register, Quality and any client specific customised Registers.

What is an Alert?

User Defined Alerts are a means by which the system can autonomously monitor Notifications/Items/Activities for pre-defined conditions, and when they occur, notify one or more users with a pre-defined e-mail.

There are 3 types of Alerts

Standard Alerts: These are alerts where, when the conditions are met in the notification, the alert is triggered. The alert can be triggered once (immediately when the conditions are met) or every time the conditions are met e.g. Notify the CEO and Executives if an Incident has a Severity = ISR 1 or ISR 2.

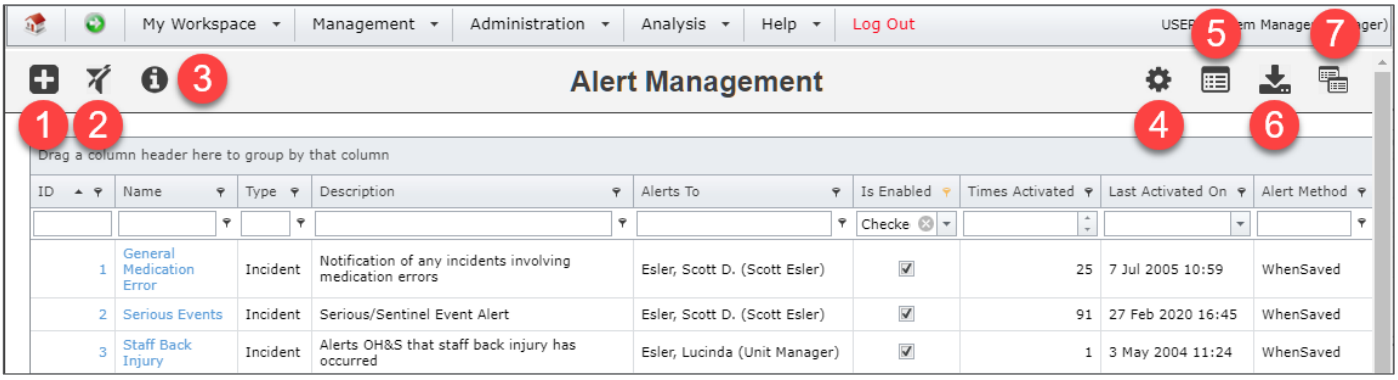
Time Based Alerts: These are alerts that can be processed at specified intervals until the condition of the notification changes e.g. Notify the reporter's manager if investigations are not complete within 2 days of the incident date; Notify the owner of a Journal Task that the Journal is more than 2 days overdue; Notify the owner of a Risk that it needs to be reviewed in a week.

Threshold Alerts: These alerts monitor the frequency of notifications based on a set of conditions in a given period of time. Examples might include:

- Notify the owner of the Medication related risk if the number of medication related incidents that resulted in an adverse drug reaction has occurred more than twice in a month
- Notify the OHS Manager if there are more than 3 staff incidents resulting in an injury in a particular location in a month
- Notify the manager of the relevant Department if there are more than 2 complaints raised in a particular department in a week
- Notify the OHS Manager when there is a department with non-compliance re the OHS Environmental Audit

Threshold alerts will **ONLY** send an email notification to the allocated recipients when the number of notifications **exceeds** the specified number in a particular time period. It **WILL NOT** grant the recipient/s permission to these notifications/activities/items. Another alert may need to be created to grant the users access to these notifications/activities/ items so they can view or run a report on them if the Threshold is exceeded.

Alert Management Inbox



Icon ❶: Add an Alert

Add Alert icon allows you to add a new Alert.

Icon ❷: Clear Filter

Will clear ant filters that have been applied to the Alert Management inbox list.

Icon ❸: Hide/Show Information Panel

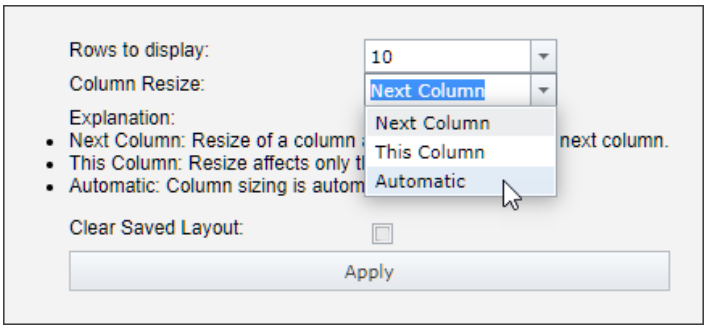
Information provided about the specific functions that can be completed within the Alert Management inbox.

Icon ❹: Apply Settings

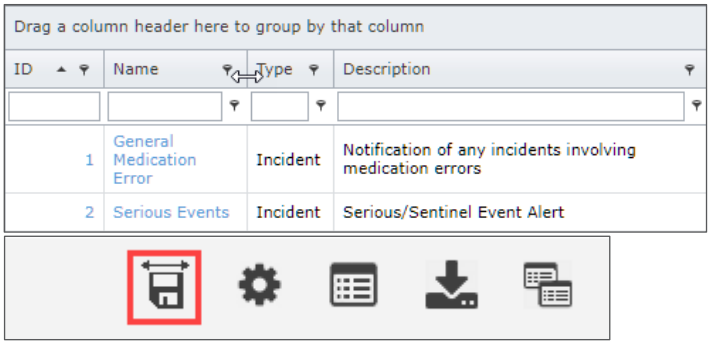
Change the layout of your Inbox for columns and rows (Will not change other users Inbox setting).

Column Resize: There are 3 options available in the dropdown box to adjust your inbox columns/view:

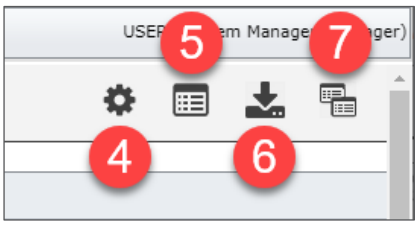
- **Next Column** - When adjusting a column, the column next to it will also adjust along with it as you resize
- **This Column** - Adjusts the column you select and no other columns will be affected as the option above will do
- **Automatic** - Will automatically adjust the columns to fit all text



- You can also adjust the width of your columns by placing your cursor between columns and dragging them to the desired width.
- Once the columns have been resized, another icon will appear to save that layout. This will ensure that the view is saved each time you log back into the system.



Icon ❺: Change Columns



Choose which columns of information you would like to see on your Alert Management page.

Icon ❻: Export to Excel

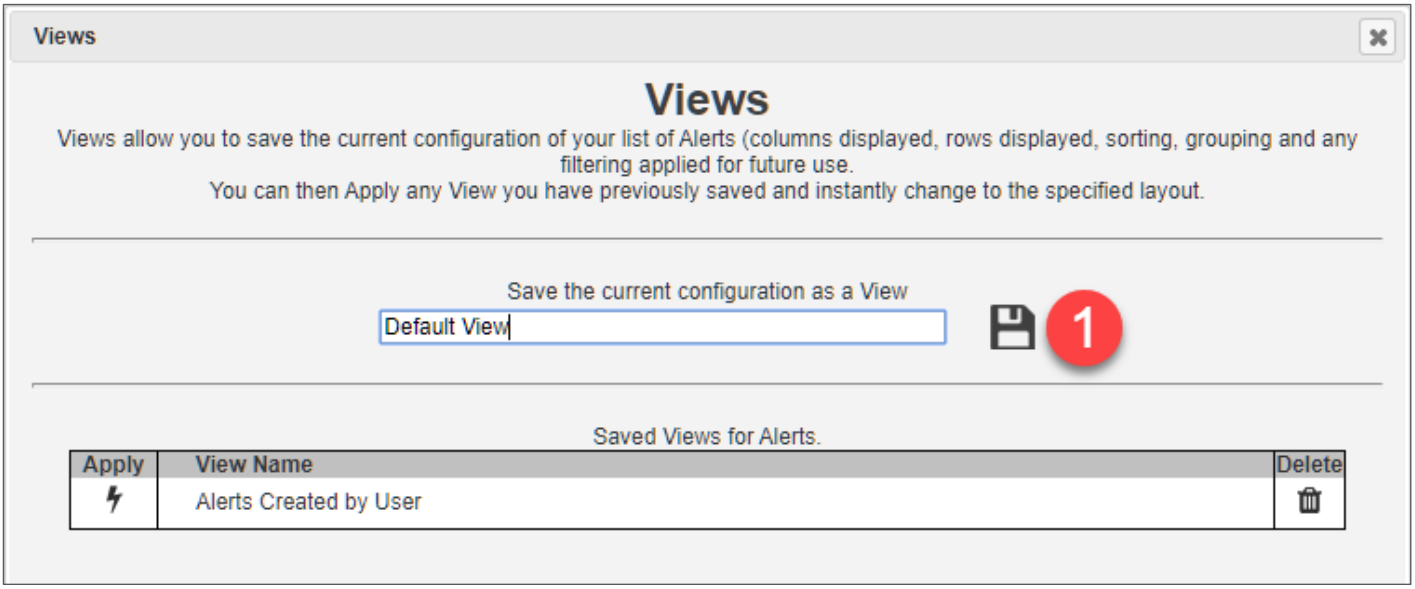
Export the inbox to Excel. When exporting the inbox, it will export all sorting, filtering and grouping applied.

Icon ❼: Views

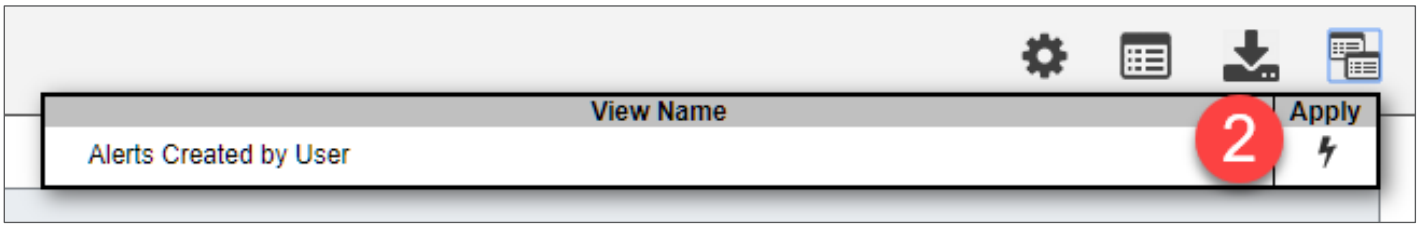
Views allow a user to save the current configuration of the Alerts list (columns displayed, rows displayed, sorting, grouping and any filtering applied for future use.

Apply any view you have previously saved and instantly change to the specified layout.

❶ To save the view, the view requires a title for future reference. For example, “Alerts created by”. Then select the save icon

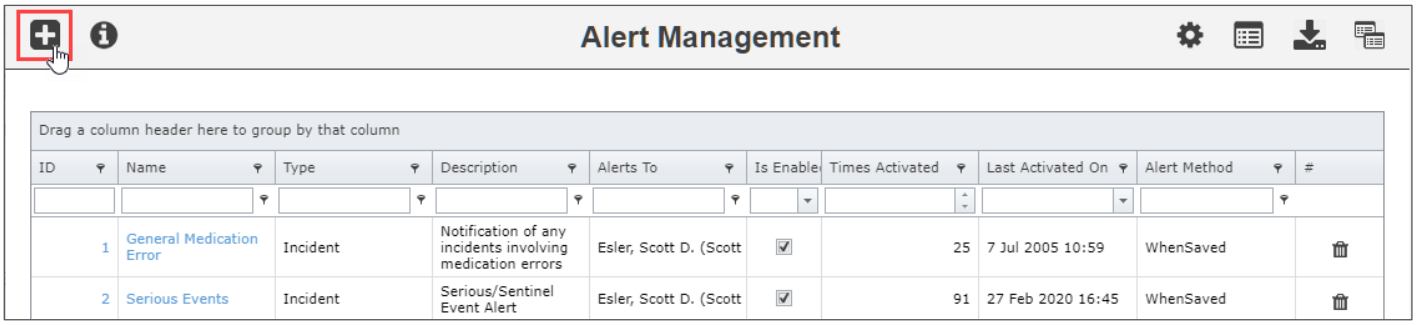


❷ Once the view has been saved, select the saved view by moving the cursor over the view icon and select the apply icon

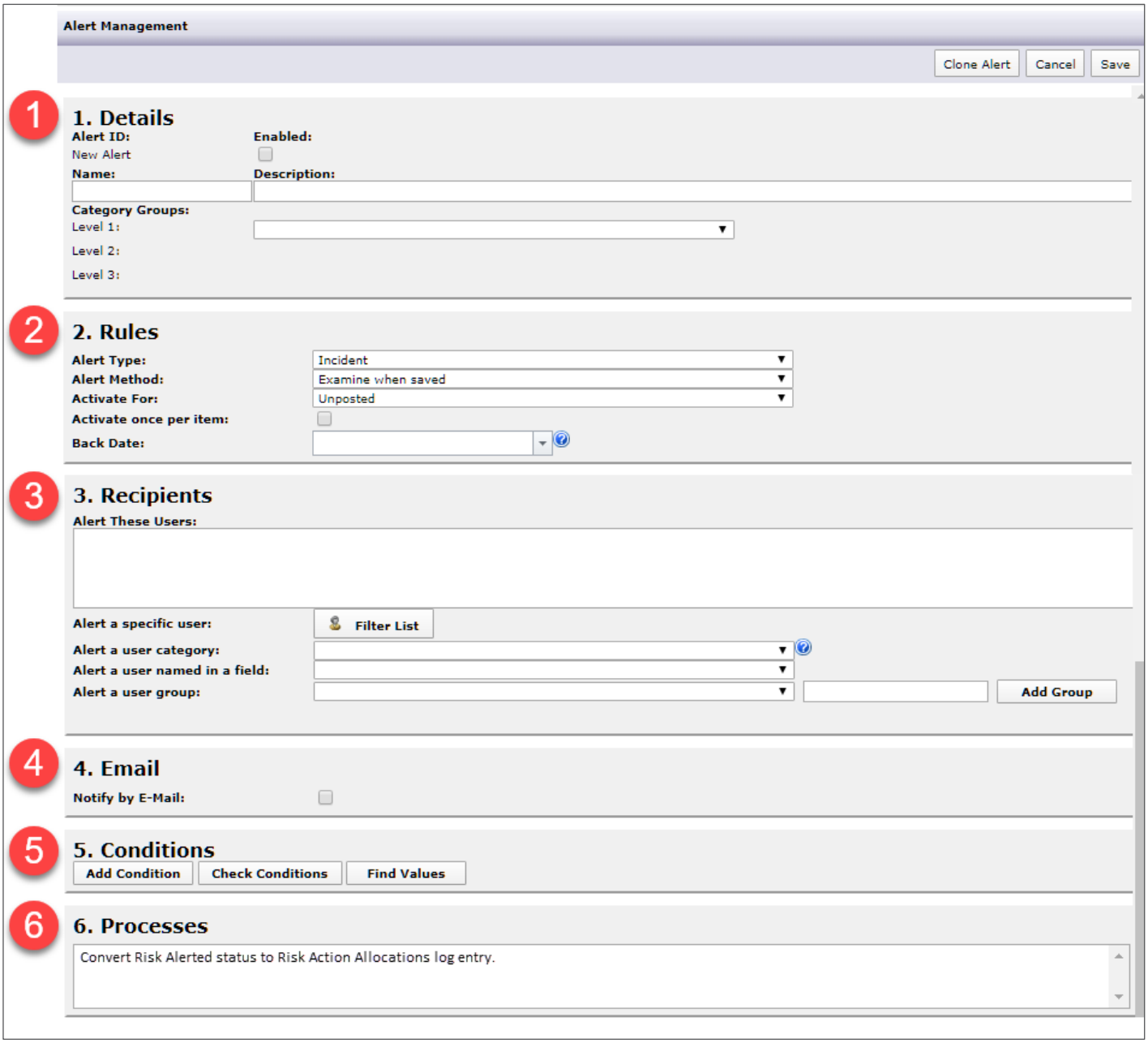


How do I create an Alert?

