

- Alert Examples Supplement -

FOR RISKMAN VERSION 2509

Last reviewed October 2025

CONTENTS

Introduction.....	4
Notification Alerts.....	6
Notify the WHS manager by email when an OHS injury occurs	7
Notify falls coordinator of a new resident fall.....	10
Notify a user’s nominated line manager when they enter a new incident (uses Manager/Staff Relationships).....	12
Notify a Department Manager of a new incident lodged in their department (uses Org Structure list).....	13
Notify a unit manager that a new incident has been lodged for their unit (uses Org Structure Register).....	14
Notify a user when they are listed as a the accountable executive for a new risk.....	18
Create an exception which doesn’t sent workplace harassment incidents on to a user’s line manager; instead sends them to a certain HR user	21
Notify a user who created a journal task that it has been marked as complete	24
Notify the CEO of all the serious patient incidents that happened in the previous 7 days via a digest alert.....	26
Acknowledgement Alerts	34
When a user submits an incident, send them an acknowledgement email to confirm receipt of the record, and inform them what they can do next	34
When an incident is marked as closed, send an acknowledgement email to the original reporter, thanking them for submitting the incident and confirming what has been done about it	37
Reminder Alerts	39
Remind the responsible line manager that the investigations for an incident have not yet commenced, and the incident has now been in the system for more than 7 days. Add an escalation alert if nothing is still done 21 days later.	39
Remind a user that a journal task assigned to them is now overdue, and has not been actioned	44
Remind a user that an action assigned to them for a risk is overdue	46
Remind the key users that the anticipated completion date for a quality activity is 14 days away, and the status of the activity is currently not set to ‘completed’	47
Restriction Alerts.....	49

Alert Examples Supplement

Allow a user to see only records of a certain type in a register.....	49
Threshold Alerts.....	51
If there are more than 4 manual handling incidents in a 21 day period at a given facility, notify a particular user.....	53
If resident #7654321 has 3 or more falls in a 14 day period, notify the facility manager	54

INTRODUCTION

This document aims to provide examples of the various types of alerts that can be configured in RiskMan in order to orchestrate the workflows and processes required by your organisation.

When reviewing the examples of alerts in this document, please keep the following points in mind:

- It is intended that this document is used in conjunction with the **Alerts Management Guide**. This document provides examples of alert setup and configuration, whereas the Alerts Management Guide explains the actual functionality in-depth.
- The alert examples provided in this document were created in various different system configurations. Every RiskMan client configures RiskMan differently, so while some of the fields, registers, or functionality shown in the examples may not match your own system, what is more important is understanding the concepts behind the functionality. You can then transplant the examples into your own system, being sure to make adjustments to fit your own datasets, system functionality, etc.
- Most of the examples in this document are centred on the **Incident Register**. This is because the Incident Register is far and away the most commonly used register by RiskMan clients. Again, the concepts that are used can be applied to basically any other register in RiskMan.
- For each example alert provided, we quite deliberately do not exhaustively show every single setting or piece of configuration. Doing so would likely make it more difficult to read, and many settings are consistent or are up to you to decide. For example, most alert examples do not show how an email might be configured, unless the email itself was particularly unique to the alert example in question.
- This document will be amended as time goes by to include further examples of different types of alerts, including those which serve to demonstrate new alert-related functionality which may be added to the system in future releases of the software.
- Finally, remember that alerts are the most important part of your system. They control how your system behaves, and primarily grant users permission to see appropriate records.
 - They can be tricky, or sometimes difficult. RiskMan International wants to ensure when you are setting up alerts that you “*measure twice and cut once*”. With that in mind, please do not hesitate to contact RiskMan Support if you have any questions about setting up an alert, or if you would like us to double-check the setup of an alert you have created before you switch it on.

You can contact RiskMan Support via the following:

- By phone: Call the helpdesk directly on **+61 3 9686 0009**
- By email: Send your queries, along with other helpful materials to <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.

NOTIFICATION ALERTS

Common settings

Notification alerts will use the following settings in all examples, unless there is cause for an exception, which will be explained on a per-example basis.

Rules > Alert Method

The Alert Method will always be *Check each item when it is saved.*

The other 2 alert methods are specifically for

- Reminder alerts, and
- Threshold alerts

Alert Method	
<p>This setting determines when the items should be checked, and thus the alert triggered. Click the setting you want to use to select it.</p> <div style="background-color: #c00000; color: white; padding: 5px; text-align: center;"> Check each item when it is saved. </div>	<p>When the user enters a new item, or when an existing item is modified, the alert will run, and trigger if all the conditions are met. This is the most common method.</p>
<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> Scan all items periodically </div>	<p>The alert scans all items at the interval you specify (eg. Every 5 days), and triggers for each item that matches the conditions you specify. Usually used when you are creating a 'reminder' alert.</p>
<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> Trigger the alert once a threshold has been exceeded </div>	<p>The alert will monitor for the type of item that you specify, but will not trigger until the count of that type of item has exceeded your pre-determined threshold within a given timeframe.</p>

used

Rules > Settings

1 If the alert is for a register that utilises posting (incidents, feedback), you can stipulate here that the alert should not trigger unless the record has been posted. This can be useful in certain scenarios, such as ensuring a manager has confirmed the severity of an incident before notifying senior management of serious incidents

2 In the vast majority of cases, for a notification alert, *Trigger only the first time for each recipient* should be selected.

3 Your requirements determine which email option(s) to choose.

4 Seeing as these alerts are to *notify* somebody of something, we will always use the *Authorise* option

5 The backdate function does not need to be used for notification alerts. Refer to the Special Alert Functions section of this document for an example on when and how to use the backdate function.

Settings

Should this alert be triggered as soon as an item is entered, or should it only trigger once there is a posted version?

1 Trigger on the unposted record
 Wait until there is a posted version before triggering

Would you like this alert to trigger only the FIRST time it meets the conditions? Or would you like it to trigger EVERY time an item is saved and meets the conditions?

2 Trigger only the first time for each recipient
 Trigger every time an item is saved and meets the conditions, for each recipient
 Trigger only once per item (usually only for Process alerts)

Email Notifications

3 Send an email every time the conditions are satisfied
 Send a Digest email at the end of the nominated interval which summarises every item that satisfied the alert conditions.

What should this alert do regarding access permissions to the item for each recipient.

4 AUTHORISE access i
 DENY access
 REVOKE ALERTED access
 REVOKE ALL access
 Remove DENY access
 NONE

Backdate 5

Use the Backdate function to apply your alert to past records. For further information please refer to the Alerts Guide.
 Note: New alerts start from 'Now'. Backdate to pick up earlier records.
 Backdate to:

Schedule

You do not need to make any changes to the Schedule options for a notification alert. There are some scenarios where you might need to, and these are explained as variations for some alert examples.

Notify the WHS manager by email when an OHS injury occurs

Conditions

On the incident form, we have determined that the following fields and values would need to be present in order for it to be considered a staff injury:

<p><i>The subject affected is a...</i> must be Worker</p>	<p>Who Was Affected?</p> <p>The subject affected is a... *</p> <p>Type of worker *</p> <ul style="list-style-type: none"> Patient / Client Worker Relative / Visitor Non-Individual / Environment
<p><i>Level of harm sustained</i> must be either Injury/illness or Death</p>	<p>Level of harm sustained</p> <p>Primary nature of injury / illness</p> <ul style="list-style-type: none"> NO harm Injury/illness Death

Our resulting conditions look like this:

Where Subject affected is equal to Worker

And Level of harm sustained is one of 2 selected

+

Recipients

In this example, we have named a specific user. This might be the case in a single facility or other smaller scale implementation.

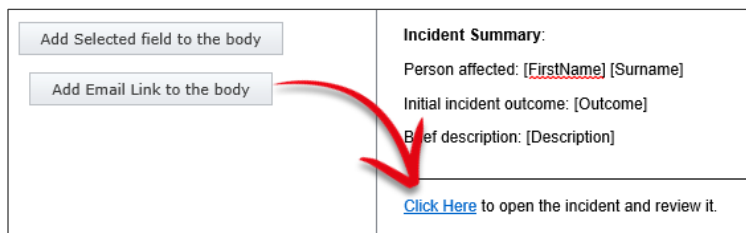
Email

1 We have decided to put the name of the ward / unit in which the incident was recorded into the subject line of the email. What is shown in the square brackets is the database field name, as opposed to the friendly label that you see on the incident form.

② [NotificationName] is the database field name for the field Reporter's Name.

③ In the body of the email, we have included the name of the person affected – achieved by entering the First Name and then Surname fields; the initial outcome rating of the incident, and the content of the Summary field. This is considered good practice – try not to include too much information in the email, lest the user perhaps be disinclined to click the link and open the record as they may feel they have all the information they need.

④ You are able to determine where the link to open the record should appear in the email. Click the *Add email link to body* button to insert the "Click here" link text wherever your cursor is. Note that you can change the link text from "Click Here" to something else just by typing what you want and deleting what you do not want.


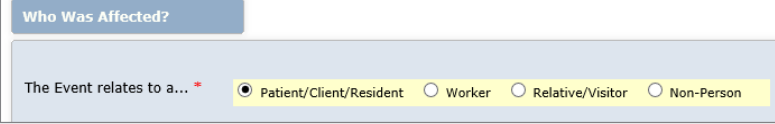
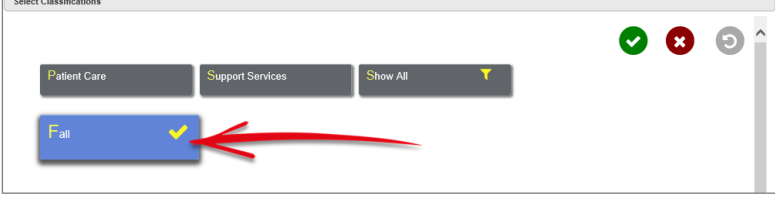


The screenshot shows a two-pane interface. The left pane contains two buttons: "Add Selected field to the body" and "Add Email Link to the body". A red arrow points from the "Add Email Link to the body" button to the right pane. The right pane displays an "Incident Summary" with the following text: "Person affected: [FirstName] [Surname]", "Initial incident outcome: [Outcome]", and "Brief description: [Description]". At the bottom of the summary, there is a blue underlined link that says "Click Here to open the incident and review it."

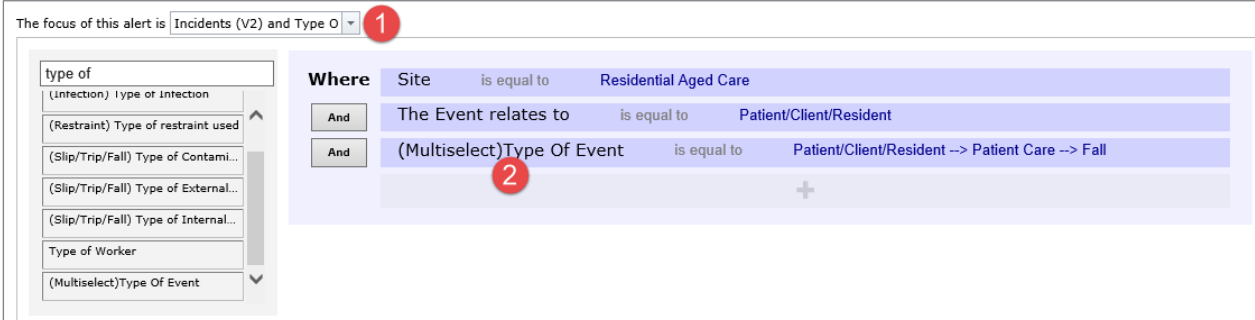
Notify falls coordinator of a new resident fall

Conditions

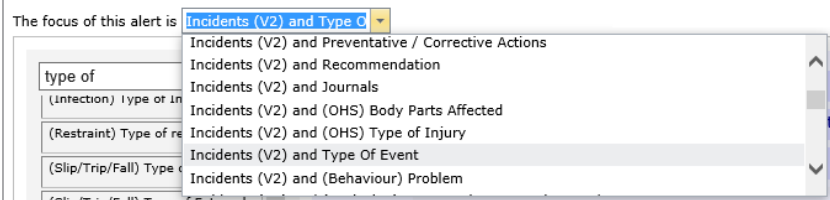
This alert needs to trigger for resident falls that happen at a multi-campus hospital which has a site for residential care.

