- Alert Examples Supplement -

FOR RISKMAN VERSION 2303

Last reviewed April 2023

CONTENTS

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:

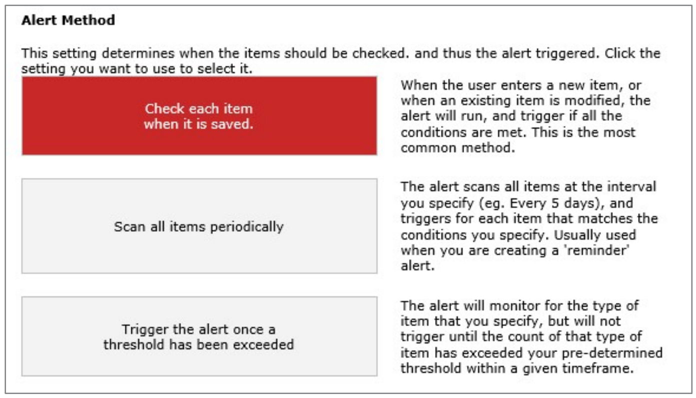
- By phone: Call the helpdesk directly on **+61 3 9686 0009**
- By email: Send your queries, along with other helpful materials to https://hub.rldatix.com/SupportHUB/s/. Please note you may need to request an account to access this service.
- If an account is needed, then please go to HUB: Sign In (rldatix.com) 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

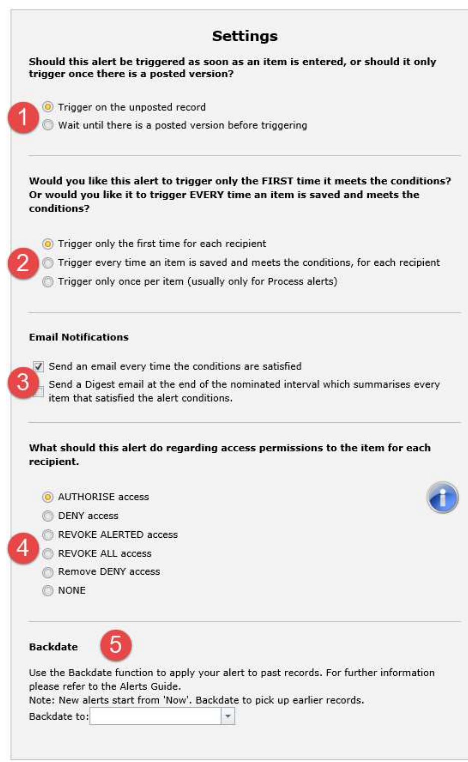


The Alert Method will <u>always</u> be *Check each item when it is saved*.

The other 2 alert methods are used specifically for

- Reminder alerts, and
- Threshold alerts

Rules > Settings



❶ 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

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

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

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

❺ 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.

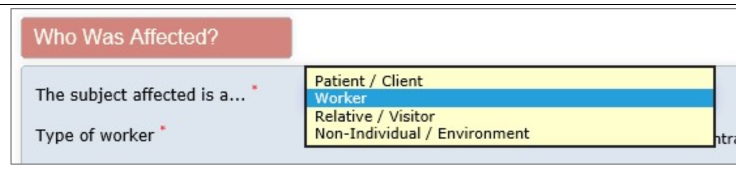
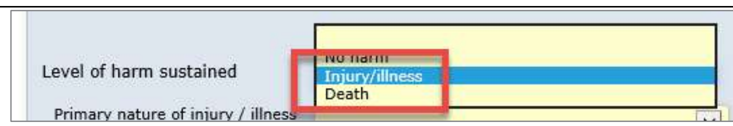
Schedule