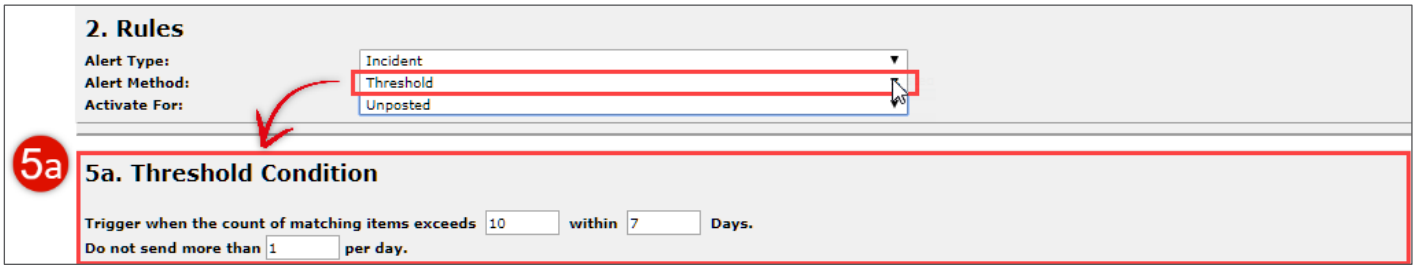
Alerts are created from the Alert Management page, by selecting Administration -> *Alert Management*
To create an Alert, select the icon 



***Note**: The below example represents the 6 areas used to create an Alert*

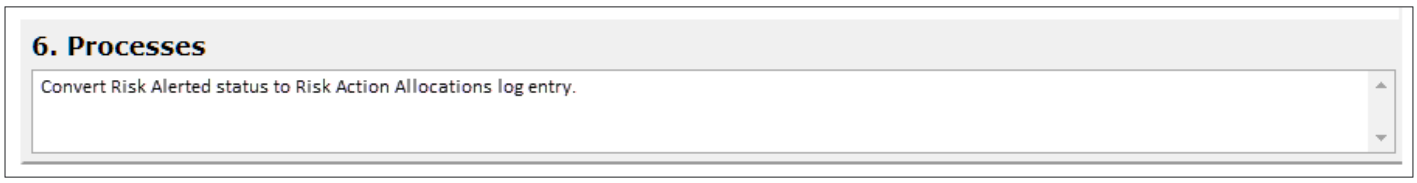


***Note**: If the Alert is a Threshold Alert an additional section will display as in the example below*

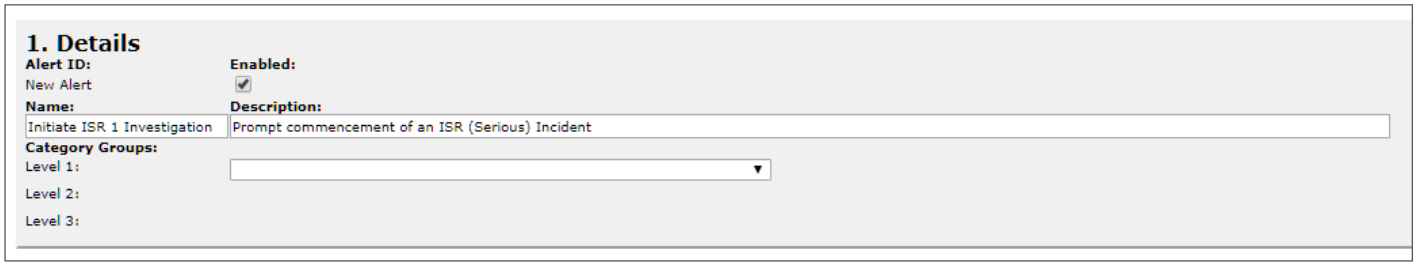


***Note**: One of the delivered Risk Alerts - "**Assign Action Response emails**" has an additional process to enable users who are assigned an action from a Risk to be able to provide a response to the assigned action without giving the user permission to the risk (if they do not normally have access to the Risk Register)*

Some organisations may have specific Processes included in their Alerts e.g. update information in the Review History of a Register item when the alert is triggered; extract information from a Register item so that it can be updated into a 3rd party database



Step ❶: Details



This section allows you to enter the following information

1. The **Name** and **Description** of the Alert. The **Name** will appear in your Alert list to easily identify the alert
2. **Is the Alert Enabled?**
   - If **checked**, the Alert will be active as soon as the notification/item/activity is saved
   - If this is **unchecked**, the Alert will **not** be active. If you choose to activate the alert on a later date, the system will check all notifications/items/ activities that match the condition of the alert from when the alert was first created (not when it became active). If that is the case and you want the alert to be active from today, then under the **Step 2: Rules** section enter today's date in the **Back-Date** field
3. **How is the Alert categorised?**
   - Each Alert can be categorised by user defined categories e.g. OHS, Serious Incidents, Complaints, System Workflows, Facility, Audits, Reminders. These categories are used to filter and group the alerts on the Alert Management listing page.
   - These categories are maintained in the Administration -> List & Codes Maintenance page under the following lists: *(Alert) Level 1*; *(Alert) Level 2*; *(Alert) Level 3*

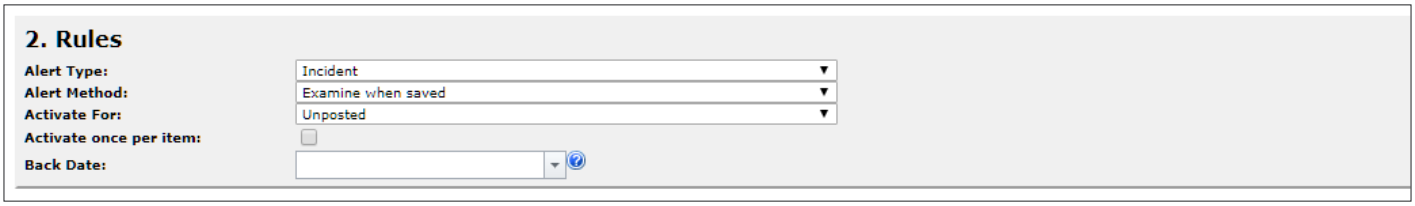
Step ❷: Rules – Standard Alerts

The following information describes the rules when creating standard alerts i.e. **Alert Method = Examine When Saved**.

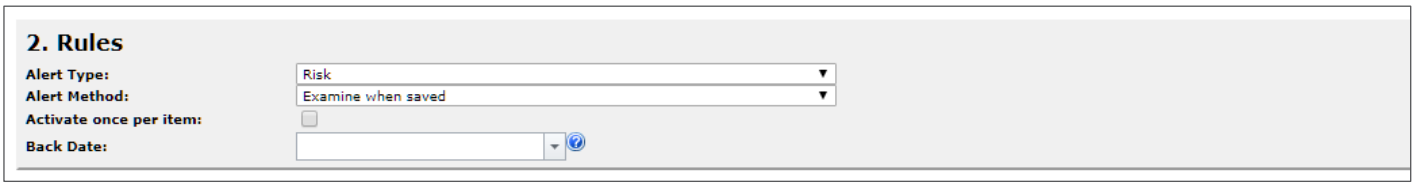
Examples of these types of alerts might include:

- Incidents with a Severity = ISR 1 or ISR 2
- Incidents that relate to Infection Control
- Incidents where a staff injury has occurred
- A Complaint has been lodged
- A Risk has been assigned to an Accountable Executive
- A recommendation from a Quality Activity has been assigned to a Manager

***Example:** Rules for **Standard Alerts** on **Incidents**, **Feedback** and any other Registers that use the concept of Posted and Unposted items*



***Example:** Rules for **Standard Alerts** on **Risks**, **Quality Activities** and any other Registers that do not use the concept of Posting*



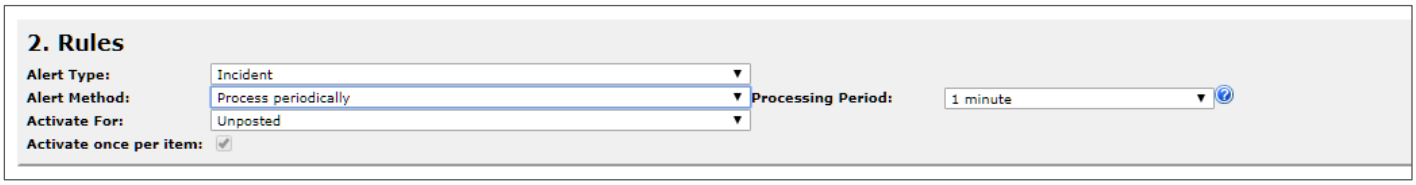
1. **Type of alert:** Select the Register the alert relates to i.e. Incidents, Feedback, Risk, Activity - this will depend on your permissions and the Registers that are activated in your RiskMan
2. **Alert Method:** Examine When Saved
3. **Activate For:** This field will only show if the selected Register in the **Alert Type** field uses the concept of Posted and Unposted Notifications e.g. Incidents & Feedback. **Activate For** asks you - “Is the alert activated on posted or unposted notifications?”
    - If **Unposted** is selected, it means that the alert will trigger as soon as the conditions are met on the notification e.g. new incident or complaint.
    - If **Posted** is selected it means the alert will only trigger if the notification is posted i.e. A master version has been created. Users selected to be notified of the alert need to at least have the permission to **view posted <register> items** in their respective Register User Profile
4. **Activate Once per Item:** Check if you only want the alert to trigger when the conditions are initially met or leave unchecked if you want the alert to trigger every time the conditions are met *(in most cases this option would be checked)*
5. **Alert Back Date:** Check this field and enter the respective date, if the alert is to be back dated so the user has access to past register items e.g. Incidents, Feedback, Quality Activities, Risks. This date represents the date the Notification was last edited so if you wish to give a recipient permission to all notifications then select a date that was prior to you using RiskMan e.g. 1/1/1990.

***Recommended:** If you are backdating an alert, **turn off** emails to ensure the user does not receive an excessive number of emails. Once the alert has triggered you can modify it and turn emails on. Back dating is useful if a new manager is taking on an existing role where he/she needs access to past notification/activities/items*

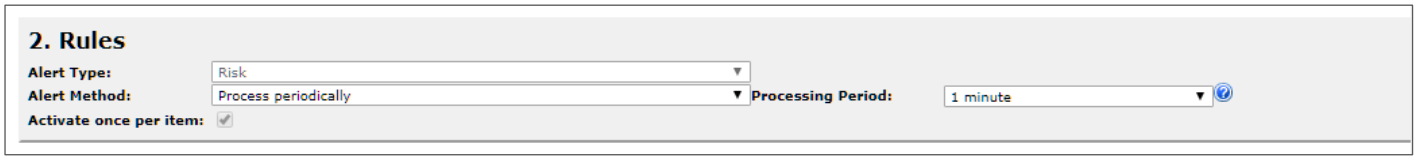
Step ❷: Rules – Time Based Alerts

The following information describes the rules when creating time-based alerts i.e. **Alert Method = Process Periodically**. Examples for these types of alerts include:

- Remind Line Managers if they have not completed their investigations based on the number of days since they were notified of the incident.
- Remind Consumer Advocates that a complaint has not been closed and it is over 30 days since it was opened
- Notify the person who has been allocated a journal task that they have 2 days until the task needs to be completed
- Notify the person allocated a Recommendation that the it has been 2 days since the due date
- Notify the person allocated to review a Risk Control that the review is coming up in 5 days time



***Example:** Rules for **Time Based Alerts** on **Incidents**, **Feedback** and any other Registers that uses the concept of Posted and Unposted items.*



***Example:** Rules for **Time Based Alerts** on **Risks**, **Quality Activities** and any other Registers that do not use the concept of Posting.*

1. **Type of alert:** Select the Register the alert relates to i.e. Incidents, Feedback, Risk, Activity - this will depend on your permissions and the Registers that are activated in your RiskMan
2. **Alert Method:** Process Periodically
3. **Processing Period:** Select how often you wish notifications/items/activities to be checked to see if they meet the conditions of the alert and trigger the alert accordingly. If the cycle is under a day the alert can only be triggered once – this is to prevent excessive emails being sent.
4. **Activate For:** This field will only show if the selected Register in the **Alert Type** field uses the concept of Posted and Unposted Notifications e.g. Incidents & Feedback. **Activate For** asks you - “Is the alert activated on posted or unposted notifications?”
    - If **Unposted** is selected it means that the alert will trigger if the conditions are met on the notification
    - If **Posted** is selected it means the alert will only trigger if the notification is posted ie. A master version has been created. Users selected to be notified of the alert need to at least have the permission to **view posted <register> items** in their respective Register User Profile
5. **Activate Once per Item:** If the **Processing Period = 1 or more days**, then this field will become available. Check this option if you only want the alert to trigger when the conditions are initially met or

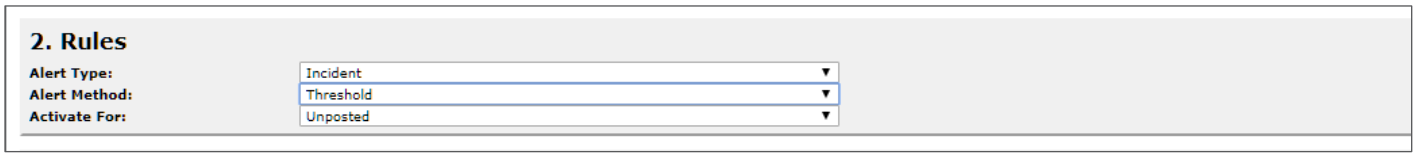
leave unchecked if you want the alert to trigger every time the conditions are met until the conditions of the notification change