<p>Site must be Residential Aged Care</p>	
<p>The Event relates to must be either Patient/Client/Resident</p>	
<p>Type of Event must be Fall</p>	

Our resulting conditions look like this:



1 Because one of the fields we needed to test was a multi-select field, we needed to select the appropriate field in the **The focus of this alert is** list.



Without this, the **Type of Event** field would not be available to test against. This same action must be performed whenever you need to create conditions for multi-select lists, subforms, and journals.

Alert Examples Supplement

You're able to create a second Focus, if you need to build the condition based on a second multi-select field. Click **Select to add a related filter for** then clicking on the sub form. This will present a second condition builder row. This second condition builder row will display the fields from the selected sub forms

The focus of this alert is **Just Incidents**

Select to add a related filter for

Preventive Action
Contacts
Causal Factors
Recommendations
Click to enter event type
File Notes

Restriction filter for **Preventive Action** to act upon records and emails Disable this Filter

The second condition builder will need to be selected as a **And**, or an **But not** option.

Restriction: means to add or include this condition

Exclusion: means to not include this condition

(Or) against the alert focus: or it can be either condition build

Disable this filter, removes the second condition builder row that you have added

Please enter a Descriptive name for these conditions: Eg. Staff manual handling injuries; Risks with overdue status, etc...

The focus of this alert is **Just Incidents**

Start typing a field name here

(Formal Review) Date report due to C...
(Formal Review) Date signed by CEO
(Formal Review) Date submitted to Q...
(Formal Review) Executive Sponsor
(Formal Review) Final RCA report sig...

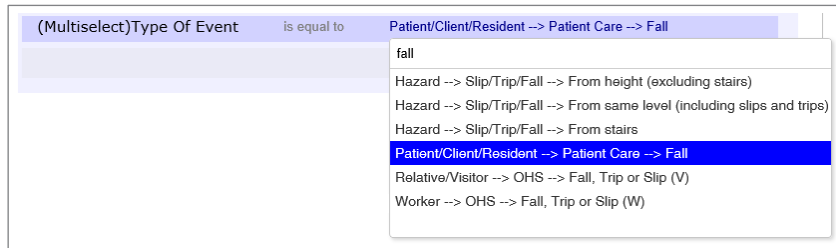
Or (against alert focus) filter for **Preventive Action** Disable this Filter

Start typing a field name here

(Preventive Action)Action ID
(Preventive Action)Associated Contrib...
(Preventive Action)Corrective Action

Alert Examples Supplement

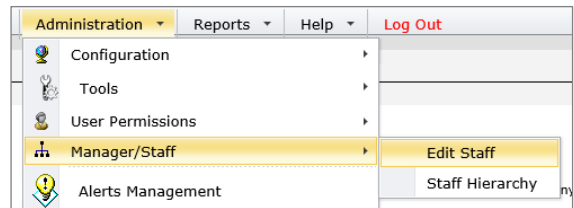
2 You can then search for the required value you wish to test.



Notify a user's nominated line manager when they enter a new incident (uses Manager/Staff Relationships)

Purpose

If your configuration of RiskMan utilises Manager/Staff Relationships to establish reporting pathways, then this example is relevant to you.



Recipients

In this case, the Recipient will be set as the "Reporter's Manager":

Recipients

The nominated line manager(s) of the user who originally reported the record

Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

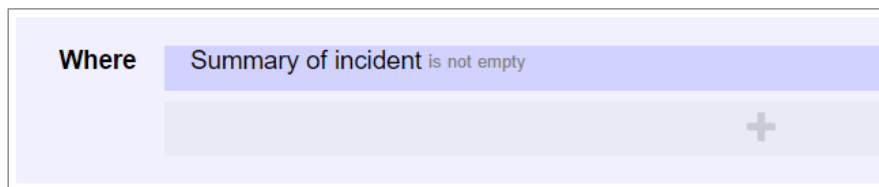
Alert a user named in a field
Select a field that contains a Username

Add a group of recipients

In a system where Manager/Staff Relationships are used, when this alert is triggered, only the **immediate** line manager will receive the email we configure; however, all staff up the reporting channel will have permission to see the record in question.

Conditions

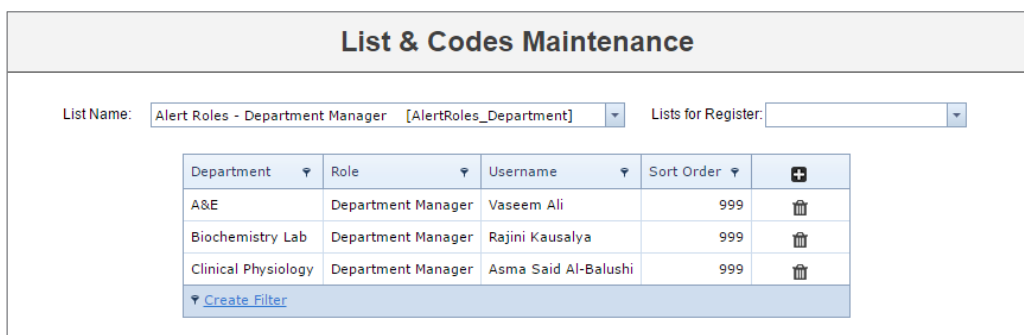
In order for this alert to trigger, we only need one simple condition to be met. We usually base this on a mandatory field that the default user needs to complete, thereby assuring that all incidents will trigger this alert. In this case, we have chosen the **Summary** field:



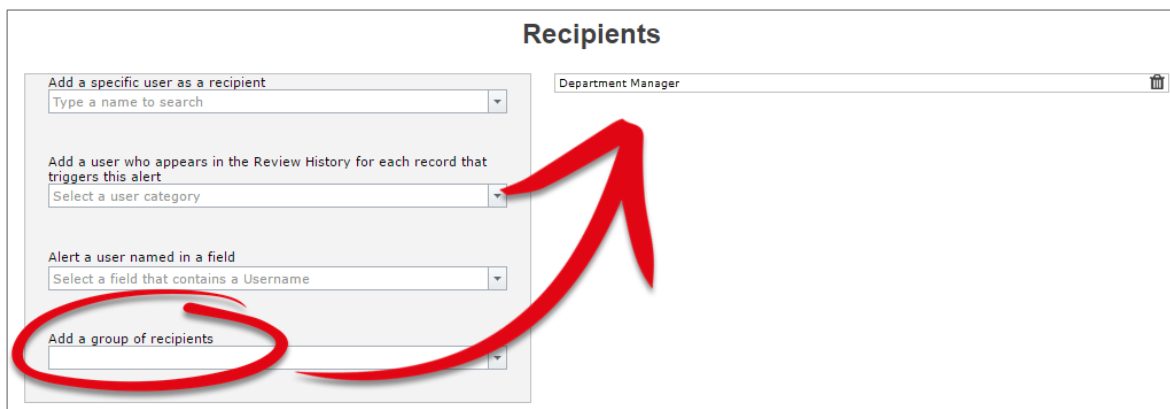
Notify a Department Manager of a new incident lodged in their department (uses Org Structure list)

Recipient

This example is rather similar to the previous one. However, this example refers to organisational structure lists contained within list & codes maintenance:



Various permutations of this type of list exist in some systems today; however, the principal in selecting the recipient is always the same:



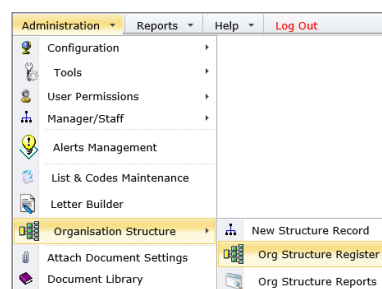
Remember that this kind of list allows you to target the responsible line manager in case a record is overdue for being followed up, or other similar situation.

Escalation processes

If your system uses manager/staff relationships, then you can easily have an escalation process in place if, for example, an incident does not have investigations performed in a satisfactory timeframe.

[Refer to Reminder Alerts](#) for an example on notifying a manager that they have not yet completed their investigations, and also creating escalation processes if nothing is done.

Notify a unit manager that a new incident has been lodged for their unit (uses Org Structure Register)



This is an example of an alert in a system that uses an Organisation Structure register in order to automatically assign the recipient.

Conditions

As this is an initial notification alert, all we need to do is ensure that we have a condition whereby a field that is mandatory for the default user has been filled in, which will ensure this alert will trigger every time for any new incident:

A screenshot of a form titled 'What Happened?'. It contains three input fields: 'Summary', 'Details', and 'Action taken at time'. The 'Summary' and 'Details' fields are highlighted in yellow. A red arrow points from the 'Summary' field to the 'Details' field. The 'Summary' field has a red asterisk and a checkmark icon. The 'Details' field has a red asterisk and a checkmark icon. The 'Action taken at time' field has a checkmark icon.

In this example system, we know that the **Summary** field is displayed for every incident, regardless of what type it is, and it is always mandatory. We will use this field as our condition to trigger the alert:

A screenshot of a form showing a condition. The word 'Where' is followed by a blue bar containing the text 'Summary is not empty'. Below this bar is a grey bar with a plus sign (+).

Recipient

In this example, we will use the last option; Add group of recipients, and select **Unit/Department Owner** Owner:

1 **Recipients**

Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

Add a group of recipients

Group Name	Parameter Help
HHS Groups	Please enter the name of the group
Facility Groups	Please enter the name of the group
Unit/Department Owner	No parameter required
Unit/Department Secondary Owner	No parameter required
Division Owner	No parameter required
Division Secondary Owner	No parameter required
Service/Stream Owner	No parameter required

The **Unit/Department Owner** group recipient has been selected. The next thing to do is click the **Tick** button to add this selection as our recipient:

2 **Recipients**

Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

Add a group of recipients
Unit/Department Owner

In this final screenshot, you can see our selection added as the recipient:

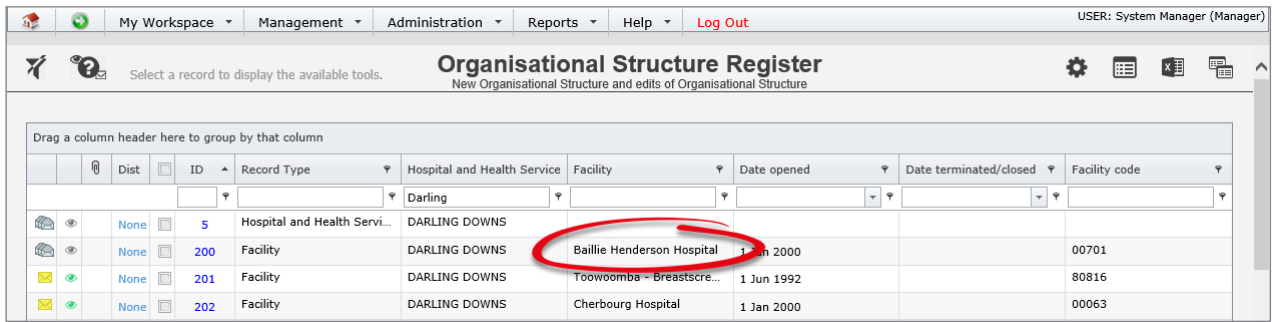
How the lookup works:

When an incident is entered, based on the combination of where it occurred, RiskMan will look up the corresponding matching value in the Organisational Structure register.

In the example to the right, we can see that the incident occurred in the ward/unit of **Pharmacy**, at **Bailey Henderson Hospital**.