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

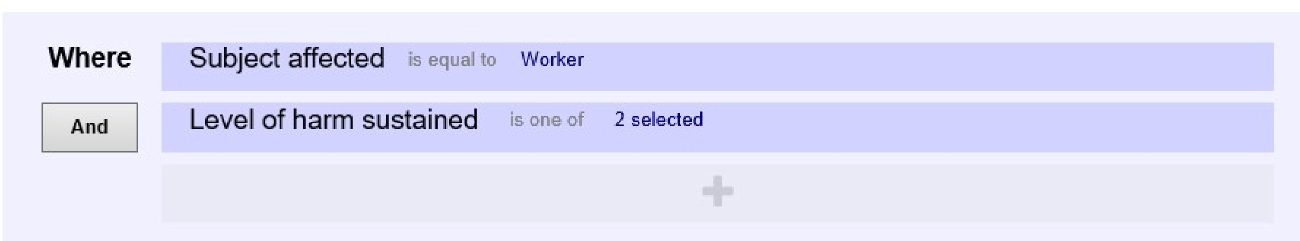
Notify the WHS manager by email when an OHS injury occurs

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:

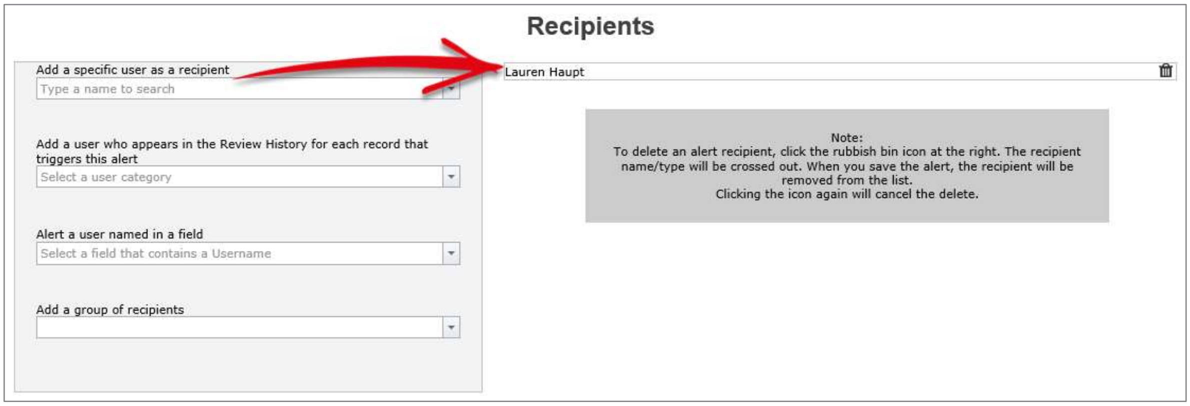
The subject affected is a… must be **Worker**	
Level of harm sustained must be either **Injury/illness** or **Death**	

Our resulting conditions look like this:

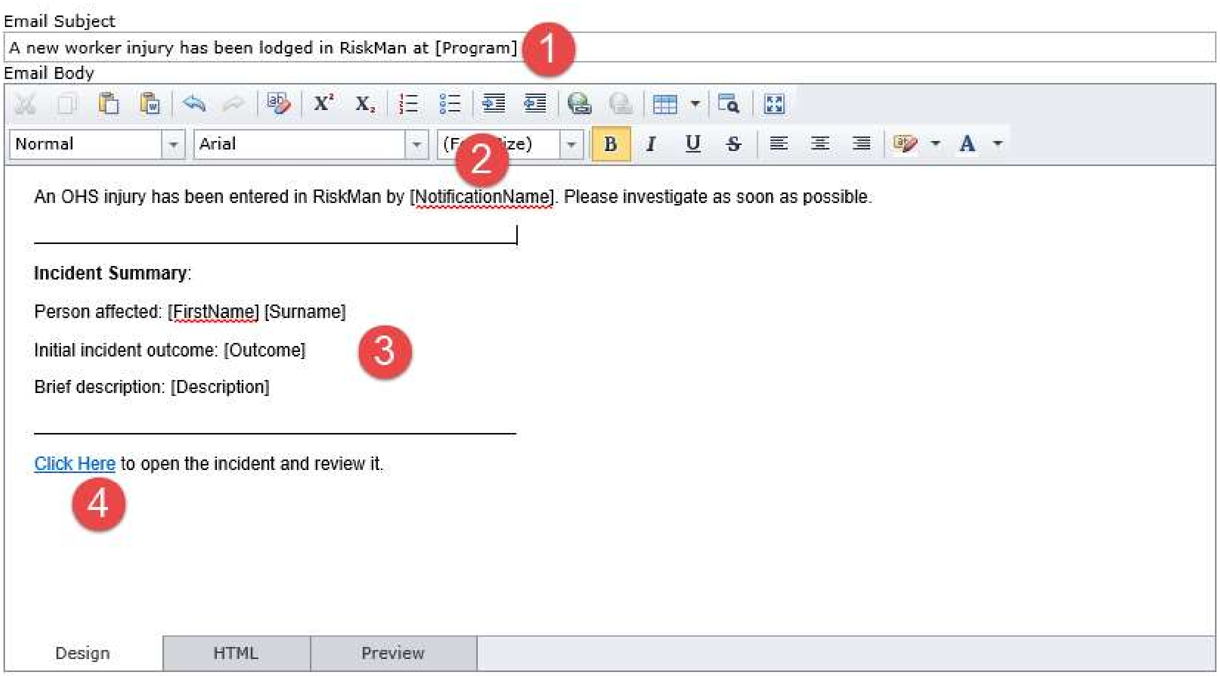


Recipients

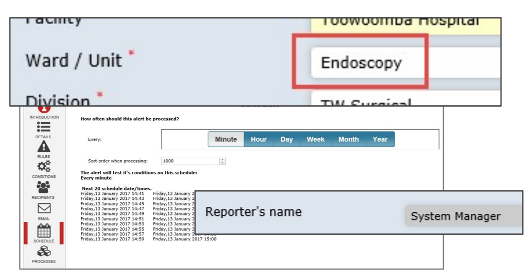
In this example, we have named a specific user. This might be the case in a single facility or other smaller scale implementation.



Email



❶ 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.



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

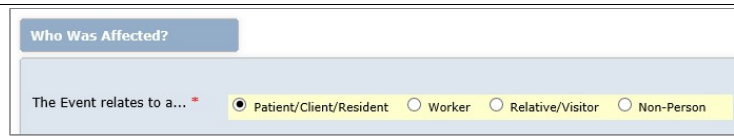
❸ In the body of the email, we have included the name of the person affected – achieved by entering the First Name and then Surname fields; the initial outcome rating of the incident, and the content of the Summary field. This is considered good practice – try not to include too much information in the 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.

❹ 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.

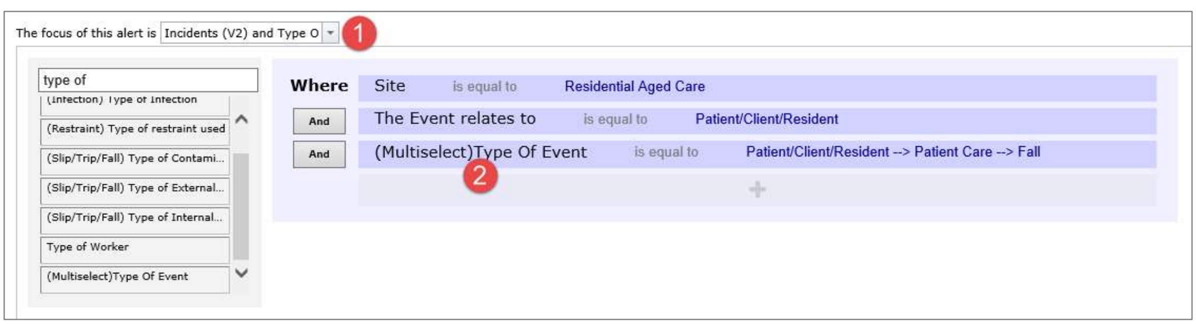
Notify falls coordinator of a new resident fall

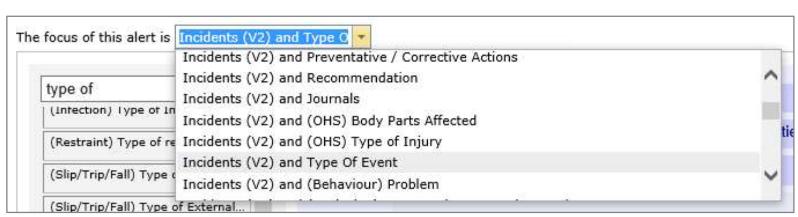
Conditions

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

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

Our resulting conditions look like this:

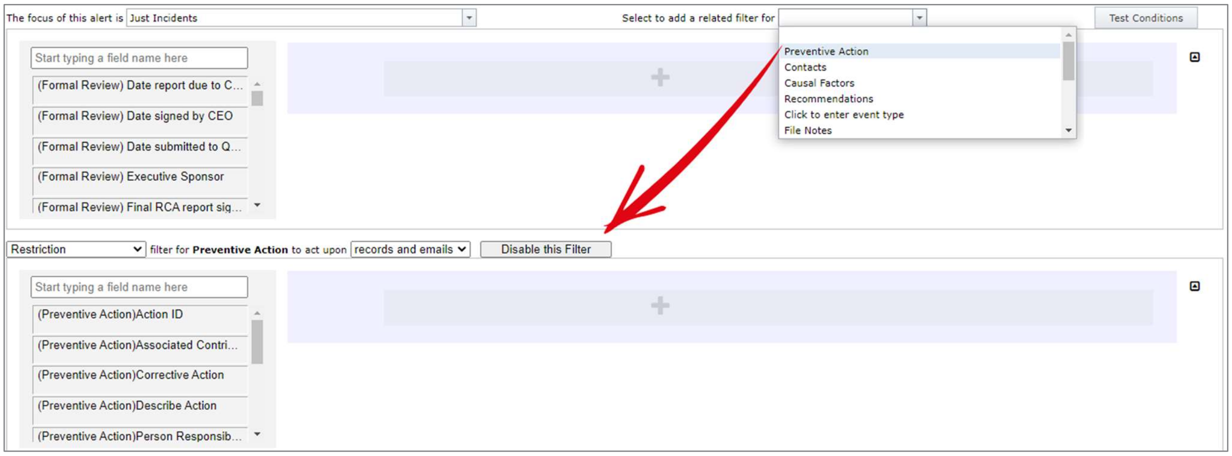




❶ Because one of the fields we needed to test was a multi-select field, we needed to select the appropriate field in the **The focus of this alert is** list.

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.

Youre 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



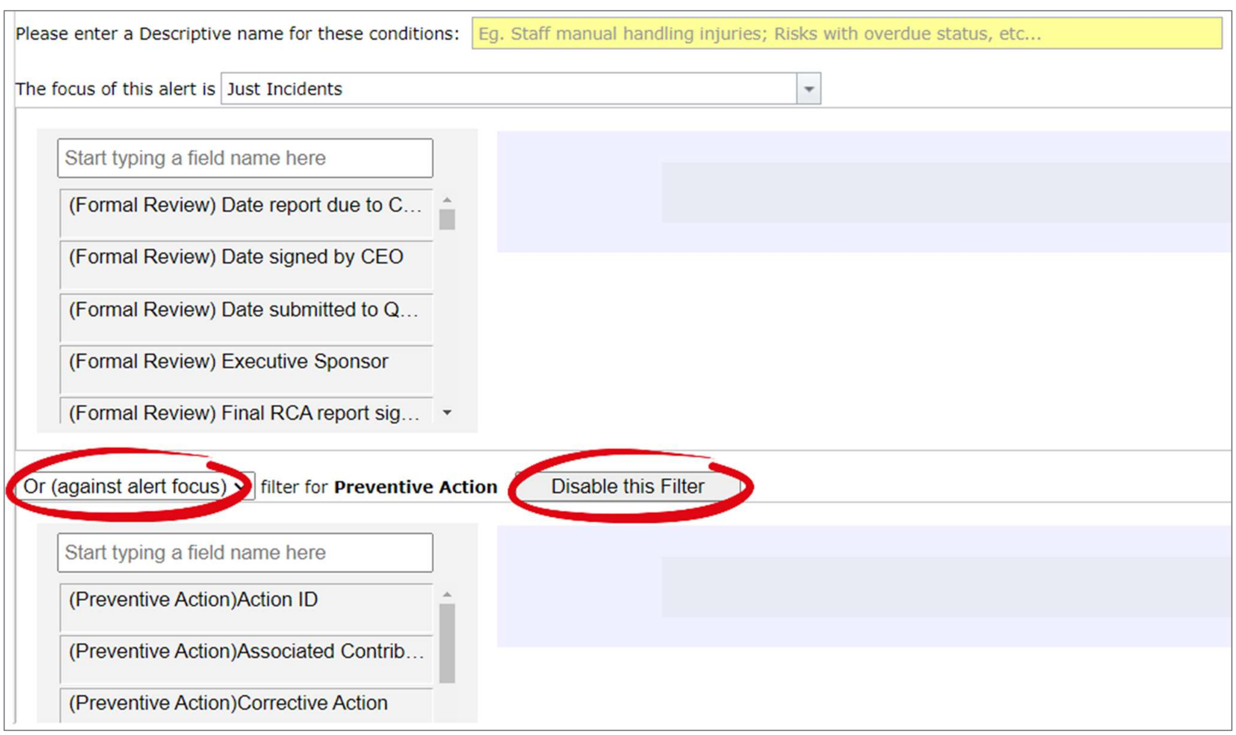
The second condition builder will need to be selected as a And, or an But not option.