Step ❷: Rules – Threshold Alerts

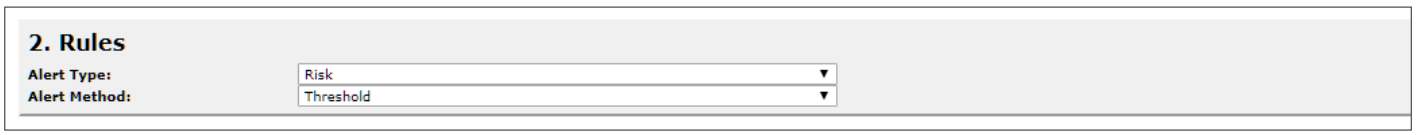
The following information describes the rules when creating Threshold Alerts i.e. **Alert Method = Threshold Alerts.** Examples for these types of alerts include:

- If the number of medication related incidents that resulted in an adverse drug reaction has occurred more than twice in a month, alert the owner of the Medication related Risk
- If there are more than 3 staff incidents resulting in an injury in a particular location in a month, alert the OHS Manager
- If there are more than 2 complaints raised in a particular department in a week, alert the manager of this department

If the number of non-compliant items in an Environmental Audit exceeds a specific total, alert the OHS Manager



Example: *Rules for Threshold Alerts on Incidents, Feedback and any other Registers that use the concept of Posted and Unposted items*



Example: *Rules for Threshold Alerts on Risks, Quality Activities and any other Registers that do not use the concept of Posting*

1. **Type of alert:** Select the Register the alert relates to i.e. Incidents, Feedback, Risk, Activity - this will depend on your permissions and the Registers that are activated in your RiskMan
2. **Alert Method:** Threshold Alert
3. **Activate For:** This field will only show if the selected Register in the **Alert Type** field uses the concept of Posted and Unposted Notifications e.g. Incidents & Feedback. **Activate For** asks you - “Is the alert activated on posted or unposted notifications?”
    - If **Unposted** is selected it means that the alert will trigger if the conditions are met on the unposted version of the notification.
    - If **Posted** is selected it means the alert will only trigger if the notification is posted i.e. A master version has been created. Users selected to be notified of the alert need to at least have the permission to **view posted <register> items** in their respective Register User Profile

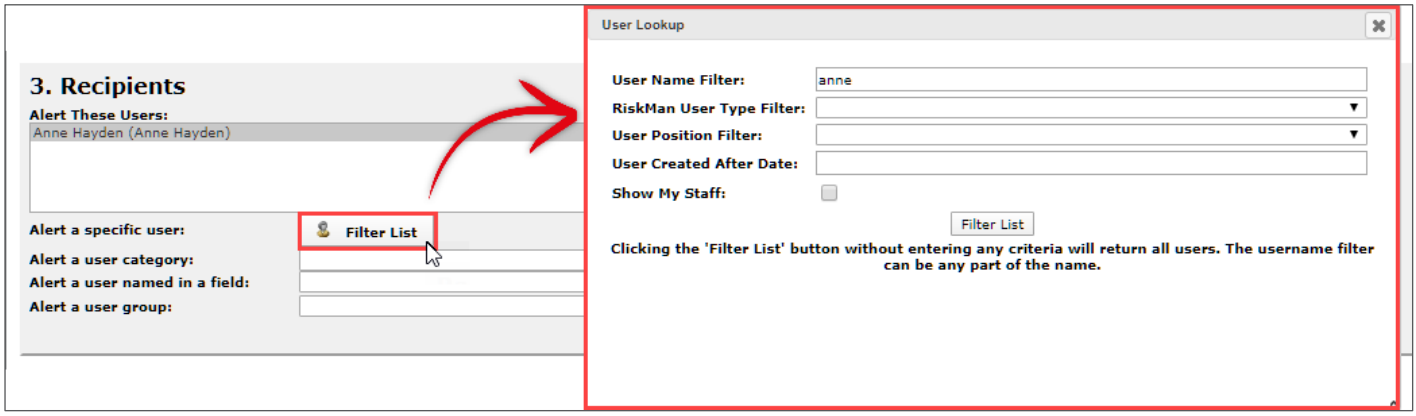
Step ❸: Recipients

The recipients section specifies who is to be alerted. The "**Who**" can be one or more of the following:

- Specific users
- Users who belong to a specific User Category
- Users named in a field
- Alert a user group

Note: *The selected user/s need to be registered in RiskMan*

1. **Alert a Specific User:** If you wish your alert to be allocated to a specific user or users



   - Click on the **Filter List** button
   - In the Filter pop-up window enter the User's first or last name in the **User Name Filter**. Press **Filter List.** The list of users matching your filter criteria will appear in the **Alert These Users** list
   - Highlight the user or users who are to be alerted. *(Hold your **CTRL** key if you wish to select more than one user).* Any users **not selected** in the **Alert These Users** list will **not be saved** with the Alert
   - Repeat the above steps if you wish to add more users to the Alert

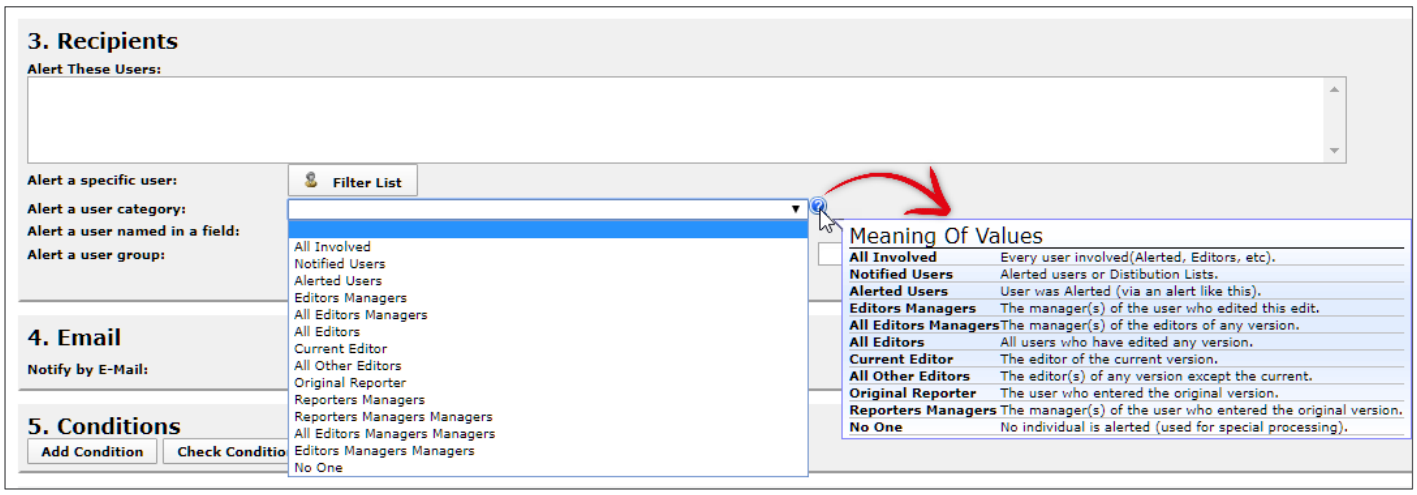
2. **Alert a User Category:** This option is used if you wish to notify a number of users based on a generic category rather than specific users; for example:

   Reporter's Managers *(the manager/s of the person who reported the notification/item/activity)*;

   Original Reporter *(the person who entered the notification/item/activity)*;

   All Involved *(all users involved in the notification/item/ activity i.e. users listed in the Review History)*

Select a category from the "**Alert a user category"** list based on the descriptions accessed by clicking on the **Help** icon



3. **Alert a user named in a field:** The only fields that you can select from this list are fields where a user can be selected (via a list or a filter) in a Notification/Item/ Activity; for example:

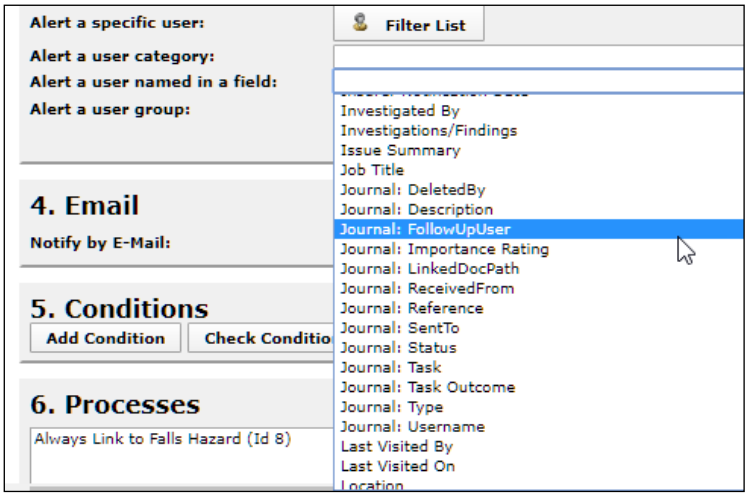
Journal: Followupuser: The user who has been allocated a task from the journals

Journal: Username: The user who has created a journal

Responsibility for Rec #: The person responsible for a recommendation

RRControls: Next Review By: The person allocated to a Risk Control

Accountable Executive: The person who has been nominated as the Owner of a Risk

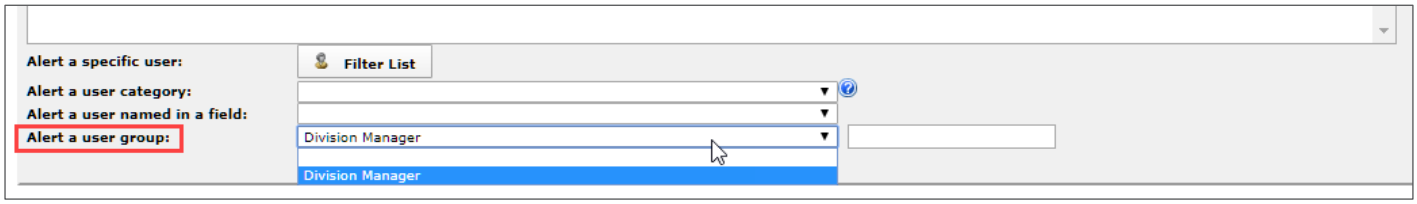


Select an appropriate field from the **"Alert a user named in a Field"** list and it will appear in the **Alert. These Users list** – ensure the field is highlighted in the list.

4. **Alert a user group:**

A user group is designed to provide email alerts in a simplified manner. A user group is similar to a Contact Group in MS Outlook. This eliminates the need to enter users individually.

A user group can be configured based on users, locations, roles etc. To have a user group configured, you will need to contact RiskMan.



Step ❹: Email

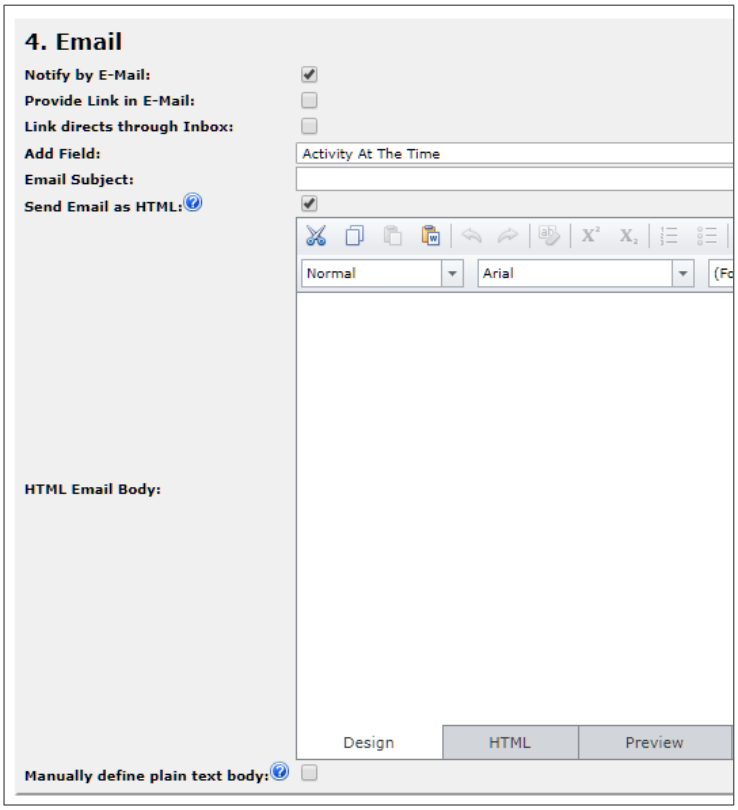
The **Email** section specifies if the alerted users are to be notified by email when the alert is triggered.

If the Alert is **Examine When Saved**, it is **not necessary** to include an Email notification, if the recipient/s only want to be granted permission to notifications/items/activities and do not want an email notification

If the Alert is a **Process Periodically** or **Threshold Alert** then you will **need** to include an Email.

- Threshold Alerts **only** send emails and do not grant recipients permission to the notifications/items/ activities involved in the Alert.
- Process Periodically alerts are Reminders so it makes sense to include an email

If the user is to be notified by email, **BOTH** the **Email Subject** and **Email Body MUST** to be configured. When configuring the email, you will be able to select whether the email sent will be in HTML or plain text format. By default, the HTML format will be selected. HTML emails come with additional formatting such as font, font size, colour, hyperlinks to email addresses or web pages