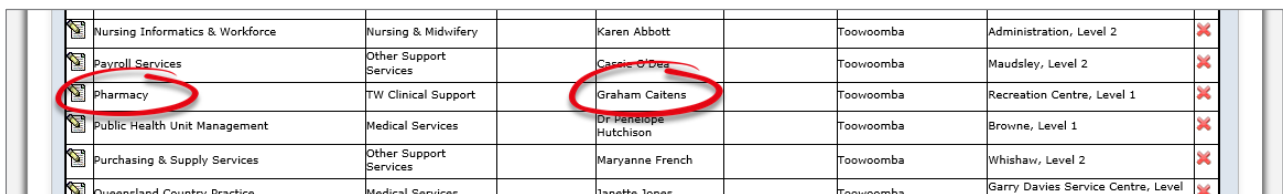
Alert Examples Supplement

The system locates the corresponding record in the Organisational Structure register:



Organisational Structure Register									
New Organisational Structure and edits of Organisational Structure									
Drag a column header here to group by that column									
	Dist	ID	Record Type	Hospital and Health Service	Facility	Date opened	Date terminated/closed	Facility code	
	None	5	Hospital and Health Servi...	DARLING DOWNS	Baillie Henderson Hospital	1 Jan 2000		00701	
	None	200	Facility	DARLING DOWNS	Toowoomba - Breastscre...	1 Jun 1992		80816	
	None	201	Facility	DARLING DOWNS	Cherbourg Hospital	1 Jan 2000		00063	

Then it locates the matching ward/unit, and identifies the user(s) currently listed as responsible for it:



Nursing Informatics & Workforce	Nursing & Midwifery	Karen Abbott	Toowoomba	Administration, Level 2	✘
Payroll Services	Other Support Services	Cassie O'Dea	Toowoomba	Maudsley, Level 2	✘
Pharmacy	TW Clinical Support	Graham Caitens	Toowoomba	Recreation Centre, Level 1	✘
Public Health Unit Management	Medical Services	Dr. Penelope Hutchison	Toowoomba	Browne, Level 1	✘
Purchasing & Supply Services	Other Support Services	Maryanne French	Toowoomba	Whishaw, Level 2	✘
Queensland Country Practice	Medical Services	Janette Jones	Toowoomba	Garry Davies Service Centre, Level	✘

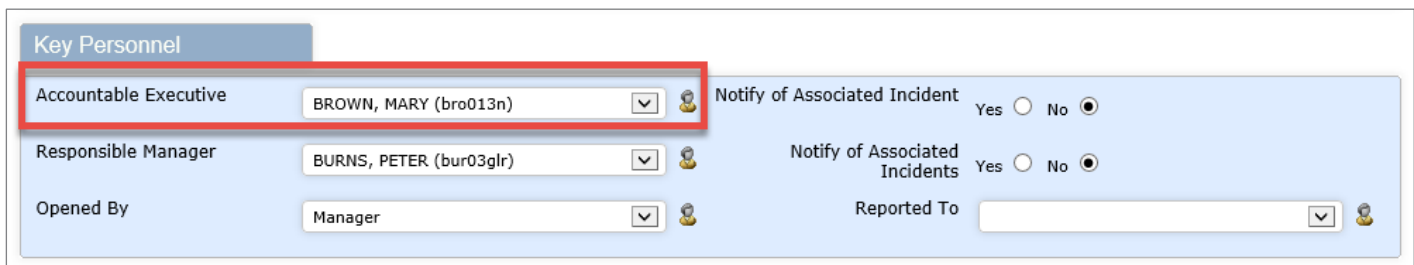
So in the case of this incident, we can see that **Graham Caitens** will be the user alerted.

Notify a user when they are listed as the accountable executive for a new risk

This example is the common method used to notify any user that they have been nominated as responsible for something. Although we are using the example of the executive accountable for a risk in the risk register, this example is fairly universal and you can simply switch out the register and field name of your choice.

Scenario

When a user is nominated as the accountable executive for a new risk, notify them via email:

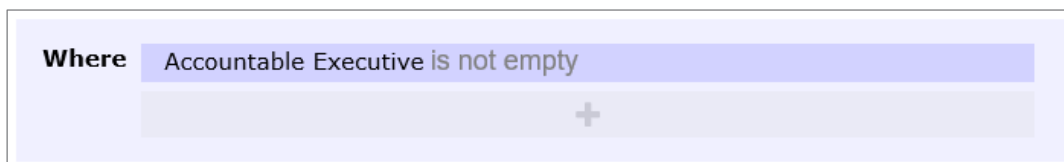


The screenshot shows a 'Key Personnel' form with the following fields and options:

Accountable Executive	BROWN, MARY (bro013n)	Notify of Associated Incident	Yes <input type="radio"/> No <input checked="" type="radio"/>
Responsible Manager	BURNS, PETER (bur03glr)	Notify of Associated Incidents	Yes <input type="radio"/> No <input checked="" type="radio"/>
Opened By	Manager	Reported To	<input type="text"/>

Conditions

At the most basic level, all we need to do is check to see if the **Accountable Executive** field has been completed. As soon as there is a user listed in that field, we want this alert to be triggered:



The screenshot shows a 'Where' condition in a rule builder interface:

Where Accountable Executive is not empty

Recipient

We need to tell the system to choose the user listed in the **Accountable Executive** field and make them the recipient:

Recipients

Add a specific user as a recipient
Type a name to search

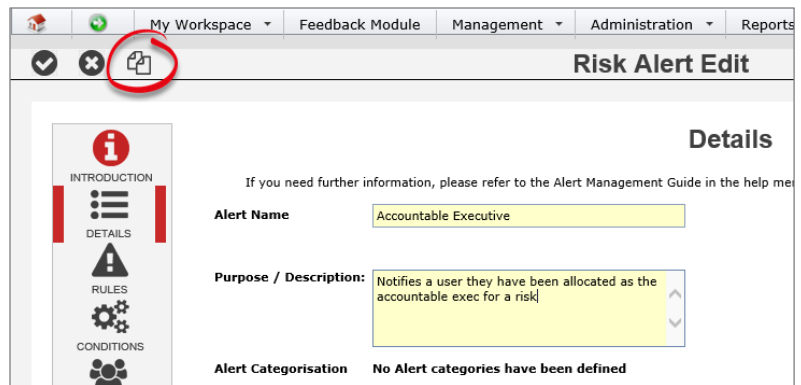
Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

User(s) listed in the "Accountable Executive" field

Pro Tip 1: Alert Cloning

You will notice that in the example listed above, there were two fields where responsible users can be nominated; Accountable Executive, and Responsible Manager. Once you have saved the first alert, you can use the alert **Clone** button (as shown to the right here) to instantly create the alert that monitors the Responsible Manager field instead. You will just need to change the Recipient to “The user listed in the Responsible Manager field” via the “Add a user named in a field” option under Recipients.



Pro Tip 2: When using this technique to notify users named in subforms

This exact technique can be used to notify users listed in subforms, however in order to be able to choose the fields from subforms, you must remember to do the following.

Let’s suppose that we wanted to use this technique to notify a user that a preventative/corrective action has been assigned to them:

Is Preventative / Corrective Action Required? Yes No

Add Action

Action ID	Action Description	Costs (\$)	Person Responsible for Implementation	Outcome measure	Date for action implementation	Action completed?	Date action completed
1	Put up signage to inform staff of proper procedure		Andrew_mgr (Andrew_mgr)		15 Feb 2017	No	

In order to be able to use the fields from the subform as both conditions and recipients, we need to make sure that we choose that this subform is the focus of this alert:

Alert Examples Supplement

Conditions

Here you need to define the conditions which must be met in order for the alert to trigger. You can add as many conditions as necessary. The 'Test Conditions' button will tell you how many existing records there are which match the conditions you have added.

Please enter a Descriptive name for these conditions: Eg. Staff manual handling injuries; Risks with overdue status, etc...

The focus of this alert is **Incidents and Action**

Start typing a field name here

- (Accountable Medications) Action tak...
- (Accountable Medications) Actual me...
- (Accountable Medications) Additional...
- (Accountable Medications) Commenc...
- (Accountable Medications) Commenc...
- (Accountable Medications) Date loss/...

Now we are able to search not only for the fields on the main form, but also the fields in the Preventative/Corrective Actions subform:

The focus of this alert is **Incidents and Action**

action

Where (Action)Person Responsible for Implementation (Username) is not empty

- (Action)Action Description
- (Action)Costs (\$)
- (Action)Person Responsible for Imple...
- (Action)Person Responsible for Imple...
- (Action)Date Person Responsible Not...
- (Action)Outcome measure

This also allows us to see the “person” fields from the subform in order to add them as the recipient of the alert:

Recipients

Add a specific user as a recipient

Type a name to search

Add a user who appears in the Review History for each record that triggers this alert

Select a user category

Alert a user named in a field

Select a field that contains a Username

Add a group of recipients

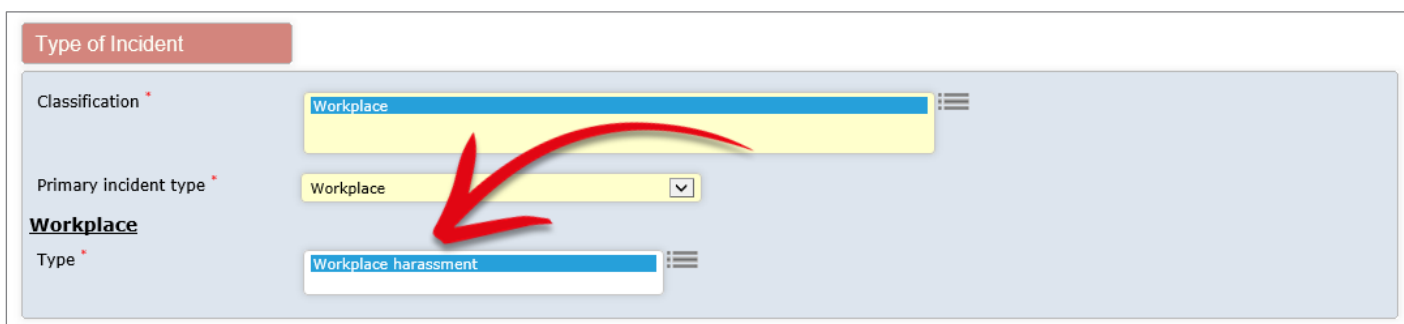
Create an exception which doesn't send workplace harassment incidents on to a user's line manager; instead sends them to a certain HR user

This example involves not one, but two alerts. One alert will send on all incidents to a user's manager, excluding staff workplace harassment incidents; the second will send on staff workplace harassment incidents only to a certain user in the HR department.

This example is based on a system using Manager/Staff Relationships, but the technique itself is fairly universal.

Scenario

In this example, we will be focussing on the following section:



The screenshot shows a configuration panel titled "Type of Incident". It contains three fields:

- Classification**: A dropdown menu with "Workplace" selected.
- Primary incident type**: A dropdown menu with "Workplace" selected.
- Workplace Type**: A dropdown menu with "Workplace harassment" selected.