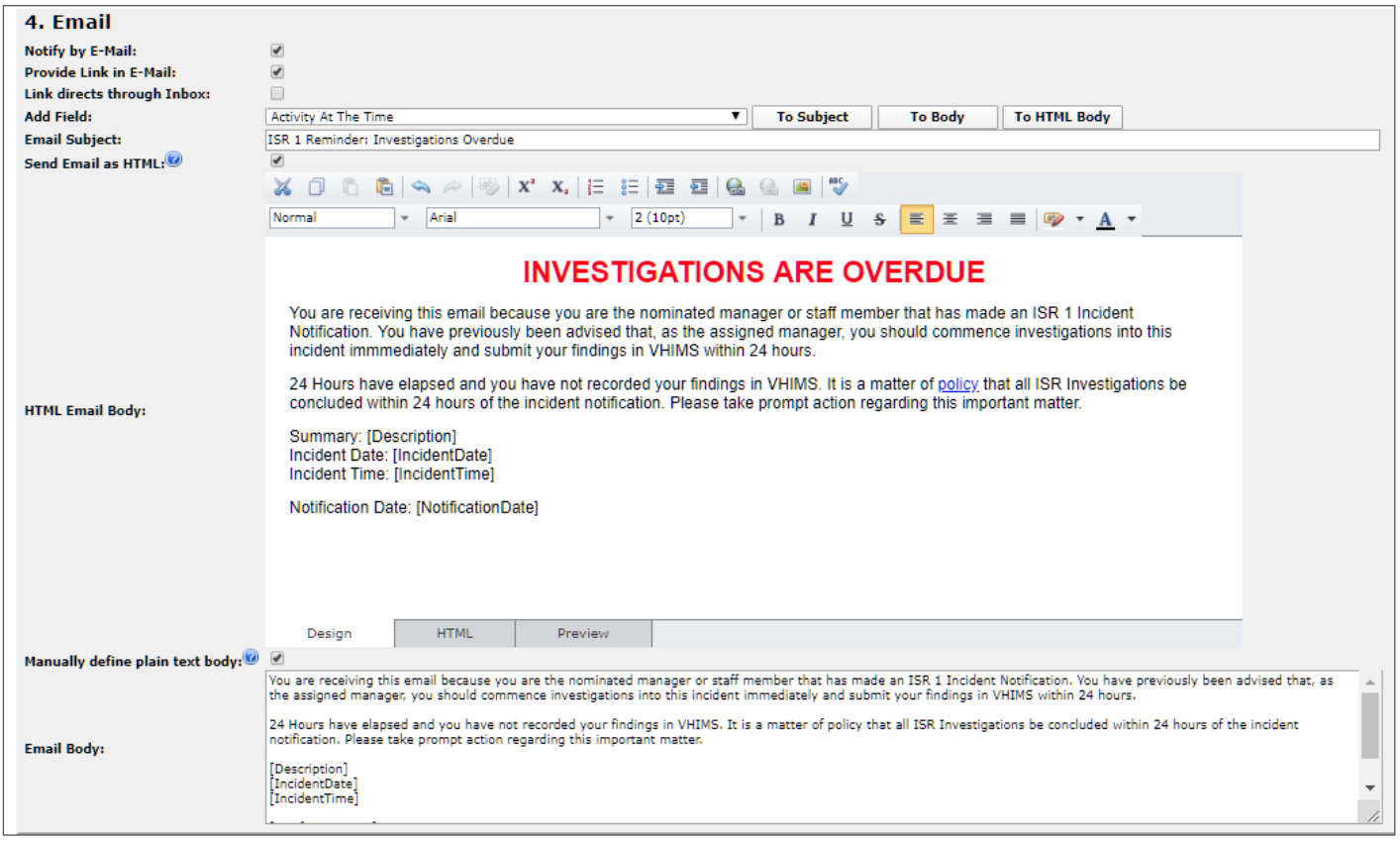
1. **Notify by E-Mail:** Check this field if the user is to be notified by email *(this will checked by default if the Alert Type = Threshold Alert)*
2. **Provide Link in E-Mail**: Check this option if you wish to provide a link to the notification/item/activity in the Email Notification
   - **Recommended** if the Alert Type = **Examine When Saved** or **Process Periodically**.
   - **Not required** if the **Alert Type = Threshold Alert** because the alert does not grant the user access to the Notification/Items/Activities referenced in the alert)
3. **Link Directs through Inbox: <u>ONLY</u>** check this option if the user has permission to the respective **Register Inbox** i.e. for Registers that use the concept of Unposted and Posted Notifications like Incidents & Feedback

   Not required if the **Alert Type = Threshold Alert** because the alert does not grant the user access to the Notification/Items/Activities referenced in the alert
4. **Add Field:** Provides a list of all the respective Notification/Item/Activity fields that are available to you to be included in the email subject or body

5. **Email Subject:** Enter a subject line for the email (this should be concise and informative). If you wish to populate data from a set of fields into the subject line
   - Select a field from the **Add Field** drop down list
   - Press the **To Subject** button
   - This will put the **[field name]** where your cursor is located in the subject line
   - Suggested Columns: Severity; Location; Reporter's Name; Risk Name; Activity Name

***Warning**: DO NOT include fields that may contain substantial text e.g. **Summary** or **Details** into the Subject line of an email as there is a character limit and if exceeded will cause problems with the email notifications*

6. **Send Email as HTML:** This will be selected by default. The HTML body will contain additional formatting. If the intended recipient cannot view HTML emails then the body of the email will display as plain text i.e. the formatting will not appear in the email
7. **HTML Email Body:** Enter a message using the format options available (see examples below and on the next page). Optionally if you wish to also create a plain text email, check mark the "Manually define plain text body" option (as in the example below)



If you wish to populate data from a set of fields into the body of the email

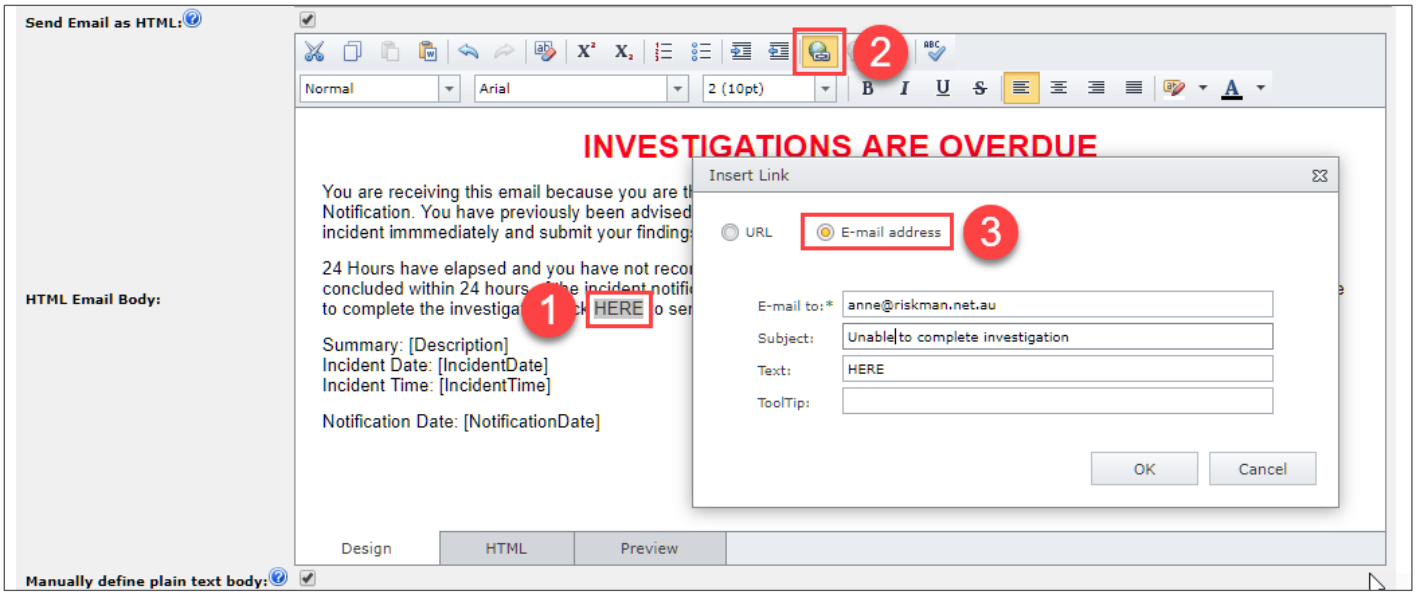
- Select a field from the **Add Field** drop down list
- Press the **To HTML Body** button
- This will put the **[field name]** where your cursor is located in the body of the email
- Suggested information may include:
  Incidents: Location; Incident Date; Summary; Reporter's Name; Severity; Incident ID
  Feedback: Location initiated; Summary; Reporter's Name; Feedback ID

Risk: Name of Risk; Category; Residual Risk Rating; Next Review Date; Risk Owner
Quality Activity: Type of Activity; Summary; Recommendation; Due Date; Activity ID

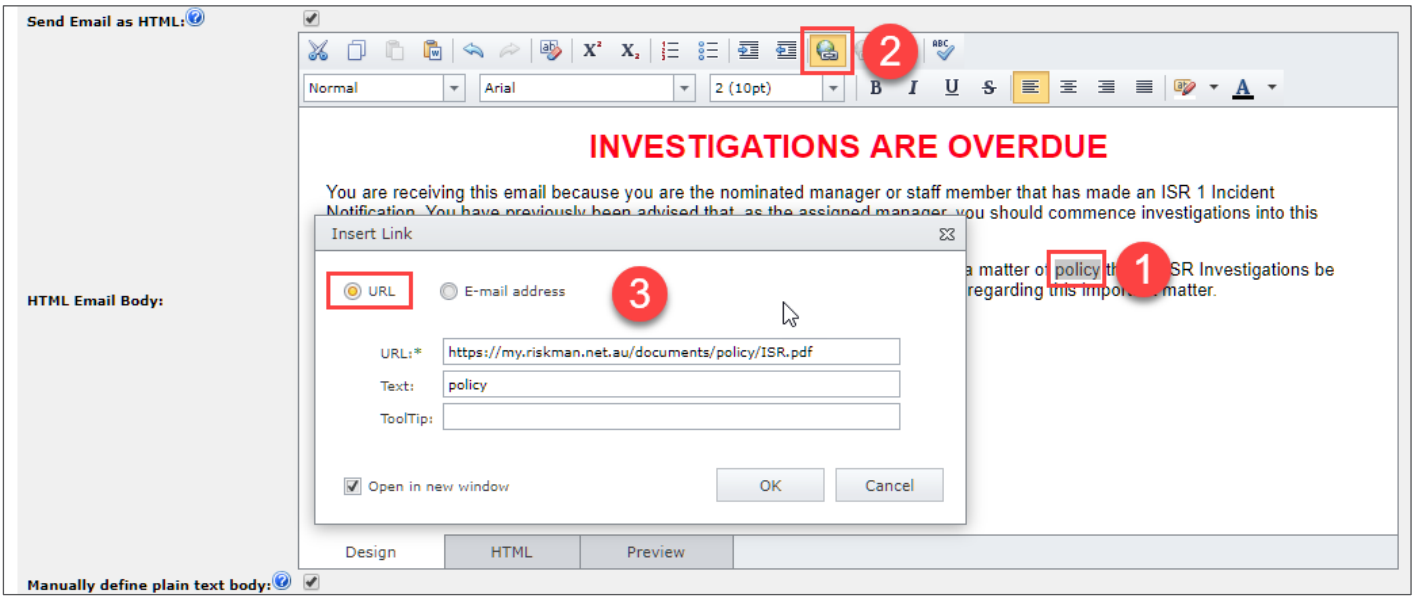
If you wish to insert a link into the email e.g. to a policy on your intranet or to an email address

Highlight the text in your email that will be changed to a **hyperlink** when the Alert email is sent

1. Press the **Insert Link** icon -
2. Fill in the details as required – the link can be an intranet or internet address or an email *(refer to example below)*.
3. Press **OK** to finish

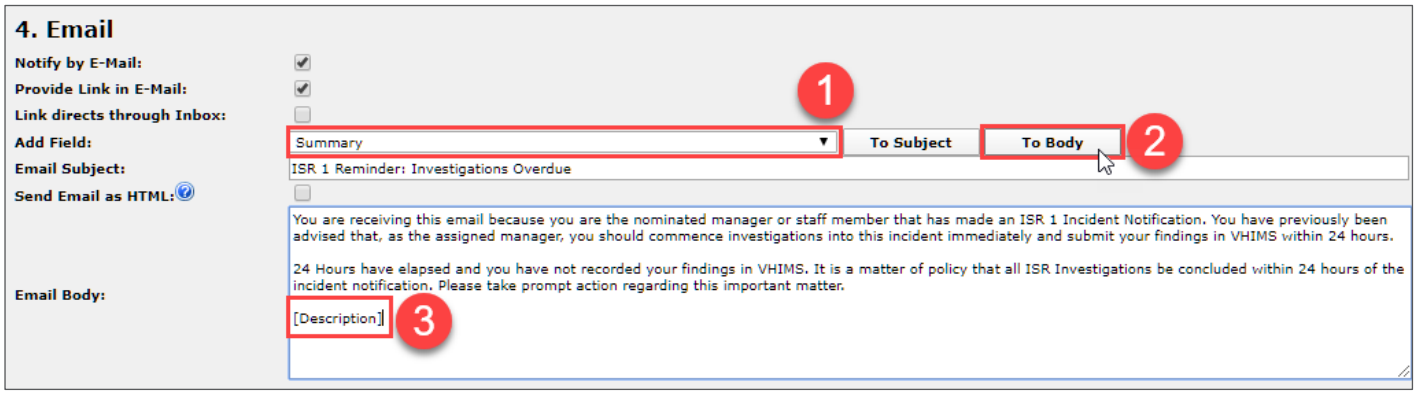


Example: *Using a link to an email address*



Example: *Using a link to a document on an intranet*

8. **Plain Text Email Body:** If you do not wish to use HTML emails then uncheck **'Send Email as HTML'** and only the plain text **Email Body** section will display



If you wish to populate data from a set of fields into the body of the email

❶ Select a field from the **Add Field** drop down list

❷ Press the **To Body** button

❸ This will put the **[field name]** where your cursor is located in the body of the email

Step ❺a: Threshold Condition

If the **Alert Method = Threshold Alert**, then an additional section will appear under the **Email** section. This section allows you to

- Specify the number of notifications/items/activities that when exceeded within the specified number of days, will enable RiskMan to trigger the email notification to the nominated recipients, based on the conditions of the Alert.
- Specify how many emails the nominated recipients would like to be sent in one day, if the threshold is met more than once in a day

1. Enter the **count** of notifications/items/activities (this is the threshold number)
2. Enter the **number of days** (the monitoring period)
3. Enter the **number of emails** the recipient would like to receive in one day if the specified threshold is exceeded

Step ❺: Conditions

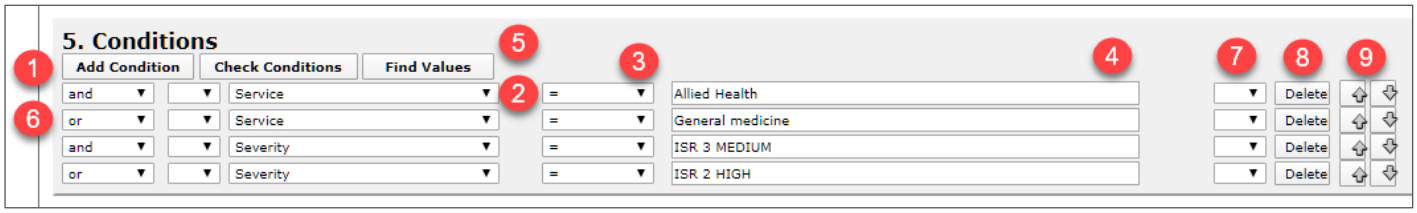
This section allows you to configure the conditions that will cause the alert to trigger based on specific information that has been entered into a Notification/Item/Activity

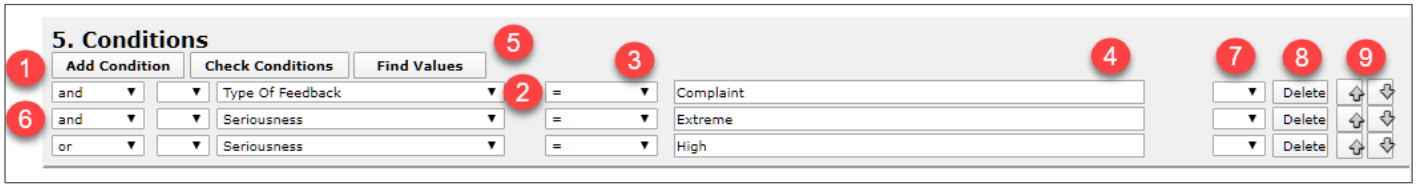
The functions available in the **Conditions** will be depend on whether the alert type is an "Examine When Saved", "Threshold Alert" or "Process Periodically"

Suggestion: *When setting up conditions for an alert it is often a good idea to open another session of RiskMan (by pressing **CTRL K** or **CTRL N** in your Internet Explorer) and opening up a New Register page e.g. New Incident, Feedback, Risk, Activity. In this way if you are unsure of the name of a field that you wish to use in the Alert, you will be able to see the name on the respective Entry Form.*

In most cases the name of the field on the Entry form will be the same as the name of the field in the Conditions list. In some cases, the names may be different e.g. A shortened version of the field name; if the field name is used more than once on the respective Entry form there may be a prefix indicating where on the Entry form the field is located e.g. Notify of Associated Risks might be associated with the Accountable Executive or Responsible Manager

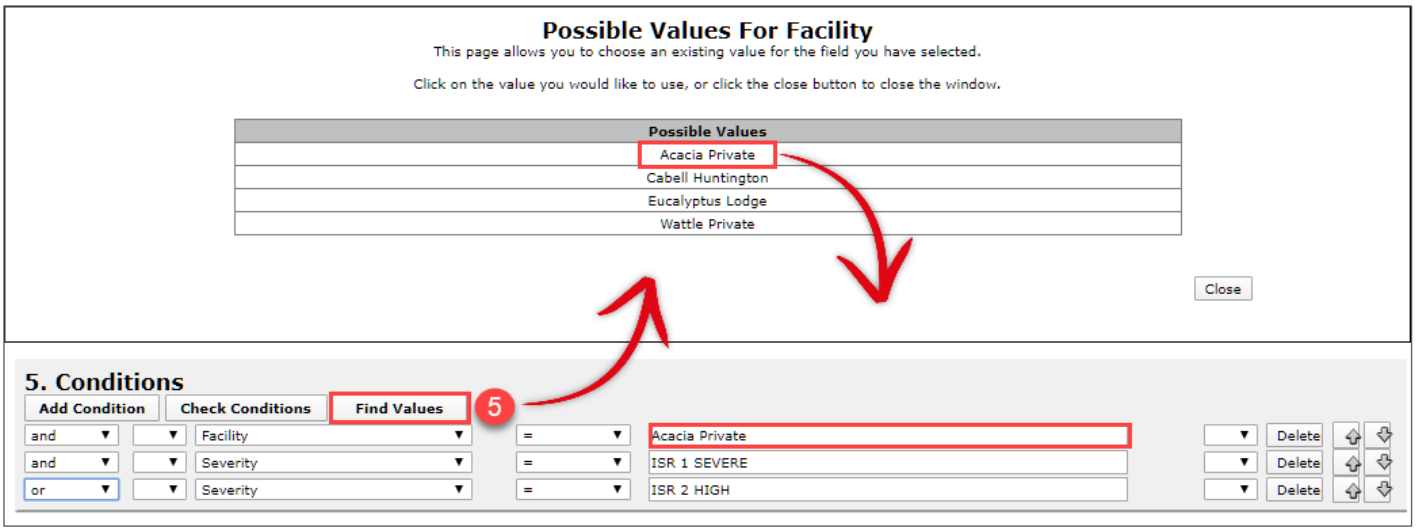
Conditions for Alert Type = Examine When Saved or Threshold Alerts



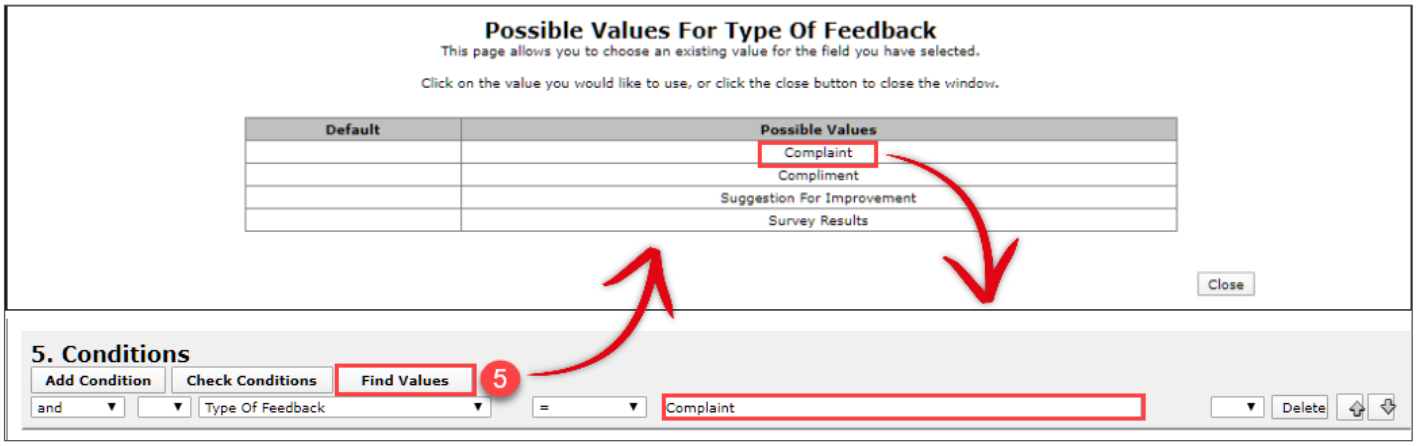


1. Press **Add Condition** ❶
2. Select a **field** from the drop down list ❷
3. Select a logical test ❸
   - **For List fields use** =, <> (not equals), Is Null (is empty), Is not null (is not empty), Like, Not Like
   - **For Date, Time or Numeric fields use** =, <>, >, >=, <, <=, Is Null, Is Not Null
   - **For Text fields use** Is Null, Is Not Null, Like, Not Like
4. Enter or select the criteria for the filter ❹
   - **Text fields**: Enter the text. The wildcard "%" can be used e.g. **Summary like %fall%** which means the word "fall" can appear anywhere in the "Summary" field
   - **Date fields**: Enter the date as **1 Jan 2012**
   - **Time fields**: Enter the time as **15:45** (24 hr clock format)
   - **Numeric fields**: Enter the number e.g. 4, 50
   - **List fields:** Press the Find Values ❺ button and select **ONE** value from the list (this ensures the correct criterion is selected).

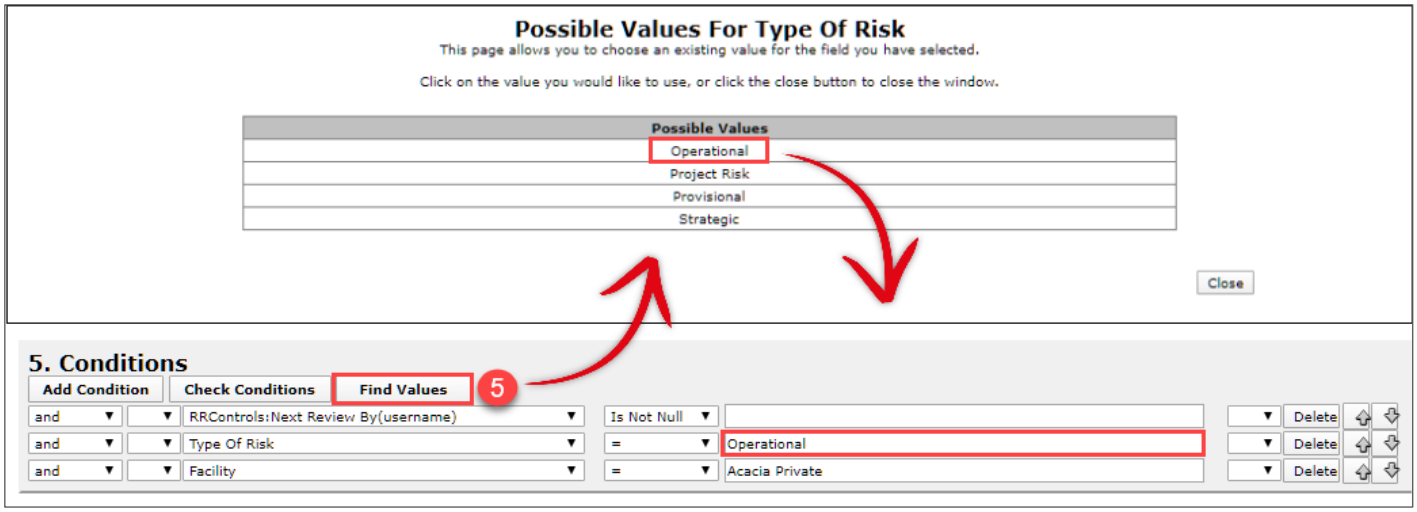
Example: *Incident Alert*



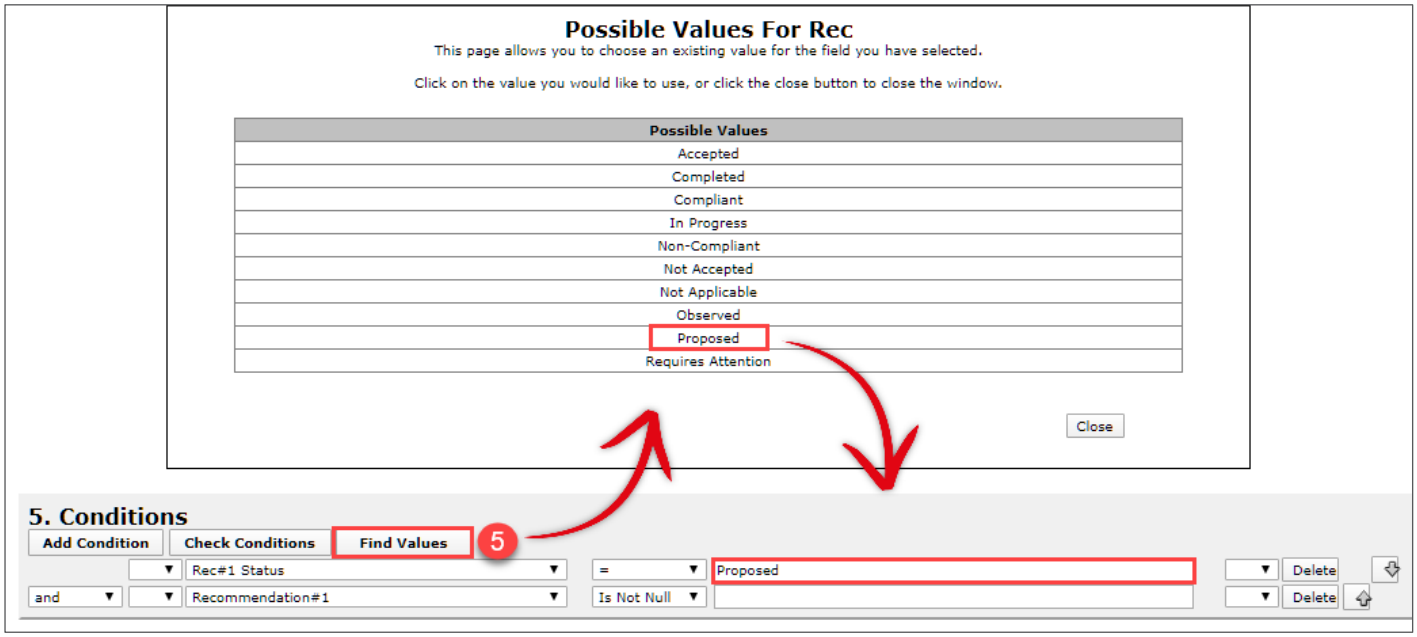
Example: *Feedback Alert*



Example: *Risk Alert*

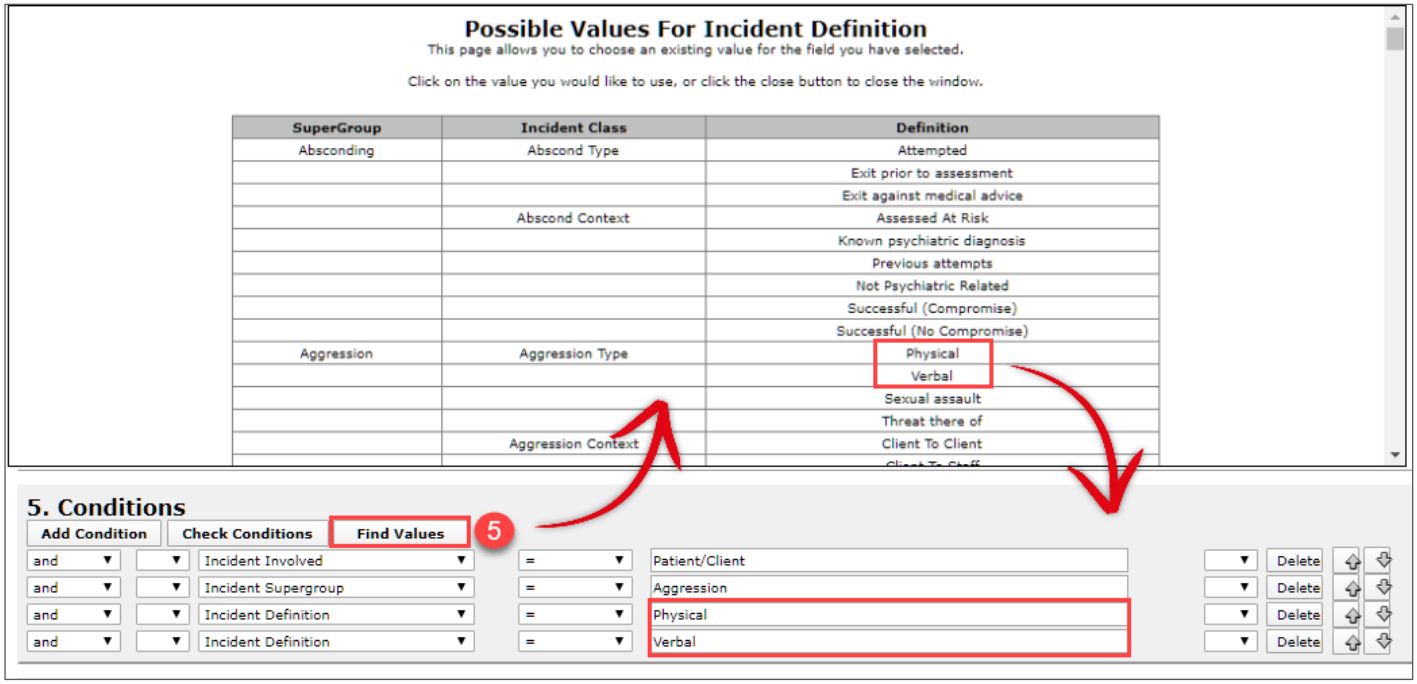


Example: *Quality Alert*



- **INCIDENTS: Classifications** - If the field is based on the Incident RiskCat, there are 3 fields that you can base your alert on: Incident Supergroup (1st Level grouping); Incident Class (2nd Level grouping): Incident Definition (3rd level grouping)