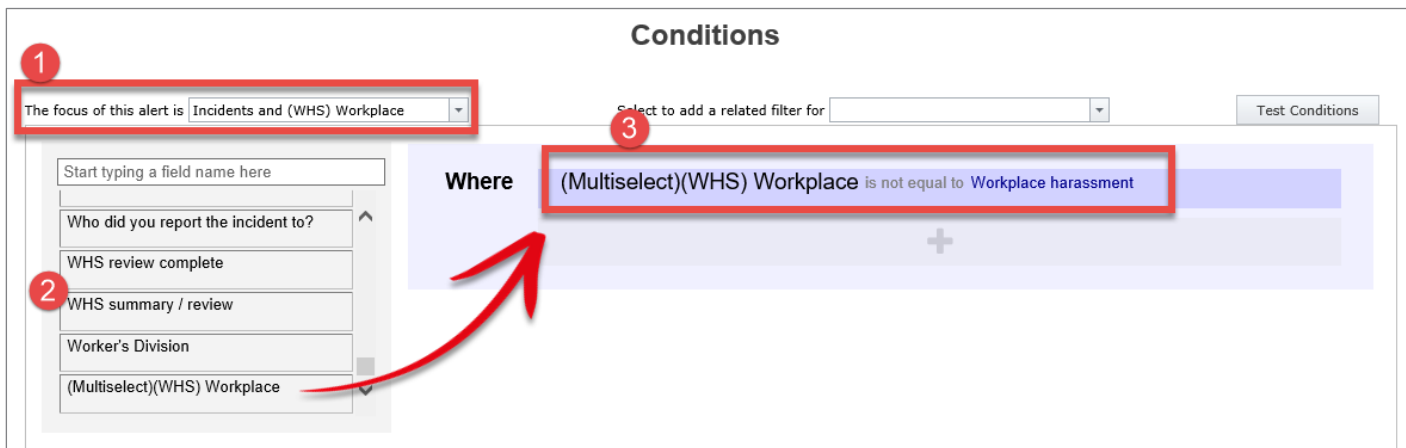
A red arrow points from the "Workplace" option in the "Classification" dropdown to the "Workplace" option in the "Primary incident type" dropdown.

You will need to adjust the following example settings to suit your own system configuration. For example, your system might have a separate classification for workplace harassment (or similar).

Alert 1: Send incidents to the line manager, with the exception of workplace harassment

Conditions

Because the field we want to test, *Workplace – Type*, is a multi-select list, we will need to ensure that we select is as part of the **alert focus**, as shown in ❶ below:

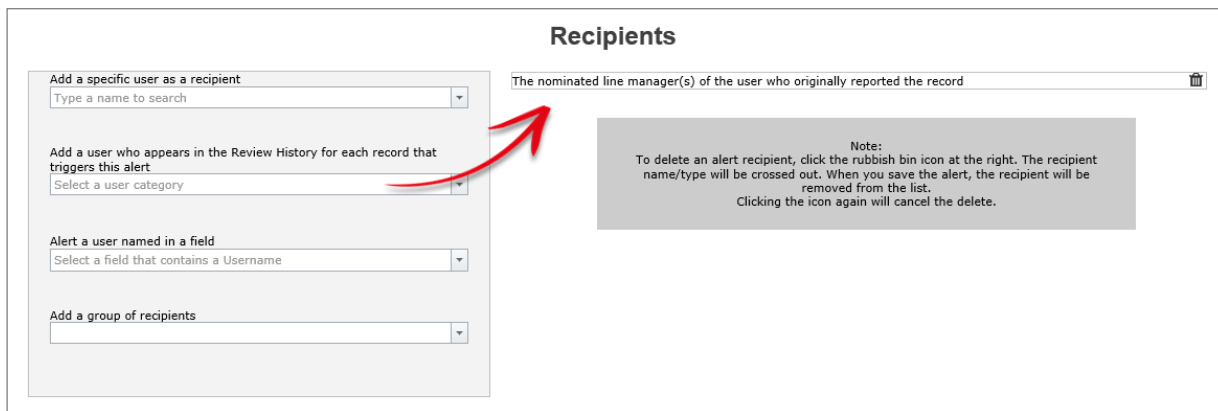


We can then see ❷ the **(WHS) Workplace** field in the list of available fields.

We will add that field as our condition: We want this alert to trigger ❸ if the value chosen in that field **is not equal to** Workplace harassment. This means the alert will trigger for absolutely anything else, and the incident will be sent to the appropriate line manager, as expected.

Recipient

Our recipient will be the line manager of the user who entered the incident:



Alert 2: Send any Workplace Harassment incidents only to a certain user in HR

Conditions

The conditions are just as simple for the second alert. If Workplace harassment was selected, then irrespective of any other information in the incident, it should only be sent to the appropriate HR user for confidential follow up:

Conditions

The focus of this alert is **Incidents and (WHS) Workplace**

Select to add a related filter for

Where **(Multiselect)(WHS) Workplace** is equal to **Workplace harassment**

Start typing a field name here

- Who did you report the incident to?
- WHS review complete
- WHS summary / review
- Worker's Division
- (Multiselect)(WHS) Workplace**

Pro Tip: Yes, you should **Clone** the original alert in order to save time!

Recipients

Now we will send any of these confidential harassment incidents only to a certain user in HR:

Recipients

Add a specific user as a recipient

Type a name to search

Nick Jones

Add a user who appears in the Review History for each record that triggers this alert

Select a user category

Alert a user named in a field

Select a field that contains a Username

Add a group of recipients

Notify a user who created a journal task that it has been marked as complete

This example “closes the loop” with journal tasks, notifying the user who *created* the journal task when the nominated user marks it as **Actioned**.

Scenario

This alert will monitor journals of the type “Action required” and for when journals of that type are marked as Actioned:

The screenshot shows a 'Journal Entries' form. At the top is a blue header with the text 'Journal Entries' and a button 'Add New Journal Entry'. Below this is a table with columns: DateStamp, Journal Type, Comment / Action Required, Follow Up Allocated To, Follow Up By Date, and Item Actioned. A single row is visible with the following data: DateStamp: 25 Jan 2017 02:01, Journal Type: Action required, Comment / Action Required: Please follow up with the NOK and report your findings. Thanks, Follow Up Allocated To: Nick Jones, Follow Up By Date: 30 Mar 2017, Item Actioned: on. Below the table, there are fields for 'Journal Type: Action required', 'DateStamp: 25 Jan 2017 02:01', 'Comment / Action Required: Please follow up with the NOK and report your findings. Thanks', and 'Follow Up By Date: 30 Mar 2017'. A red circle highlights the 'Item Actioned' field, which currently shows 'No' and an 'Action' button. To the right of this field, it says 'Follow Up Allocated To: Nick Jones (Nick Jones)'. At the bottom of the form, there are 'Edit' and 'Delete' buttons, and a green link 'New Unsaved Journal Entry'.

Conditions

Because we want to add conditions for Journal fields, we have to ensure we select Journals as the alert focus:

The screenshot shows a 'Conditions' configuration screen. At the top, it says 'Conditions' and 'Select to add a related filter for' with a dropdown menu. A button 'Test Conditions' is on the right. On the left, there is a list of fields to choose from: '(Journals)Item Actioned', '(Journals)Journal Follow Up Date', '(Journals)Journal Type', '(Journals)Linked Document Path', and '(Journals)Received Date'. A red circle highlights the text 'The focus of this alert is Incidents and Journals'. In the main area, there are two conditions listed under 'Where': '(Journals)Journal Type is equal to Action required' and '(Journals)Item Actioned is equal to Yes'. A red box highlights these two conditions. An 'And' button is to the left of the conditions, and a plus sign is below them.

Recipients

We will use the **Alert a user named in a field** option to nominate the **(Journals)Username** field, which is the name of the user who originally created the journal action.

The screenshot shows a configuration window titled "Recipients". On the left, there are four dropdown menus for adding recipients:

- Add a specific user as a recipient**: Type a name to search
- Add a user who appears in the Review History for each record that triggers this alert**: Select a user category
- Alert a user named in a field**: Select a field that contains a Username
- Add a group of recipients**

On the right, a list of selected recipients is shown: "User(s) listed in the "(Journals)Username" field". A red arrow points from the "Alert a user named in a field" dropdown to this selected option.

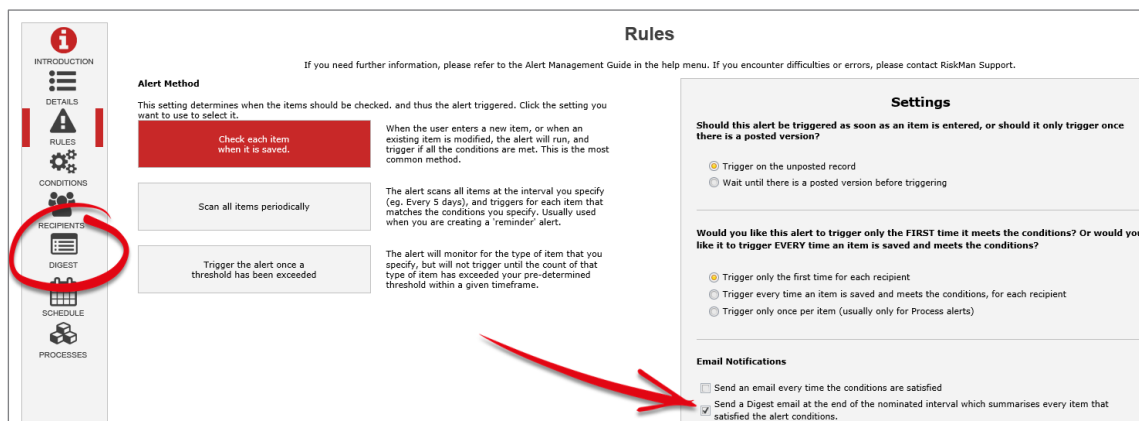
Notify the CEO of all the serious patient incidents that happened in the previous 7 days via a digest alert

This example demonstrates how to use the Digest Email functionality. A digest email is a summary of all the records that matched/triggered your alert during a given timeframe, eg. The previous 7 days.

It should be noted that at this stage, digest alerts can only be used when the recipient of the alert is a specific (i.e. Static) user, instead of dynamically assigned users.

Rules

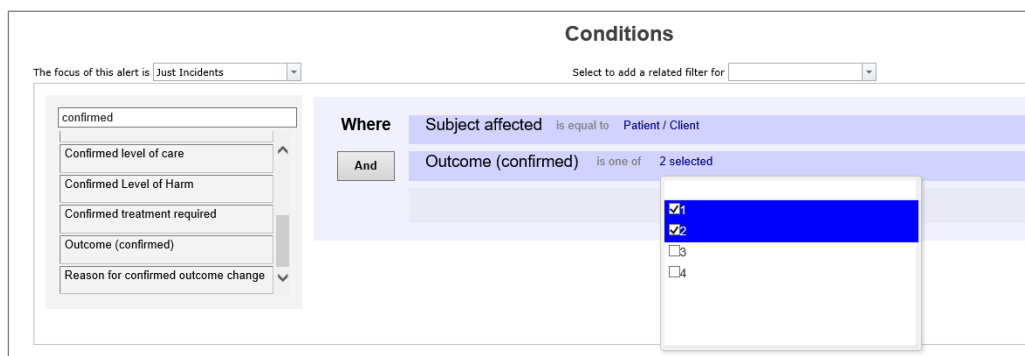
In order for the settings for a Digest Email to appear, you must have selected that you want to send a digest email in the Rules section:



Please note that Digest Emails can only be configured using the **Alert Method** of **Check each item when it is saved**.

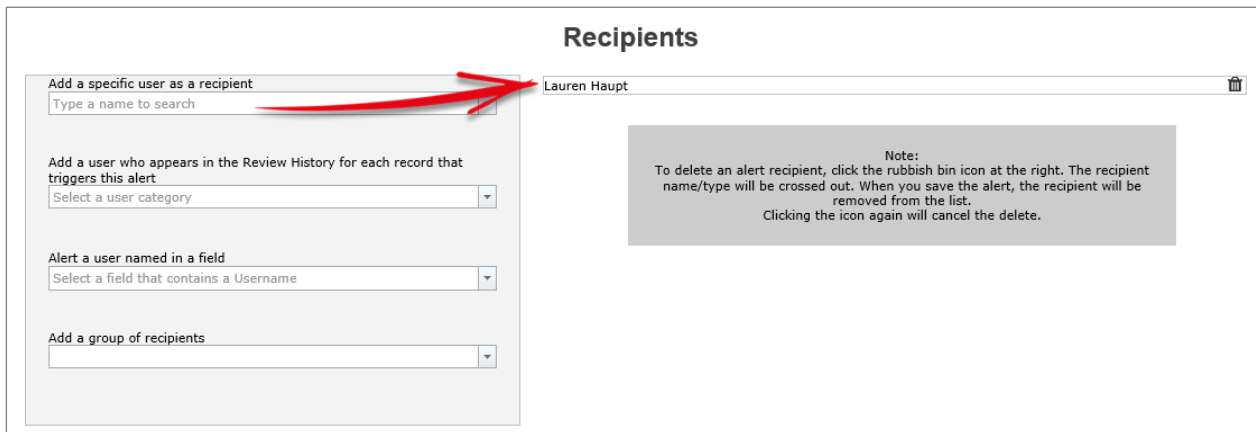
Conditions

For the purpose of this example, we have stipulated that we consider the incident to be “serious” if the **Confirmed Outcome** was either 1 or 2. We have use the “is one of” test to achieve this easily:



Recipients

We have selected our CEO manually as the intended recipient. Remember that digest alerts will only work when you select a specific user as the recipient, as opposed to the dynamic methods.