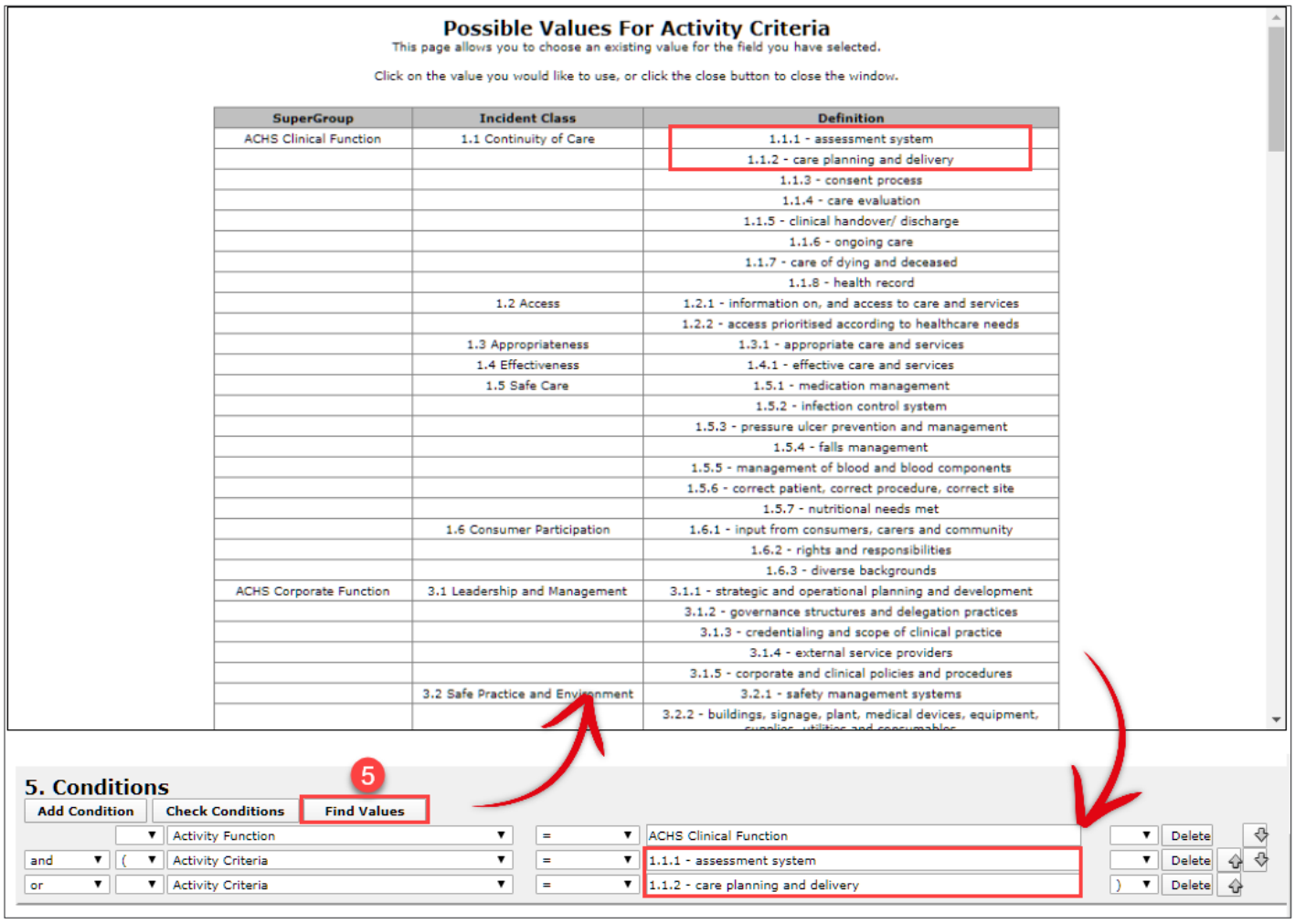
  Press the **Find Values** ❺ button and select **ONE** value from the list.



Example: *Incident Alert based on the Incident Supergroup and Incident Definitions from RiskCat*

- **QUALITY ACTIVITIES: Classifications** - If the field is based on the Quality Activity Classification, there are 3 fields that you can base your alert on: **Activity Function** (1st level grouping); **Activity Standard** (2nd Level grouping): **Activity Criteria** (3rd level grouping)

  Press the **Find Values** ❺ button and select **ONE** value from the list.

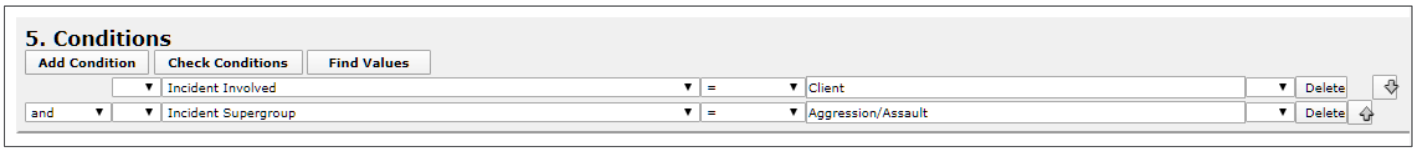


Example: *Quality Activity Alert based on the Activity Function and Activity Criteria from the Classifications*

5. If another condition is required e.g. The filter is based on more than one value from the same field or from different fields, press **Add Condition** ❶

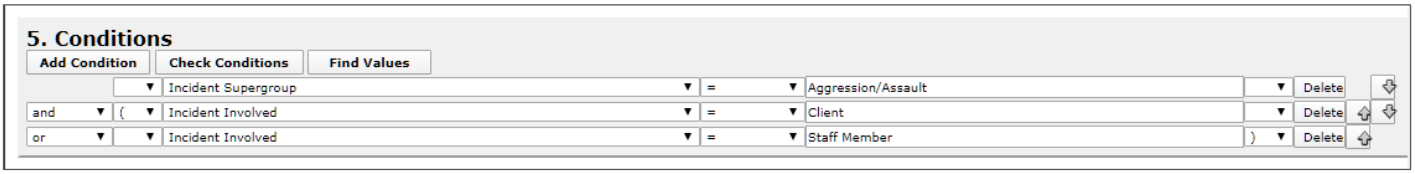
6. If 2 or more conditions are added to your filter, select **"And", "Or", "But Not"** ❻ at the beginning of the Condition *(not required for the first condition)*

"And": When more than one condition must be met



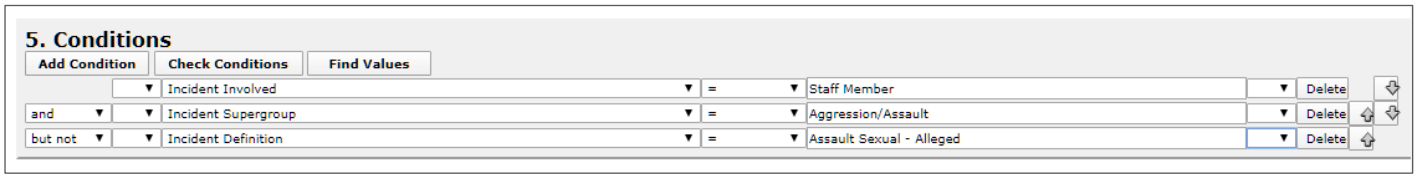
Example: *Only trigger the alert if the incident involves a Client and Aggression/Assault*

"Or": When at least one condition must be met



Example: *Only trigger the alert if the incident involves a Patient or a Resident and Aggression/Assault*

"But Not": To exclude a classification from RiskCat

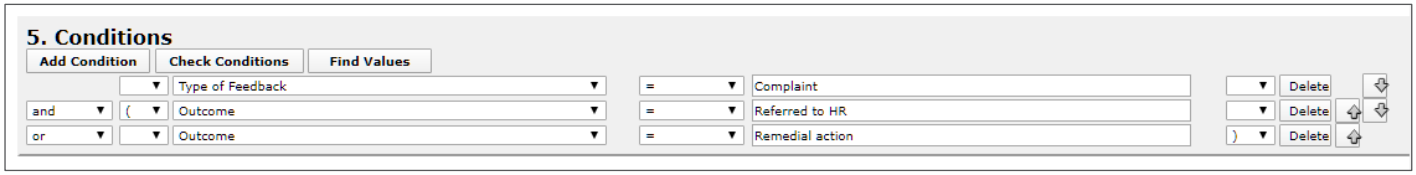


Example: *Only trigger the alert if the incident involves a Staff Mamber and Aggression/Assault but not if the aggression is of a Assault Sexual nature*

7. If required add **Brackets** ❼ around the conditions. Brackets may be required around some conditions to ensure the alert is triggered correctly

   A common scenario where you would need to use brackets is when:

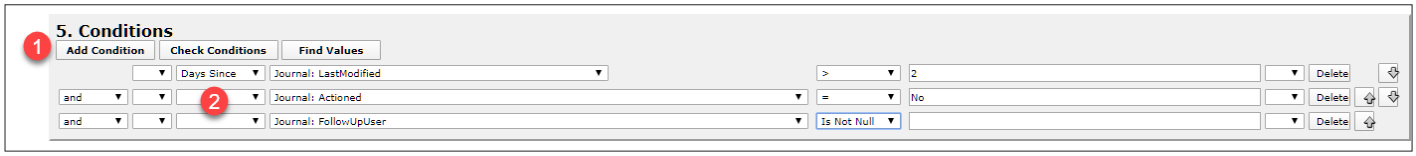
   - You have more than one condition to test for, and
   - At least one of those conditions has more than one option that could satisfy it



Example: *In this example there are 2 distinct conditions -* ***Type of Feedback*** *and* ***Outcome****.* ***Outcome*** *has 2 options so we put the brackets around the* ***Outcome*** *conditions*

8. If you wish to delete a condition press the **Delete** ❽ button next to the condition. You may need to modify your **"Or", "And"** or **"But Not"** options and your **brackets**
9. If you wish to re-order your condition statements use the **Directional** ❾ buttons - **Up** ⇧ or **Down** ⇩ next to the respective condition. You may need to modify your **"Or", "And"** or **"But Not"** options and your **brackets**

Conditions for Alert Type = Process Periodically



1. Press **Add Condition** ❶
2. Select a **Date Comparison** ❷
   - **Days Until** – Used to set up a condition where you are alerting a user in advance of a date e.g. 2 days until your allocated action is due
   - **Days Since** – Used to set up a condition where you are reminding a user that a task hasn't been completed or is overdue e.g. it has been 2 days since the incident was entered and the investigations have not been completed

Note: *Refer to the* ***Conditions for Alert Type = Examine When Saved & Threshold Alerts*** *section on the previous pages for details on how to create the rest of the conditions of the alert*

Additional Register fields available for filtering

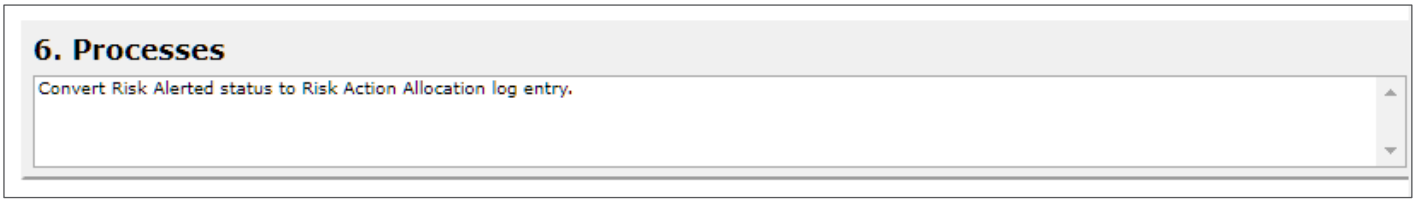
In addition to the fields that are available from your Register forms, there are some 'virtual' fields that can also be used. They include

- **Incident Day Name/Feedback Day Name:** Can be used in an alert to inform the recipient/s if the notification has been entered on a particular day of the week e.g. for weekend managers who need to know about incidents that occurred on Saturdays & Sundays starting and ending at a particular time
- **Is Grouped Incident/Feedback/Risk:** Can be used to only run an alert based on notifications/risks that are included in a group only notification
- **Is Master Incident/Feedback/Risk:** Used to run the Alert on the Master (i.e. source) report in a group only notification/risk
- **Has been posted:** Can be used to only run an alert based on registers that use the concept of Unposted and Posted Notifications e.g. Incidents & Feedback to inform the recipient/s that the notification has now been posted
- **Is Initial Incident/Feedback/Risk:** Can be used to only run an Alert on the first notification/risk (original report), or to ignore the first report and only run the Alert over subsequent edits
- **Journal Has Been Modified:** Can be used in an alert to inform the Recipient/s whether anything has changed in a Register Journal entry
- **Status:** Checks whether the notification/activity/item is posted/not posted/new/new edit/deleted
- **Sequence:** When creating an alert based on **incidents**, this field represents the number of times the posted version of the incident has been posted. For example, if Sequence = 1 then you are wanting to alert on the first time the incident is posted
- **Sequence (Posted Only):** When creating an alert based on **feedback**, this field represents the number of times the posted version of the feedback notification has been posted. For example, if Sequence = 1 then you are wanting to alert on the first time the feedback is posted
- **Sequence No:** When creating an alert based on Registers that use the concept of Unposted and Posted e.g. Incidents & Feedback, this field represents the version number of the unposted item. So the fourth version would have a Sequence No = 4, whereas the first version would have a Sequence No = 1

Step ❻: Processes

If the Alert you are creating requires a process to be included in the Alert, highlight the process in the **Processes** section. If no process is required then do not highlight.