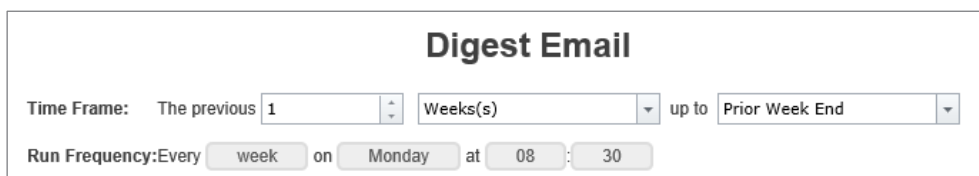
Digest Email Setup: Time Frame

The first thing to configure for our digest email is what time frame we want to include, and how often we want the digest email to be sent to the recipient.

In our example, we have said that we want the digest email to be delivered every Monday morning at 8:30am, and it should include the previous 7 days from the day prior to the run date as the time frame:

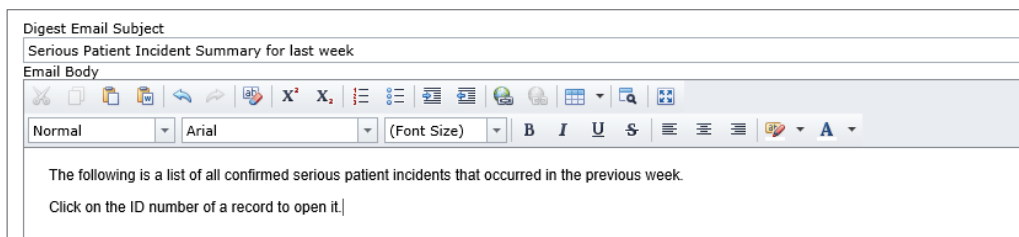


Note that we could also achieve the same time frame by saying that we want it for the previous 1 week up until the prior week's end, which is considered to be Sunday:



Digest Email Setup: Static Content

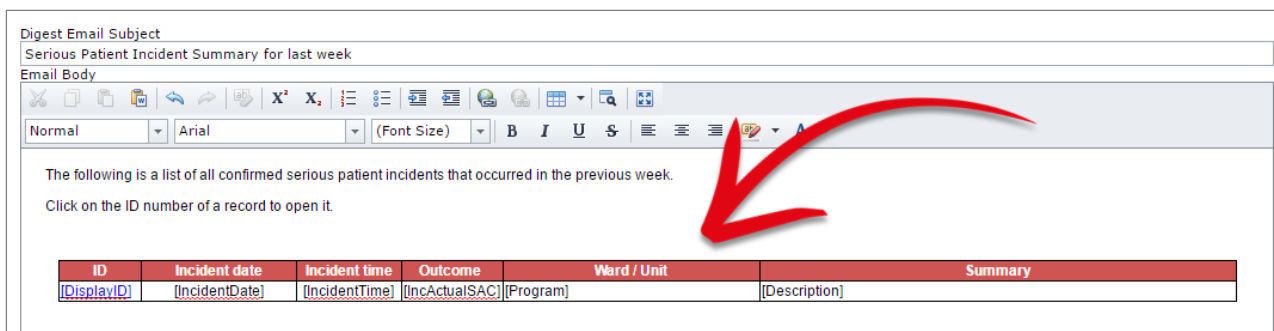
Add the static content of the email as required. Our example is as follows:



Digest Email Setup: Summary Table (dynamic content)

The idea of a digest email is to summarise all the associated records in the digest via a table. You can choose the columns you wish to display in summary of each record in the digest. You can also designate that one column should be the clickable link to open the associated record – which would usually be the ID number of the record.

Here is what our end point looks like. We will then examine how we arrived at the end point.

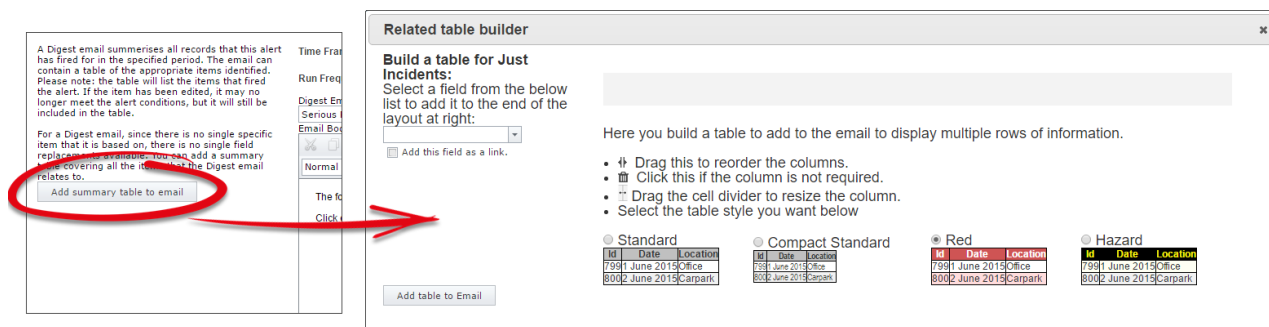


As you can see, we have decided to build our summary table including the following fields:

- Incident ID (inserted as the clickable link to open each respective record)
- Incident Date
- Incident Time
- Confirmed Outcome Rating
- Ward / Unit
- Summary

Alert Examples Supplement

In order to add this table to the body of the email, we need to click the **Add summary table to email** button, which will then open the **Related Table Builder**:



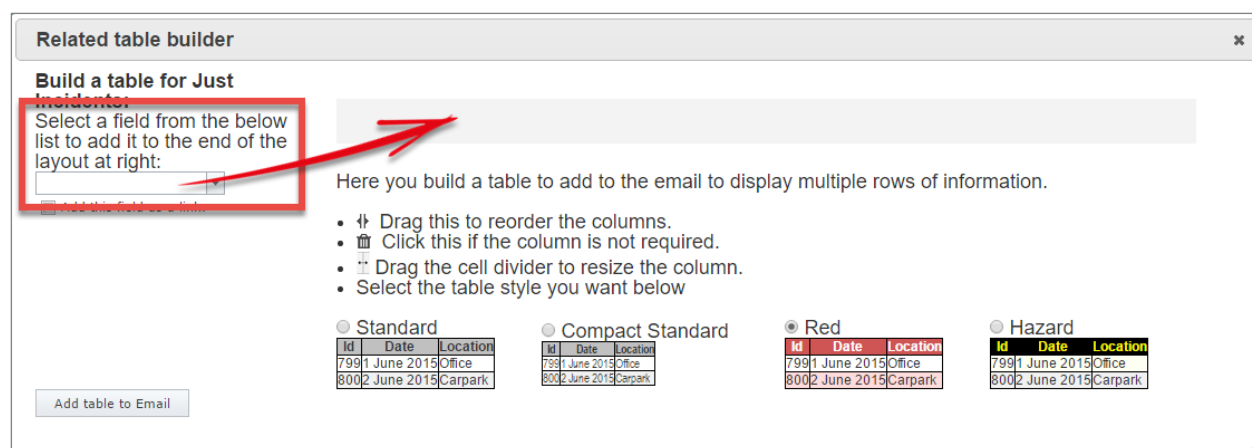
The idea of the related table builder is to:

1. Find and add all the fields from the form you want as columns in your table
2. Adjust their widths, and the order in which they appear in the table
3. Choose a pre-defined table format
4. Apply finishing touches once you have added the table to your email body.

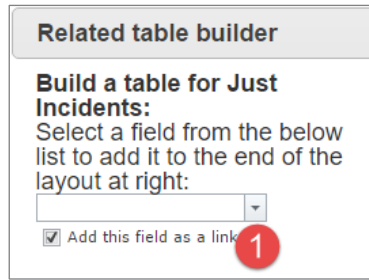
Let's follow those steps now.

Find and add all the fields from the form you want as columns in your table

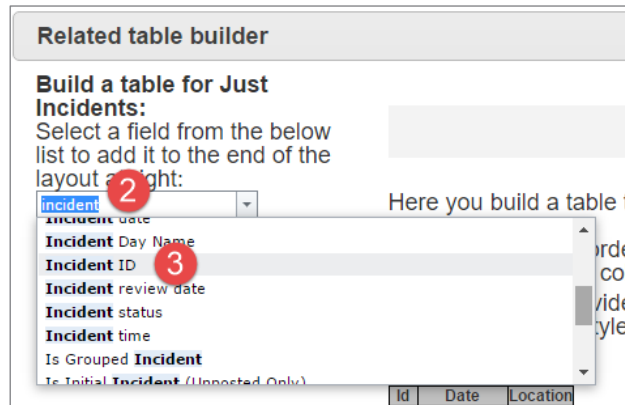
From the drop down field on the left, find each field you wish to add to the table. As you click on a field, it will be added to the table as a column header, in the grey area marked below:



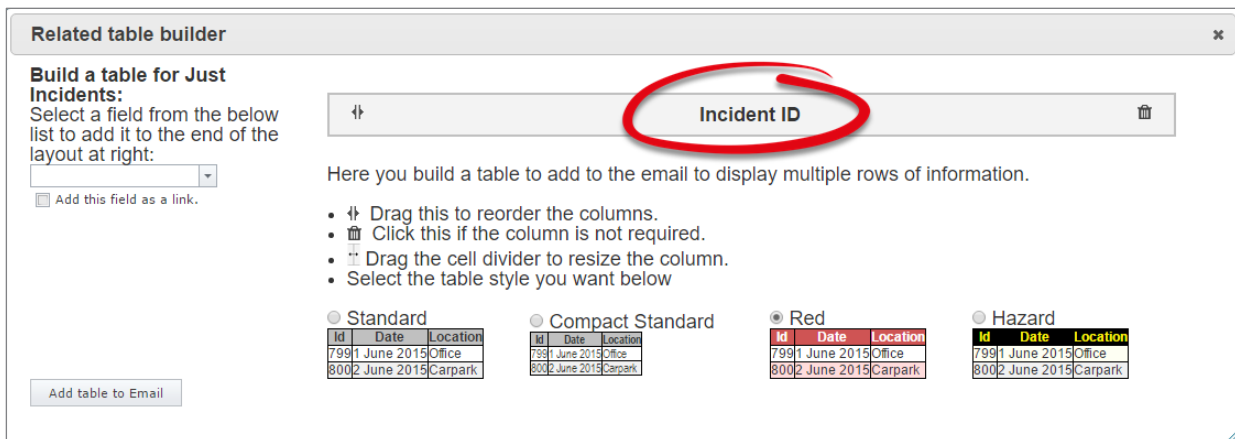
The first field we will add is **Incident ID**. Because we want Incident ID to be the clickable link to open each record in the table, **before** we add it to the table, we will **1** select the **Add this field as a link** check box:



2 Start typing the name of the field we want – ‘incident’. Then 3 click on the desired field:



The field is added to the table column header area:



Repeat to add the other fields you wish to add as columns in your table:

Related table builder ✕

Build a table for Just Incidents:
 Select a field from the below list to add it to the end of the layout at right:

Add this field as a link.

↑ Incident ID	↑ Incident date	↑ Incident time	↑ Ward / Unit	↑ Outcome (confirmed)	↑ Summary
---------------	-----------------	-----------------	---------------	-----------------------	-----------

Here you build a table to add to the email to display multiple rows of information.

- Drag this to reorder the columns.
- Click this if the column is not required.
- Drag the cell divider to resize the column.
- Select the table style you want below

Standard

Id	Date	Location
799	1 June 2015	Office
800	2 June 2015	Carpark

Compact Standard

Id	Date	Location
799	1 June 2015	Office
800	2 June 2015	Carpark

Red

Id	Date	Location
799	1 June 2015	Office
800	2 June 2015	Carpark

Hazard

Id	Date	Location
799	1 June 2015	Office
800	2 June 2015	Carpark

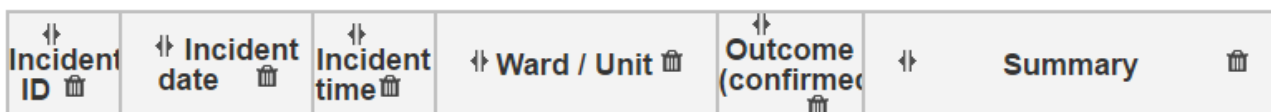
You will notice that the space allocated for each column you add is divided equally between the total number of columns. You will have a chance to adjust the column widths as appropriate in the next step.

Adjust column widths, and the order in which they appear in the table


Place your mouse cursor on the border line in between each column header in order to resize it:

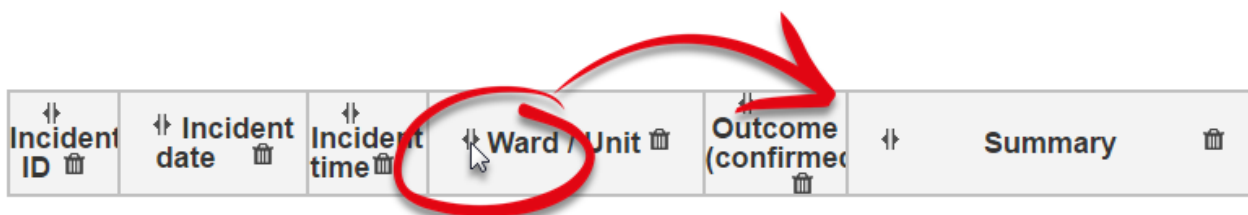


After adjusting the widths, our columns are looking more appropriate for the content they will likely contain:



Alert Examples Supplement

The next step to change the order of the columns as desired. To do this, click on the  icon of a column header, and drag it to the desired position:



Our final column header setup is as follows:

Incident ID	Incident date	Incident time	Outcome (confirmed)	Ward / Unit	Summary
-------------	---------------	---------------	---------------------	-------------	---------

Choose a pre-defined table format

1 Choose from one of the table formats at the bottom of the related table builder dialogue. 2 Click the **Add table to email** button when you are happy with the setup of the table. It will be added to your email body where the cursor was.




Related table builder

Build a table for Just Incidents:
Select a field from the below list to add it to the end of the layout at right:

Add this field as a link.

Incident ID	Incident date	Incident time	Outcome (confirmed)	Ward / Unit	Summary
-------------	---------------	---------------	---------------------	-------------	---------

Here you build a table to add to the email to display multiple rows of information.

-  Drag this to reorder the columns.
-  Click this if the column is not required.
-  Drag the cell divider to resize the column.
- Select the table style you want below

Standard

Id	Date	Location
7991	June 2015	Office
8002	June 2015	Carpark

Compact Standard

Id	Date	Location
7991	June 2015	Office
8002	June 2015	Carpark

Red

Id	Date	Location
7991	June 2015	Office
8002	June 2015	Carpark

Hazard

Id	Date	Location
7991	June 2015	Office
8002	June 2015	Carpark

ACKNOWLEDGEMENT ALERTS

When a user submits an incident, send them an acknowledgement email to confirm receipt of the record, and inform them what they can do next

This is a great alert to have in your system in order to provide guidance to end users on both RiskMan functionality, and also pointers about policy / procedure in your organisation.

Granted, in many organisations, there may be a significant percentage of users who do not have a company email address. However, having an alert in place like this can really assist with getting buy-in with a new (or even existing) system.

Conditions

As seen previously, this is another scenario where we need to check for a mandatory field being filled in, order for the alert to trigger. In this example we are using the Summary field:

The screenshot shows the 'Conditions' configuration interface. At the top, the title is 'Conditions'. On the left side, there is a dropdown menu labeled 'The focus of this alert is' with the value 'Just Incidents'. Below this is a list of fields: 'summary', 'Complaint summary', 'SBAR Summary', 'Summary', and 'WHS summary / review'. On the right side, there is a dropdown menu labeled 'Select to add a related filter for'. Below this, a condition is defined: 'Where Summary is not empty'. This condition is highlighted with a red oval. A 'Test Conditions' button is visible in the top right corner.

Recipients

The recipient will be defined as the original reporter of the record, based on the Review History content:

Recipients

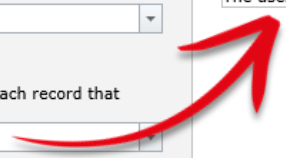
Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

Add a group of recipients

The user who originally reported the record



Email

The email is the most important facet of this alert. We want the email to be as useful as possible for the user – including direction on what do to next in the incident process, as well as pointing out useful functionality – without it being so long or detailed that the user doesn't bother reading it.

With that in mind, this is one way of configuring the email:

Dear [NotificationName]:

Thank you for submitting incident #[DisplayID] in RiskMan. This email is to confirm that this [IncidentInvolved] incident has been received, and has been forwarded on to your immediate line manager for review.

The following is a summary of the incident for your information:

Incident Type: [IncidentInvolved]

Summary: [Description]

Initial Severity/Impact Rating: [Outcome] *(please note that this rating may be altered when your manager reviews and investigates the incident)*

Incident Location: [Specialty], [Program]

What happens next?

Your incident will be reviewed by your line manager, and depending on the severity, by additional personnel too. Please note that you can [always](#) return to any incident you have submitted and:

- Add further information as it becomes available
- Correct any information as required; for example if the severity of an injury ended up being different than what was first suspected
- Check to see who else has viewed and/or modified your incident.

How do I open the incident?

To open this incident again, you can either:

- Click on the [blue link](#) at the bottom of this email, or
- Log in to RiskMan, and from the menu at the top of the screen, choose *My Workspace > Review My > Incidents*. This will display a list of all the incidents you have submitted. You can open any of these incidents by clicking its [blue ID number](#).

What can I do once I've opened the incident?

When you review an existing incident, you are able to:

- Check the [Review History](#). The Review History is an electronic audit trail which details every action associated with the incident. You will be able to see who has been notified of the incident, who has looked at it, who has edited it, and when all these actions occurred. The Review History is located at the [very bottom](#) of the Incident form.
- Check the [Change History](#). The Change History outlines the exact modifications made on the form, and who made each change. This will allow you to see who has added which pieces of information (or who has edited information you wrote). The Change History is a button located in the Control Panel at the top of the Incident form.
- Create a [Personal Alert](#). If desired, you can create a Personal Alert for this incident, which will notify you via email whenever this incident is modified by somebody else. To setup a Personal Alert, in the Control Panel at the top of the form, click the **Alert Me!** button, and choose the length of time you would like the system to monitor this incident for changes.
- If you add any further information to the form (or modify any existing information), click the **Submit** button at the bottom of the page to save your changes. Remember, every time anybody modifies an incident, a new historic version of the incident is created, meaning no information is ever 'lost'.

If you require any further assistance with RiskMan, please consult your line manager. Alternatively, in the **Help** menu within RiskMan you will be able to access the appropriate reference guides.

When an incident is marked as closed, send an acknowledgement email to the original reporter, thanking them for submitting the incident and confirming what has been done about it

This example is obviously going to be very similar to the previous one. Again, the aim is to close the feedback loop and include the original reporter in the overall process.

Conditions

Depending on how your system is configured, there are a number of ways you may elect to trigger the alert, including:

- Investigations completed date has been filled in
- Investigation status = complete
- Incident Closed on date has been filled in
- Incident status = closed

This is our example:

The screenshot shows a configuration window titled "Conditions". At the top, it says "The focus of this alert is" with a dropdown menu set to "Just Incidents (V2)". To the right, there is a dropdown menu labeled "Select to add a related filter for" and a "Test Conditions" button. Below this, a list of fields is shown on the left: "status", "Assessment of risk status documen...", "Emergency response status", "Incident Status", "Investigation Status", and "Status (Unposted only)". The main area shows a condition rule: "Where Incident Status is equal to Closed - Review Completed". This rule is highlighted with a red border.

Recipients

As with the previous example, the recipient will be defined as the original reporter of the record, based on the Review History content:

Recipients

Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

Add a group of recipients

The user who originally reported the record

Email

As with the previous alert example, the email is arguably the most important part of the alert. You need to decide what information is included, such as should you include information from fields to which the user does not have permission. We have configured our example as follows:

Dear [NotificationName]:

On [DateEntered] you submitted the following incident on RiskMan:

Incident Type: [IncidentInvolved]

Summary: [Description]

Severity/Impact Rating: [Outcome]

Incident Location: [Specialty], [Program]

This email is to confirm that the investigations for this incident have now been marked as **completed**. Thank you for reporting this incident - it has helped us provide a better and safer environment for all our patients, staff and visitors at [Incident_Location].

Investigations were completed by [InvestigatedBy] on [DateClosed]. The severity/impact of the incident has been recorded as [Outcome].

If you wish to review the outcome of the investigations, you can click on the link below to open and review the incident.

REMINDER ALERTS

Remind the responsible line manager that the investigations for an incident have not yet commenced, and the incident has now been in the system for more than 7 days. Add an escalation alert if nothing is still done 21 days later.

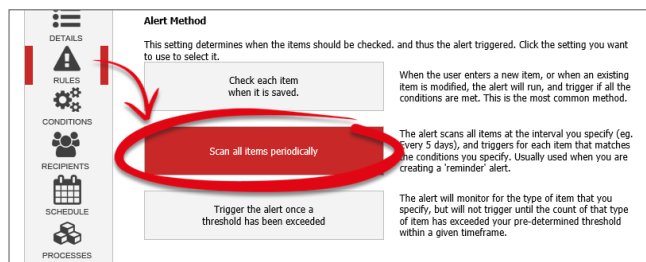
Situation

If an incident has no investigation/follow up added at all after **7 days** of an incident being reported; then, remind the appropriate line manager every 4 days via email that this hasn't been done. If, **after 21 days**, there is still NOTHING entered in that field, **escalate** this to *that* manager's line manager.

Alert 1: Checking if the immediate line manager has entered something into investigations or not

Rules

This alert will be a **periodic** alert; meaning that we will scan all items periodically at the interval we specify using the **Schedule** settings.



Conditions

We will check if anything has been entered into the investigations/findings field. We will also check to see how long since the incident was entered - greater than 7 days, and fewer than 21 days:

Alert Examples Supplement

Note that when you are creating a periodic alert, as in example above, there will be two versions of each date field – **Incident date**, and **Incident date (Periodic)**. The latter is the field to use in your test for the number of days until or since that date, as it allows you to use the numerical operators such as greater than or equal to, and less than or equal to.

The reminder will only be sent to the user while the record is between 7 and 21 days old in the system. Please note that this is just one example of how you might measure the age of the record; you could also opt to base this timing on when the record was first entered into RiskMan instead.

Recipients

The recipient will be the line manager of the person who entered the original record, as they are expected to perform the follow up for an incident in the first instance.