The Process section does not appear on all Alerts that you create - only where it is relevant. The example below is only for Risk Alerts



Step ❼: Check Conditions

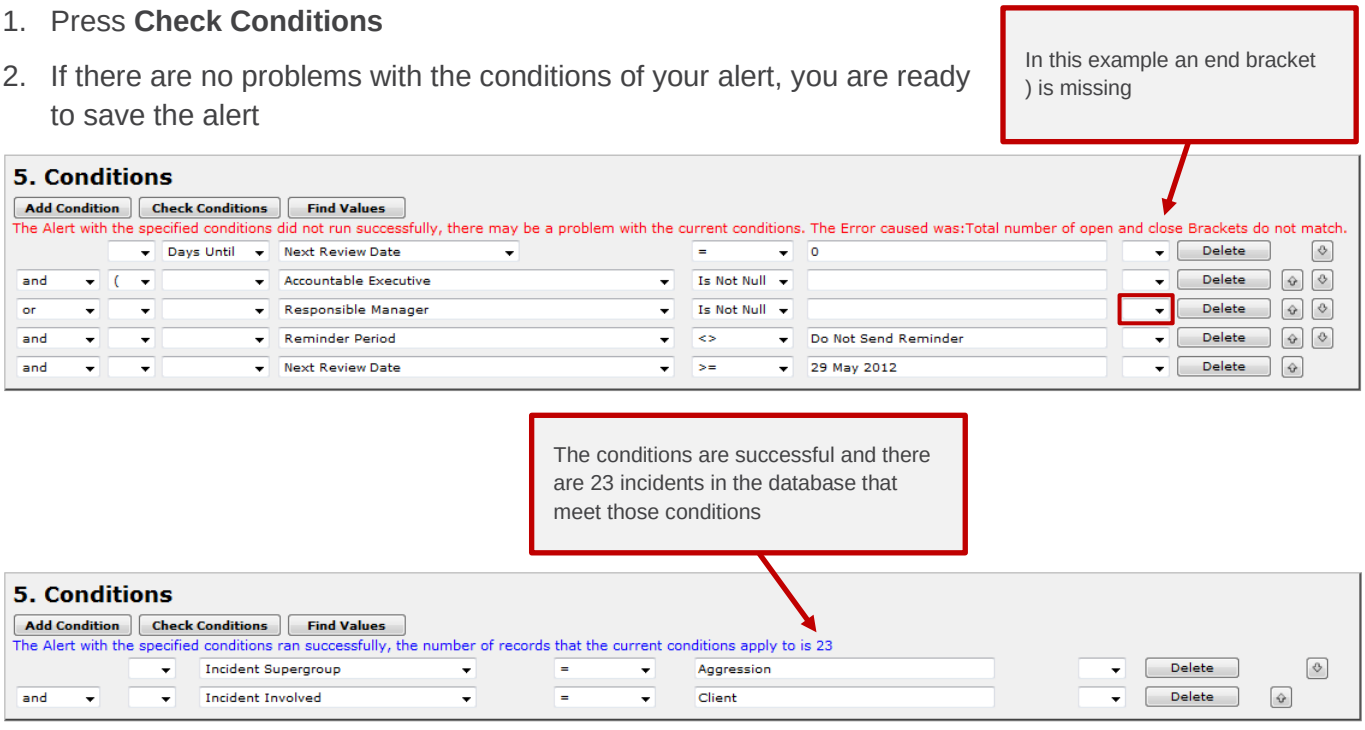
After you enter the conditions of your alert you should check these conditions. Checking the conditions will

- Inform you if you have missing brackets (if brackets are used in your conditions)
- Inform you of the number of notifications/items/ activities in the database that will meet the conditions of your alert

> ***Note:*** *When you check the conditions of your alert and the number of notifications/items/activities that the alert would trigger for exceeds or is less than what you expect, check your alert conditions again - it maybe the "**AND**", "**OR**" or "**BUT NOT**" selection or the brackets around your conditions. If you are unsure of your conditions, contact RiskMan Support -* https://hub.rldatix.com/SupportHUB/s/. *Please note you may need to request an account to access this service. If an account is needed, then please go to* HUB: Sign In (rldatix.com) *and click on Request an account at the foot of the login box*.

To check the conditions of your alert

1. Press **Check Conditions**
2. If there are no problems with the conditions of your alert, you are ready to save the alert



Step ❼: Save Alert

When you have completed your Alert, press **Save**

Alert is successful (no issues)

If your alert has no issues, a pop-up **"Alert Saved"** window will display informing you that ***"The Alert saved successfully"***

To return to your Alert Listing page

- Click on the **Return to Alert Selection** link

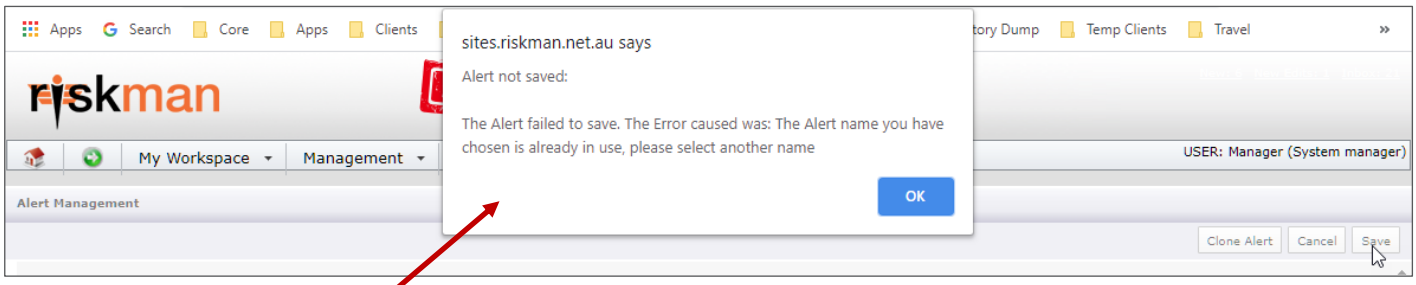
If you wish to keep your Alert opened

- Press the  icon on the **Alert Save** message

This is useful if you wish to **Clone** the Alert

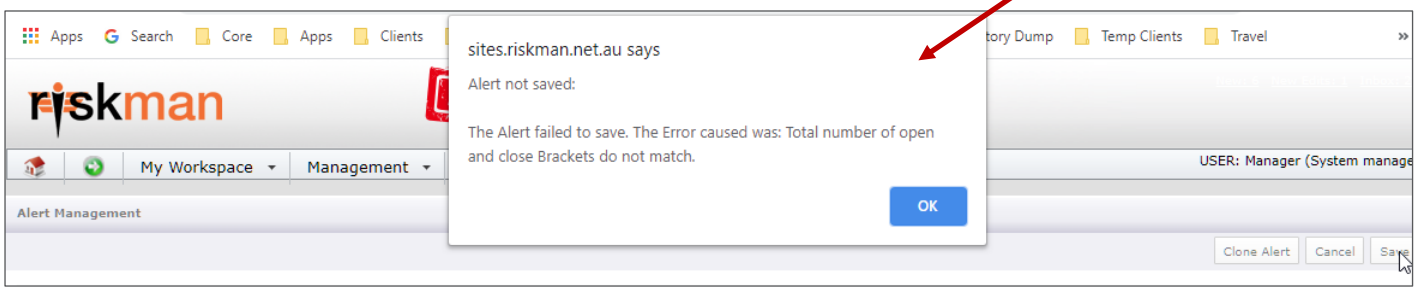
Alert is Unsuccessful (Issues)

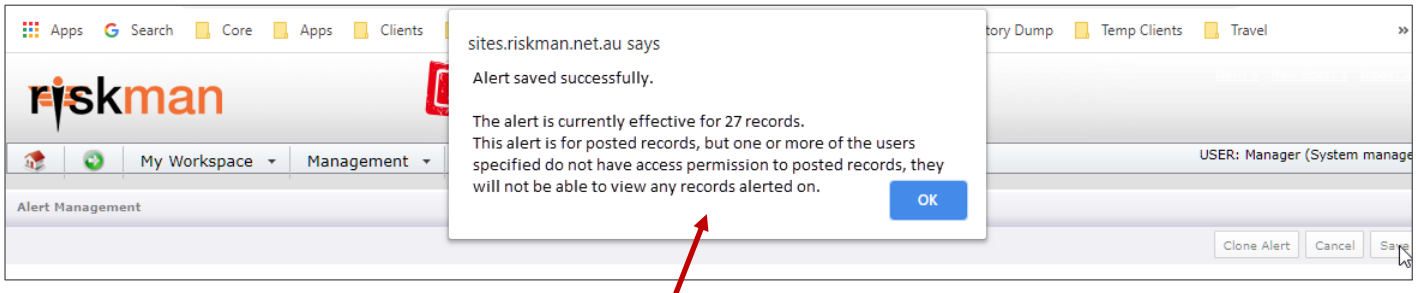
If there is an issue with the alert e.g. alert name has already been used; there is a missing bracket in the conditions; a user has no permission to the Posted records; a relevant message will display at the top of the alert. Make any necessary changes to the alert, and save the alert again



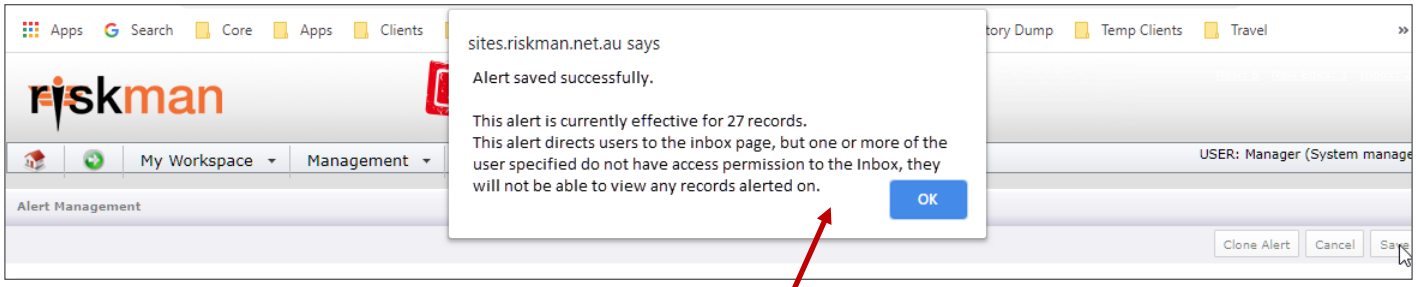
In this example you would need to change the **Name** of the alert as it has been used in another alert, before saving again

In this example you would need to check the **Conditions** of your alert to make sure you have the correct number of open and closed brackets





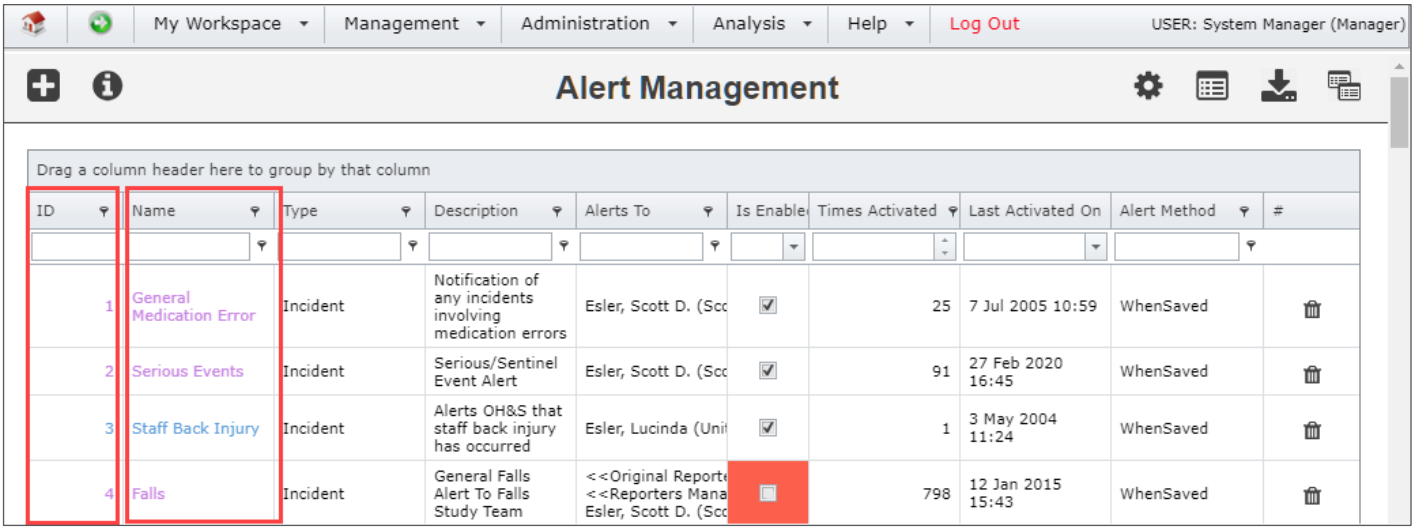
In this example one of the Recipients does not have access to **Posted Records** and yet the Alert is based on "Posted" Incidents. Either remove the recipient/s from the Alert and create a separate alert for these recipient/s, or update the recipient/s permissions so that they have access to at least view posted records



In this example one of the Recipients does not have access to the **Inbox** and yet this alert means that when the recipients click on the link in the email, the notification will open from the Inbox page. Either remove the recipient/s from the Alert and create a separate alert for these recipient/s, or update the recipient/s permissions so that they have access to the Incident Inbox

How do I modify an Alert?

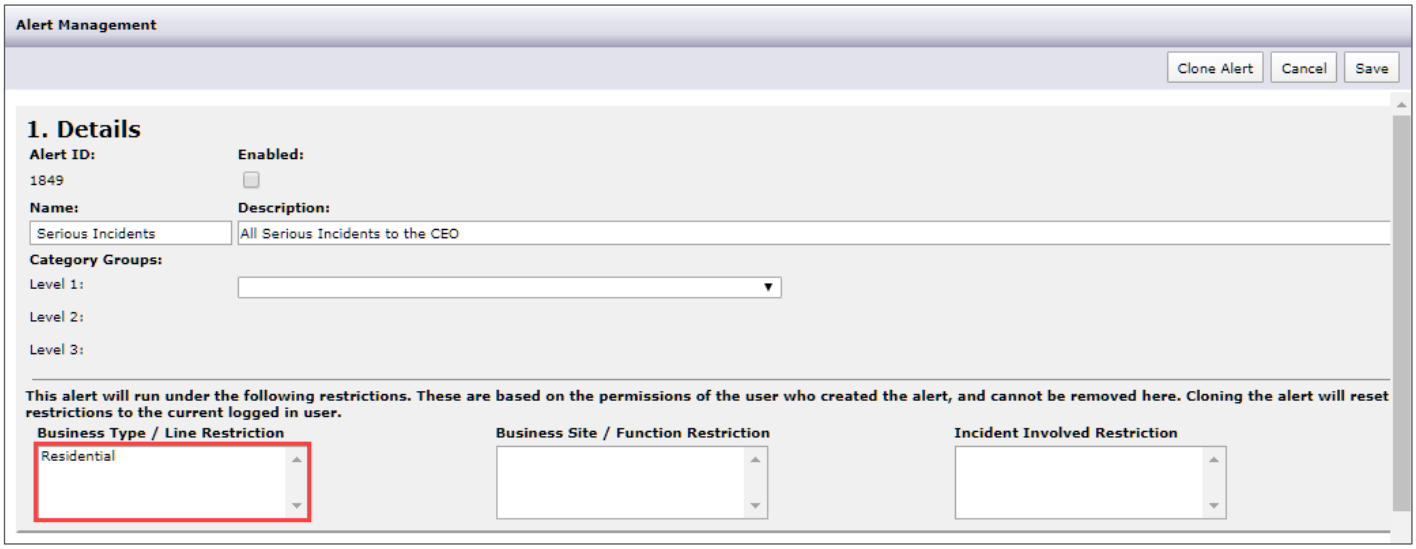
1. On the Alert Management listing page, either click on the **ID** or **Name** of the Alert and the alert will open