Recipients

Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

Add a group of recipients

The nominated line manager(s) of the user who originally reported the record

Schedule

We wanted to remind the responsible manager **every 4 days** that they haven't started any investigations for an incident. So we will setup the Schedule accordingly:

Schedule																																									
How often should this alert be processed?	<table border="1"><tr><td>Minute</td><td>Hour</td><td>Day</td><td>Week</td><td>Month</td><td>Year</td></tr></table>	Minute	Hour	Day	Week	Month	Year																																		
Minute	Hour	Day	Week	Month	Year																																				
Every:																																									
Days of month:	<table border="1"><tr><td>1st</td><td>2nd</td><td>3rd</td><td>4th</td><td>5th</td><td>6th</td><td>7th</td><td>8th</td><td>9th</td><td>10th</td></tr><tr><td>11th</td><td>12th</td><td>13th</td><td>14th</td><td>15th</td><td>16th</td><td>17th</td><td>18th</td><td>19th</td><td>20th</td></tr><tr><td>21st</td><td>22nd</td><td>23rd</td><td>24th</td><td>25th</td><td>26th</td><td>27th</td><td>28th</td><td>29th</td><td>30th</td></tr><tr><td></td><td></td><td></td><td></td><td>31st</td><td></td><td></td><td></td><td></td><td></td></tr></table>	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th	15th	16th	17th	18th	19th	20th	21st	22nd	23rd	24th	25th	26th	27th	28th	29th	30th					31st					
1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th																																
11th	12th	13th	14th	15th	16th	17th	18th	19th	20th																																
21st	22nd	23rd	24th	25th	26th	27th	28th	29th	30th																																
				31st																																					
Hours of the day:	<table border="1"><tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td></tr><tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td></tr></table>	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23																
00	01	02	03	04	05	06	07	08	09	10	11																														
12	13	14	15	16	17	18	19	20	21	22	23																														
	<table border="1"><tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td></tr><tr><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr></table>	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19																				
00	01	02	03	04	05	06	07	08	09																																
10	11	12	13	14	15	16	17	18	19																																

You could set up the reminder schedule based on day of the week if you wanted; it just depends on your requirements. In this case, we will remind the responsible manager every 4 days (based on the date of the month) that they haven't entered any investigations, and send the resulting reminder email at 11:15am.

The Escalation Alert: If the initial line manager still hasn't done anything about this record, and it's now more than X days old, let's escalate this to their immediate manager for follow up

Let us suppose that it is now more than 21 days since the incident, and STILL nobody has entered any investigations. You want this record to be escalated to the line manager of the manager who is responsible for that initial investigation.

Conditions

The conditions for the escalation alert will look like this:

The screenshot shows a configuration interface for alert conditions. It features a 'Where' section with two conditions stacked vertically. The first condition is 'Investigations/Findings is empty'. Below it is an 'And' button, followed by the second condition: 'Incident Date(Periodic) Days Since >= 21'. A plus sign is visible below the second condition, indicating that more conditions can be added.

So, now we are saying that if it is now at least 21 days since the date the incident occurred, and the investigations field is still empty, then trigger this alert.

Recipient

The immediate line manager has not completed their responsibilities within the given timeframe. So, we need to push this up the tree to that person's manager. We select the recipient accordingly:

The screenshot displays the 'Recipients' configuration screen. On the left, there are three options for adding recipients, each with a dropdown menu: 'Add a specific user as a recipient' (with a search box), 'Add a user who appears in the Review History for each record that triggers this alert' (with a category dropdown), and 'Alert a user named in a field' (with a field dropdown). A red arrow points from the second option to a selected recipient in a list on the right: 'The nominated line manager(s) of the line managers of the original reporter'. A trash bin icon is next to this recipient. A grey note box on the right contains the following text: 'Note: To delete an alert recipient, click the rubbish bin icon at the right. The recipient name/type will be crossed out. When you save the alert, the recipient will be removed from the list. Clicking the icon again will cancel the delete.'

Schedule

Alert Examples Supplement

This will be down to your requirements. We have opted to send the reminder email to the manager's manager every Wednesday at 10am.

Schedule																																																													
How often should this alert be processed?																																																													
Every:	<table border="1"><tr><td>Minute</td><td>Hour</td><td>Day</td><td>Week</td><td>Month</td><td>Year</td></tr></table>	Minute	Hour	Day	Week	Month	Year																																																						
Minute	Hour	Day	Week	Month	Year																																																								
Days of week:	<table border="1"><tr><td>Saturday</td><td>Sunday</td><td>Monday</td><td>Tuesday</td><td>Wednesday</td><td>Thursday</td><td>Friday</td></tr></table>	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday																																																					
Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday																																																							
Hours of the day:	<table border="1"><tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td></tr><tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td></tr></table>	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23																																				
00	01	02	03	04	05	06	07	08	09	10	11																																																		
12	13	14	15	16	17	18	19	20	21	22	23																																																		
Minutes of the hours:	<table border="1"><tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td></tr><tr><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr><tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr><tr><td>30</td><td>31</td><td>32</td><td>33</td><td>34</td><td>35</td><td>36</td><td>37</td><td>38</td><td>39</td></tr><tr><td>40</td><td>41</td><td>42</td><td>43</td><td>44</td><td>45</td><td>46</td><td>47</td><td>48</td><td>49</td></tr><tr><td>50</td><td>51</td><td>52</td><td>53</td><td>54</td><td>55</td><td>56</td><td>57</td><td>58</td><td>59</td></tr></table>	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
00	01	02	03	04	05	06	07	08	09																																																				
10	11	12	13	14	15	16	17	18	19																																																				
20	21	22	23	24	25	26	27	28	29																																																				
30	31	32	33	34	35	36	37	38	39																																																				
40	41	42	43	44	45	46	47	48	49																																																				
50	51	52	53	54	55	56	57	58	59																																																				

Remind a user that a journal task assigned to them is now overdue, and has not been actioned

Scenario

This alert is designed to monitor journals where action is required, we are now PAST the due date of that action, and the task has not been marked as actioned.

Conditions

The conditions for this alert warrant some further explanation:

The screenshot shows the 'Conditions' configuration screen. At the top, it says 'The focus of this alert is' with a dropdown menu set to 'Incidents (V2) and Journal' (marked with a red 1). Below this is a list of available conditions on the left and a 'Where' clause on the right. The 'Where' clause consists of three conditions connected by 'And' operators: 2. '(Journals)Follow Up By Date(Periodic) Days Since >= 3', 3. '(Journals)Item Actioned is equal to No', and 4. '(Journals)Journal Type is equal to Further Action'. A fifth condition, 5. 'Status (Unposted only) is not equal to Deleted', is shown below the others. A 'Test Conditions' button is visible in the top right corner.

❶ Remember to select Incidents & Journals as the **focus** of the alert – otherwise the Journal fields will not be available to be added as conditions, and you will not be able to select users named in journals as recipients.

❷ This condition lets us determine when we should start to remind the user that their task is overdue. If you set this to be 1, then the reminder will be sent on the first day after the due date. We have opted to give the user a 3 day grace period before we start to remind them. It's up to you to find the right balance!

❸ This test ensures that the alert will on trigger for journal tasks which have not yet been marked as actioned.

❹ We have restricted the alert to only look at journal types of Further Action. You may need to do something similar in your own alert, depending on how you have configured journals for this register.

❺ This test ensures that the alert should not trigger for journals which are attached to incidents which have been deleted. We would always recommend adding this condition to journal-related

Alert Examples Supplement

alerts. If we didn't include this condition, and a journal task is assigned for an incident, and that incident is subsequently deleted, then the alert doesn't care whether it is triggering for journal tasks attached to deleted incidents or not. This is an undesirable behaviour, so be sure to include this condition with your journal-related alerts.

Recipients

We will use the "Alert a user named in a field" function to dynamically assign the recipient:

Recipients

Add a specific user as a recipient
Type a name to search

Add a user who appears in the Review History for each record that triggers this alert
Select a user category

Alert a user named in a field
Select a field that contains a Username

User(s) listed in the "(Journals)Follow Up Allocated To" field

Optional: You could also notify the user who created the journal task by adding "(Journals) Username" as a recipient.

Email

Here is an example of an email we might send to the responsible user to inform them that their task is overdue:

Dear [FollowUpUser]

This email is to inform you that a journal task assigned to you as part of incident #[DisplayID] is now **overdue**.

Please complete this task as soon as practical by clicking the link below and marking the journal task as **Actioned**.

Task Summary:

Originally assigned to you on [JournalDate Stamp]

The original due date of the task was [JournalFollowUp]

Task Description:
[JournalDescription]

[Click Here](#) to open the associated incident and mark the task as Actioned.

Remind a user that an action assigned to them for a risk is overdue

This example monitors the Action subform in a Risk Register, and reminds a user when an action assigned to them has become overdue. The following is the subform in question:

Action Plan								
Add Action								
	Action Assigned Date	Action By Date	Action Description	Allocated To	Allocated To (Username)	Completed On	Action Response	
	25 Jan 2017	08 Feb 2017	Provide additional signage around the facility on the importance of handwashing	Sally Kruger (sallyk)	sallyk			

Conditions

Given the available fields in this subform, we will base our conditions around the **Action By Date** field, and that the **Completed On** field is still empty:

Conditions

The focus of this alert is: Risks and Treatment/Action Select to add a related filter for: Test Conditions

Where

(Treatment/Actions)Action By Date(Periodic) Days Since >= 3

(Treatment/Actions)Completed On is empty

+

As you can see, we still favour giving the user a grace period. Also, don't forget to select the appropriate subform as your alert focus (as highlight in the screenshot).

Recipients

We have use Alert a user named in a field to add the "Allocate to" field to determine the recipient:

Recipients

Add a specific user as a recipient

Add a user who appears in the Review History for each record that triggers this alert

Alert a user named in a field

Remind the key users that the anticipated completion date for a quality activity is 14 days away, and the status of the activity is currently not set to 'completed'

Here is an example of a reminder alert that notifies users that a key date is approaching, rather than past.

Scenario

Key personnel involved	
Person #1 name	Caine, Therese (Therese Caine)
Person #2 name	Piriatinski, Boris (Boris Piriatinski)
Name of group (if applicable)	
Key dates	
Activity status	Commenced
Anticipated commencement date	
Approval by	Dunlop, Lisa (Lisa Dunlop)
Anticipated completion date	8 Feb 2017
Approval date	

We will have 3 recipients for this alert; **key person 1 & 2**, and also the person who **approved** the quality activity.

We will be testing the Activity Status field, and we will also add conditions so that the alert will only trigger 14 days before the date listed in the **Anticipated completion date** field.

Conditions

The focus of this alert is **Just Quality Activities** Select to add a related filter for **Test Conditions**

anti

Anticipated commencement date

Anticipated completion date

Anticipated outcome

Anticipated commencement date(P...

Anticipated completion date(Periodi...

Where Activity status is equal to **Commenced**

And Anticipated completion date(Periodic) Days Until <= 14

And Anticipated completion date(Periodic) Days Until >= 13

+

There are two things we are concerned with for these conditions:

- The alert should only trigger on quality activities which have a status of **Commenced**. This eliminates the chance that the alert will trigger for activities which were not accepted, or have already been completed, or are just proposed at this stage, etc.
- The way we have added the periodic date tests for the Anticipated Completion Date field will ensure the alert will only trigger 14 days before the date listed in that field.