2. Modify the alert as required. For example: Change the alerted users; Modify the conditions; Modify the content of the email; Back date the alert for a new recipient who has not had access to the respective past notifications/items/activities
3. If modifying the conditions, press **Check Conditions** to ensure the correct number of brackets (if used) are around the conditions, and to also check how many notifications/items/activities meet the conditions of the alert. If the number of notifications/items/activities is less than or exceeds your expectations you may need to check the conditions have been set up properly
4. Once your alert is modified press **Save**

An alert has been created by a user with Restrictions

If an alert has been created by a user with Incident Involved (only in Incident Alerts), Site and/or Location restrictions, then at the top of the Alert in the Details section, these restrictions will display *(refer to example below)*



Example: *The alert will only trigger for incidents where* ***Site = Residential*** *because this alert was created by a user with this Site restriction.*

If you open an alert with a restriction, the restriction will remain if you modify the alert. If you wish to create a similar alert with the same restrictions as you have in your user profile (this might be no restrictions), **clone** the alert, provide a new name and modify as required

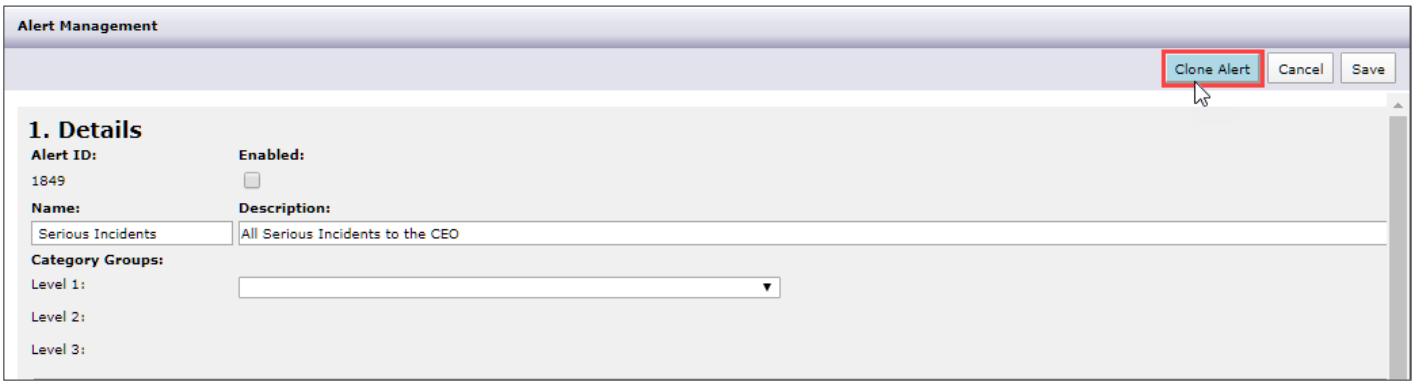
Can I make a copy of an Alert?

Cloning is useful if you have multiple Services/Sites/ Departments and you wish to create a similar alert and you only want to change the Service/Site/Department condition

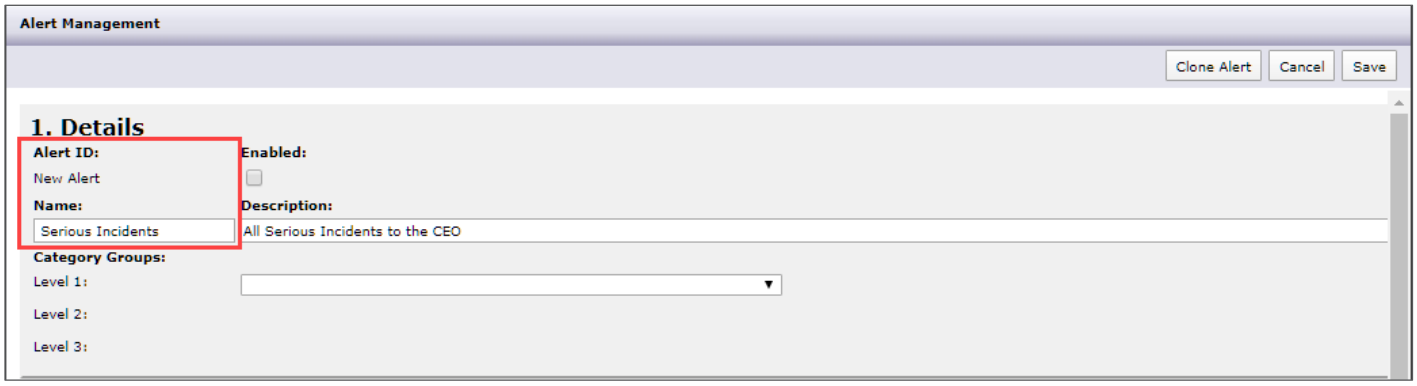
If the alert you are cloning was created by a user who has Site, Location or Incident Involved Restrictions, these will be removed and your restrictions (if you have restrictions in your User Profile) will be applied to the cloned alert

To clone an alert

1. On the Alert Management listing page, either click on the **ID** or **Name** of the Alert
2. In the opened alert, press the **Clone Alert** button



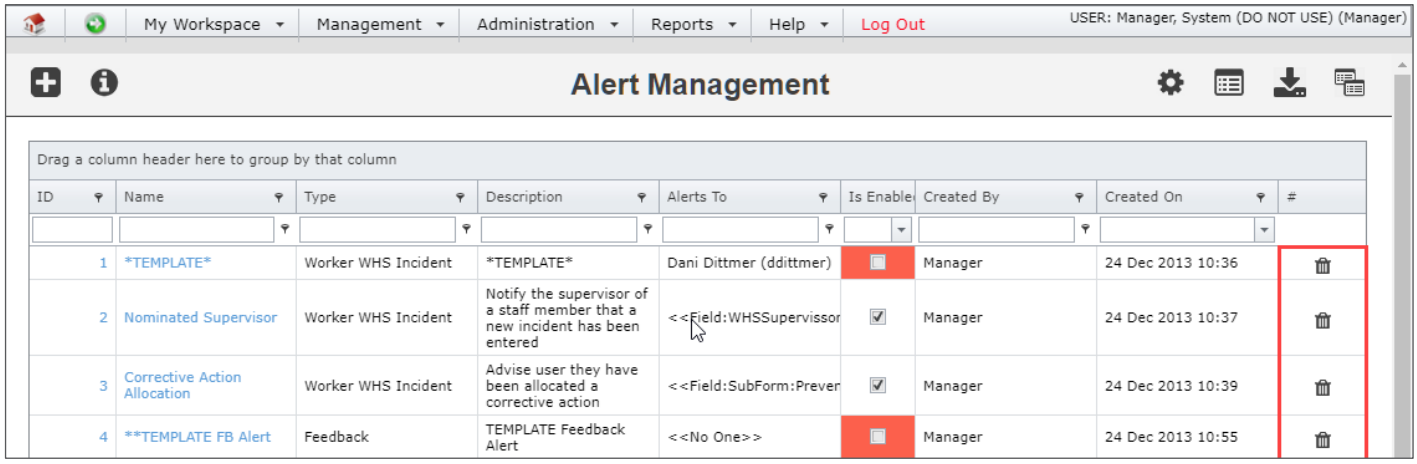
3. When the alert is cloned, the **Alert ID** will be cleared.
4. It will be necessary to provide a new **Name** for the alert



5. **Modify** the alert as required
6. Press **Check Changes** (to check your conditions)
7. **Save** the alert

How do I delete an Alert?

1. On the Alert Management listing page, click on the **Delete** button next to the respective Alert
2. A pop-up message will ask you to confirm the deletion



Workflow Scenarios

The following provides you with examples of the types of alerts you may wish to use within your RiskMan based on the Incident, Feedback, Risk and Quality Activity Registers

INITIAL INCIDENT NOTIFICATION: Alert To Executive

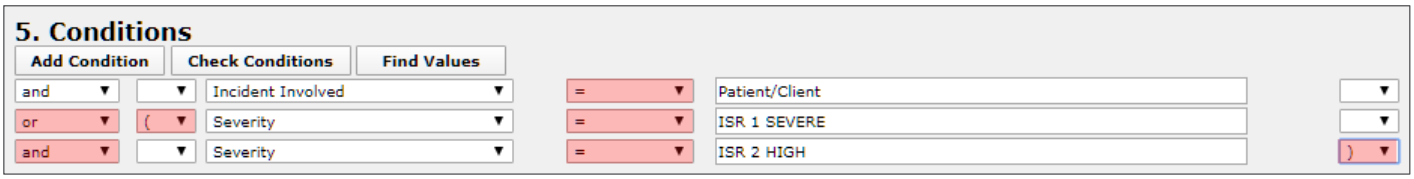
- Notify an Executive of serious clinical incidents
- Select specific user(s) by name
- Author a meaningful email message, with some details from the incident

  Suggestion: Include the Severity Level in the Email Subject to gain attention

- Activate for Unposted (runs as soon as the incident is submitted)

  Suggestion: In the email, highlight the fact that this is an initial notification, and that the investigations may not yet have commenced, so confirmation of severity level has not yet been made

  Suggestion: If confirmation of severity is required before notifying the Executive, run at Posted time
- Specify the required conditions to trigger the Alert



INITIAL INCIDENT NOTIFICATION: Alert To Reporter's Manager

- Tell a manager when one of their staff submits an incident
- Select the generic recipient "**Reporters Manager**"

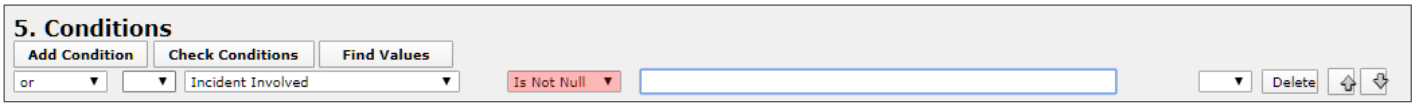
RiskMan determines who the appropriate manager is at the time the Alert triggers

- Author a meaningful email message, with some details from the incident

Suggestion: Include the Severity Rating in the Email Subject to allow the manager to quickly distinguish a serious notification from less serious ones

Suggestion: Create separate alerts for different Severity levels, and state your policy for follow-up. E.g. "Severity 1 Incidents must be investigated and documented within 48hrs"

- Activate for Unposted (runs as soon as the incident is submitted)
- Specify the required conditions to trigger the Alert



Triggers for all notifications, since all require an **Incident Involve** selection

FEEDBACK TO STAFF: Provide feedback to staff when a Complaint is resolved

- Advise all participants that a Complaint is Closed
- Select the generic recipient **"All Involved"**

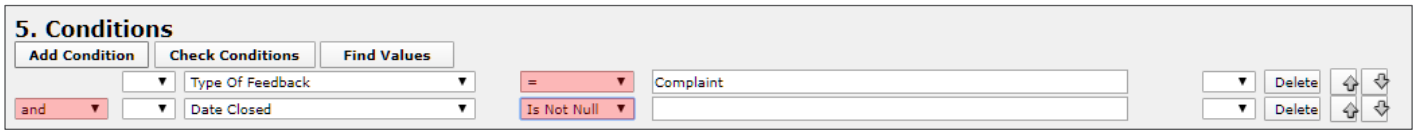
RiskMan sends to everyone who has edited the Complaint, or has been alerted or notified by a Distribution List

Alternative: Using "**Alerted Users**" may potentially exclude the initial reporter

- Author a meaningful email message, with some details from the complaint

Suggestion: Include the Resolutions, to inform all participating staff of resolution

- Activate for Posted (runs when posted/master version is Closed)
- Specify the required conditions to trigger the Alert



ASSIGNMENT EXAMPLE: Assign a Recommendation to a User from Incidents or a Quality Activity

- Let the staff/manager know that they have been assigned a recommendation
- Select "**Alert a user named in a field**" and locate the desired field in the Field List – in this case "**Responsibility For Rec #1**" *

Note: *You may have to create more than one of these alerts if your organisation allows more than one recommendation per Incident or Quality Activity. It is suggested you Clone the alert and change the recipient to the respective "Responsibility for Rec #" and the Conditions*

- Author a meaningful email message, with details of
- the user's responsibility, and the text of the recommendation
- If this alert is for an Incident Activate for Unposted (not applicable for Quality Activity)
- Specify the required conditions to trigger the Alert

** RMI must configure these fields in the Incident Register*

ASSIGNMENT EXAMPLE: Risk Control Allocation

Note: *This alert has been delivered with this version of RiskMan*

Advise a user that they have been assigned responsibility for a Control

- Select "**Alert a user named in a field**" and locate the desired field in the Field List – in this case "**RRControl: Control Next Review By**"
- Author a meaningful email message, with details of the Risk, description of the Control, the user's responsibility, and the next review date of that Control
- Specify the required conditions to trigger the Alert

	RRControls: NextReviewBy	**Is Not Null**

TIME BASED REMINDER: Risk Control Review Overdue

Note: *This alert has been delivered with this version of RiskMan*

Advise a user assigned to a Control that the review/assessment of that Control is overdue by 1 day

- Select "**Alert a user named in a field**" and locate the desired field in the Field List – in this case "**RRControl: Control Next Review By**"
- Author a meaningful email message, with details of the Risk and the Control, iterating that the Control review is now overdue and include the date it was supposed to be reviewed
- Specify the required conditions to trigger the Alert

	RRControls: NextReviewBy	**Is Not Null**
AND Days Since	**RRControls:NextReviewOn**	**> 1**

TIME-BASED REMINDER EXAMPLE: Remind an assigned user of a pending date

Advise a user assigned to a Recommendation in an Incident or a Quality Activity, that their completion notes are due in 3 days time

- Select **"Alert a user named in a field"** and locate the desired field in the Field List – in this case **"Responsibility For Rec#1" ***
- Author a meaningful email message, with details of the users responsibility to provide Completion Notes on the Recommendation in 3 days time
- If this alert is for an Incident Activate for Unposted (not applicable for Quality Activity)
- Specify the required conditions to trigger the Alert

	Rec#1 Status		**= Accepted**
AND	**Recommendation#1**		**Is Not Null**
AND	**Rec#1 Completed On**		**Is Null**
AND	**Rec#1 Outcome**		**Is Null**
AND	**Days Until**	**Rec#1 Due Date**	**< 4**

- ** RMI must configure these fields in the Incident Register*

TIME-BASED REMINDER EXAMPLE: Remind a Manager that investigations are overdue

- Advise a manager that investigations on an incident have not been recorded for a Serious event within 48 hours
- Select the generic recipient **"Reporters Manager"**
- **Suggestion:** Also include the Risk Managers specific user name
- Author a meaningful email message, reiterating the policy for investigations
- Run periodically (*at least once per day*) for unposted incidents
- Specify the required conditions to trigger the Alert

	Severity	**= ISR 1 Severe**
AND	**Investigation/Findings**	**Is Null**
AND	**Days Since Notification Date**	**> 2**