Activity status

- Proposed
- Accepted
- Commenced
- Completed
- Not accepted
- Not completed

Recipients

We have 3 recipients to add to this alert; the users listed in the fields:

- Person #1 name
- Person #2 name, and
- Approval by

Recipients

Add a specific user as a recipient

Type a name to search

Add a user who appears in the Review History for each record that triggers this alert

Select a user category

Alert a user named in a field

Select a field that contains a Username

User(s) listed in the "Approval by" field

User(s) listed in the "Person #1 name" field

User(s) listed in the "Person #2 name" field

RESTRICTION ALERTS

Allow a user to see only records of a certain type in a register

Let's picture the following scenario: In your system, there are two users who have permission to see the Incident Inbox:

Dist	ID	Group	Date Notified	Notification Type	Who was affected	Campus	Summary	Actual Severity	Overall Severity (Act)	Primary Incident
None	349		29 Apr 2015	Clinical Incident	Health Care Recipi...	The Royal Women...	a		Unknown	Adverse outcome/...
None	348		29 Apr 2015	Clinical Incident	Health Care Recipi...	The Royal Women...	a		Unknown	Hazard-emergency...
None	347		5 Dec 2014	Non Clinical/Non O...	Health Care Recipi...	The Royal Women...	Complaint made t...			
None	334		18 Aug 2011	Non Clinical/Non O...	Health Care Recipi...	The Royal Women...	see ADR form	4	4. No Harm/Near...	Adverse outcome/...
None	327		8 Dec 2010	Clinical Incident	Health Care Recipi...	The Royal Women...	cvdff	3	3. Mild	Retained Instrument
None	326		29 Nov 2010	Clinical Incident	Health Care Recipi...	The Royal Women...	anskldj	3	3. Mild	Adverse outcome/...
None	321		22 Mar 2010	Clinical Incident	Health Care Recipi...	The Royal Women...	test	3		Bruising
None	317		30 Dec 2009	OH&S Incident	Health Care Provid...	The Royal Women...	test	3	3. Mild	Death, cause unkn...
None	316		30 Dec 2009	OH&S Incident	Non-Person	The Royal Women...	test			Air quality/smoke/...
None	313		30 Dec 2009	Non Clinical/Non O...	Non-Person	The Royal Women...	test test	4	4. No Harm/Near...	Adverse outcome/...

Now, if a user has permission to see the Inbox, then unless you place any additional restrictions on that user, then they will see **all records in the Inbox** across the entire organisation.

To further restrict what a user can see in the Inbox, you can restrict them down to a particular site via their user profile:

Restriction Details (All restrictions in this section are shared between all modules.)

No Restrictions in this area have any selected items.

Entry/Update Restrictions

Site Restriction: (circled in red)

Location Restriction:

Reporting Restrictions

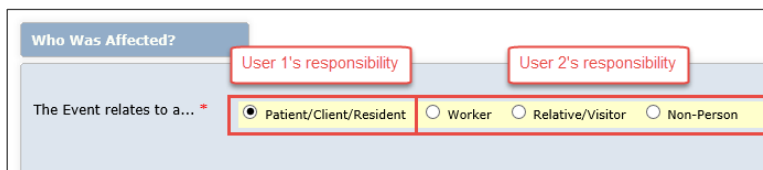
Site Restriction:

Location Restriction:

Alert Examples Supplement

Adding the site restriction shown above will allow a user only to see incidents from **Base Hospital** in the Inbox. But what if this is not granular enough?

Suppose the responsibility for posting incidents was divided between two users: one user who is responsible for posting all the patient related



The screenshot shows a section titled "Who Was Affected?". Below the title, there are two red boxes: "User 1's responsibility" and "User 2's responsibility". Underneath, the text "The Event relates to a..." is followed by four radio button options: "Patient/Client/Resident" (which is selected), "Worker", "Relative/Visitor", and "Non-Person".

incidents; and the other, responsible for posting all other incidents, including WHS, non-person, etc.

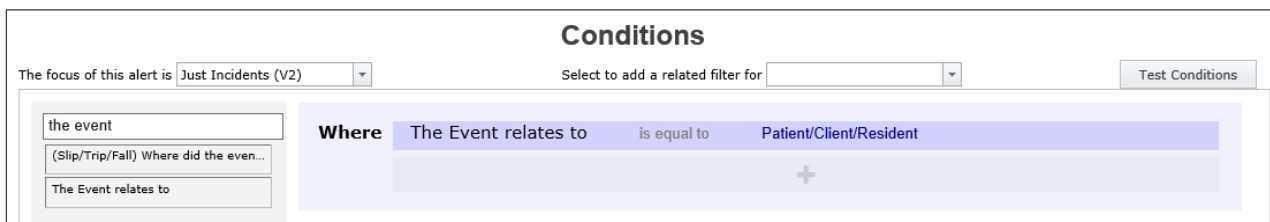
The good news is that you can further restrict the records that a user can see using alerts (also, note that this same technique applies to any register accessed via the Management menu).

Part 1: Create the requisite alerts

In our example we will need to have 2 alerts configured; one for each user.

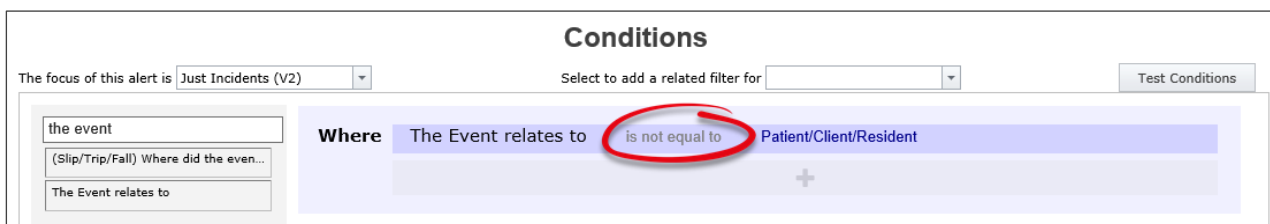
Conditions

The first alert, for the user who needs to work with patient incidents, will have the following:



The screenshot shows the "Conditions" configuration for an alert. The focus is "Just Incidents (V2)". The condition is set to "Where The Event relates to is equal to Patient/Client/Resident".

The second alert will be the opposite:



The screenshot shows the "Conditions" configuration for an alert. The focus is "Just Incidents (V2)". The condition is set to "Where The Event relates to is not equal to Patient/Client/Resident". The text "is not equal to" is circled in red.

Part 2: Apply additional restriction to each user's profile

The second step involves applying an additional setting to each user's profile. Load the profile, choose (in this case) the **Incident tab**, and scroll down to the **Specific Restrictions** section:

Specific Restrictions (Restrictions in this section are specific to the register.)

Entry/Update Restrictions

Show only "Alerted" Incident (V2) items in Inbox. ?

The Event relates to Restriction:

Patient/Client/Resident
 Worker
 Relative/Visitor
 Non-Person

Reporting Restrictions

Show only "Alerted" Incident (V2) items in Reports. ?

The Event relates to Restriction:

Patient/Client/Resident
 Worker
 Relative/Visitor
 Non-Person

Restrict to these Reports:

(Sub-Report) Journal
 (Sub-Report) Medication
 (Sub-Report) Pressure Injury
 (Sub-Report) Preventative Corrective Actions

Restrict to these Journal Types:

General Comments
 Task
 Further Action
 Internal Notification

Enabling the two options shown above will ensure the users can only see incidents in the Inbox that their respective alert has given them permission to see. This setting overrides all other methods of defining what a user can see.

THRESHOLD ALERTS

Threshold alerts count the number of occurrences of records of your chosen type. If the number of occurrences of that type of record exceeds the limit you designate during a time frame that you stipulate, then your nominated user(s) can be informed of that with these alerts.

These alerts are often used in conjunction with Indicators. Indicators can be setup to do the same thing, however we can consider having to go and run the indicator set to be “passive” – meaning if the user does not run the indicator set, they might never know that a threshold (or tolerance) has been exceeded. Therefore, for select situations, it could be advantageous to use threshold alerts to monitor certain things, as this “active” means of monitoring means the users will be informed as soon as the threshold has been exceeded.

When creating a threshold alert, in the **Rules** section, you must select the **Alert Method** of **Trigger the alert once a threshold has been exceeded**. This will then expose the threshold options in the **Settings** section:

Rules

If you need further information, please refer to the Alert Management Guide in the help menu. If you encounter difficulties or errors, please contact RiskMan Support.

Alert Method

This setting determines when the items should be checked, and thus the alert triggered. Click the setting you want to use to select it.

- Check each item when it is saved. When the user enters a new item, or when an existing item is modified, the alert will run, and trigger if all the conditions are met. This is the most common method.
- Scan all items periodically. The alert scans all items at the interval you specify (eg. Every 5 days), and triggers for each item that matches the conditions you specify. Usually used when you are creating a 'reminder' alert.
- Trigger the alert once a threshold has been exceeded. The alert will monitor for the type of item that you specify, but will not trigger until the count of that type of item has exceeded your pre-determined threshold within a given timeframe.

Settings

Should this alert be triggered as soon as an item is entered, or should it only trigger once there is a posted version?

- Trigger on the unposted record
- Wait until there is a posted version before triggering

What should this alert do regarding access permissions to the item for each recipient.

- AUTHORISE access
- DENY access
- REVOKE ALERTED access
- REVOKE ALL access
- Remove DENY access
- NONE

Number of days in the threshold timeframe: 7

Maximum number of matching items in the timeframe: 5

The alert will trigger if there are more than 5 matching items in any 7 day period.

Maximum number of emails to send per day when the threshold is exceeded: 3

What date field should the alert monitor?: [dropdown menu]

These checks will occur each time an item is entered that meets the specified conditions.

The last two settings control the following:

Maximum number of emails to send per day when the threshold is exceeded: On the day when the threshold is first exceeded, an email will be sent to the recipients. However, if another (incident) is entered on the same day that matches the alert conditions, do you want yet another email to be sent on the same day? Or is once per day enough? Most users tend to set this setting to 1.

What date field should the alert monitor: You must stipulate which date field from the register in question that the system should use to monitor and count occurrences.

If there are more than 4 manual handling incidents in a 21 day period at a given facility, notify a particular user

Threshold Settings

Number of days in the threshold timeframe:	21
Maximum number of matching items in the timeframe:	4
The alert will trigger if there are <u>more</u> than 4 matching items in any 21 day period.	
Maximum number of emails to send per day when the threshold is exceeded:	2
What date field should the alert monitor?:	Incident Date
These checks will occur each time an item is entered that meets the specified conditions.	

Conditions

Conditions

The focus of this alert is **Incidents (V2) and Type O**

Select to add a related filter for

Where (Multiselect)Type Of Event is equal to Worker --> OHS --> Manual Handling (W)

And Site is equal to Base Hospital

Test Conditions

Start typing a field name here

- (Exposure) Was all personal pro...
- (AAC) Problem
- (AAC) Process
- (ADR) Comments
- (ADR) Contact Details (email or...
- (ADR) Date reported
- (ADR) Date Reported to SAFEVIC

In the system that we made this example, “Type of Event” is a multi-select field. Subsequently, we had to ensure we chose “Type of Event” as the alert focus, so that we could add a condition for that field.

If resident #7654321 has 3 or more falls in a 14 day period, notify the facility manager

Threshold Settings

Number of days in the threshold timeframe:	14
Maximum number of matching items in the timeframe:	2
The alert will trigger if there are <u>more</u> than 2 matching items in any 14 day period.	
Maximum number of emails to send per day when the threshold is exceeded:	1
What date field should the alert monitor?:	Incident Date
These checks will occur each time an item is entered that meets the specified conditions.	

Conditions

Conditions

The focus of this alert is Incidents (V2) and Type O

Select to add a related filter for

Test Conditions

Where (Multiselect)Type Of Event is equal to Patient/Client/Resident --> Patient Care --> Fall

And Client ID/MRNRN is equal to 7654321

client

- (Elder Abuse) Client Required A...
- (Elder Abuse) Relationship of all...
- (Patient/Client) Age
- Client ID/MRNRN
- Details - Has the pressure injur...
- Has the patient/resident/client...
- Other Details - Has the pressur...

As with the previous example, the system this alert was built in has a multi-select field for incident classification.

Please note that at present, there is no functionality in the system that allows you to stipulate that the alert should simply count based on any Client ID/MRNRN. That means that if you want to monitor multiple people, you will need to setup a separate alert for each person you wish to monitor.

Remember that the **Clone** function will save you time if this is what you need to setup.