Restriction: means to add or include this condition

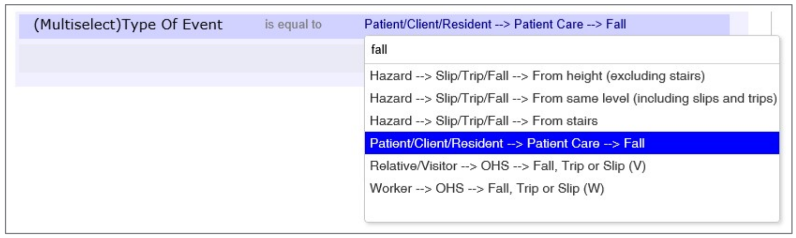
Exclusion: means to not include this condition

(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

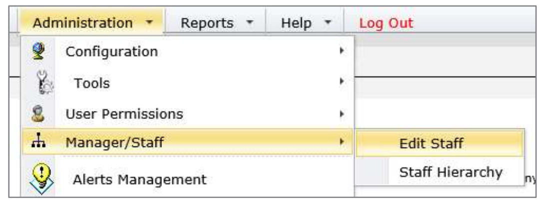


❷ You can then search for the required value you wish to test.



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

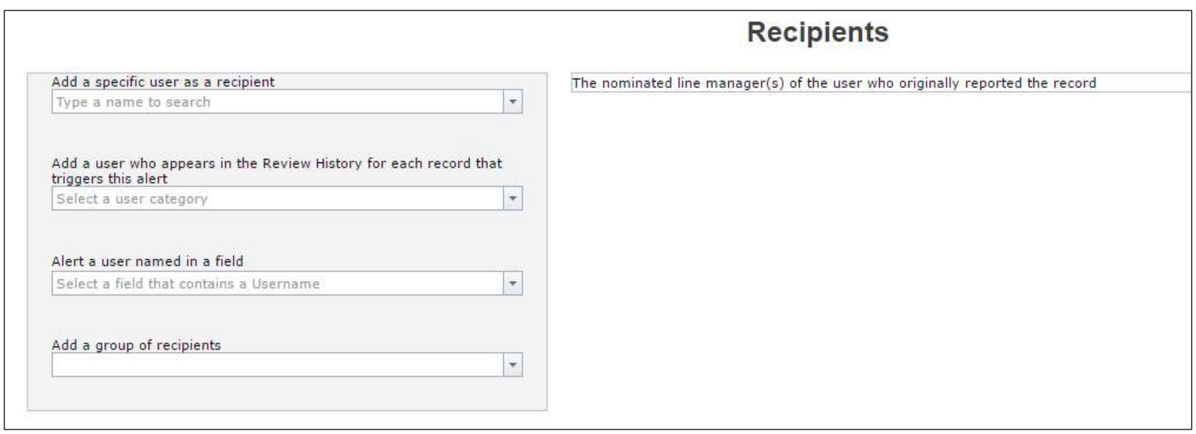
Purpose



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

Recipients

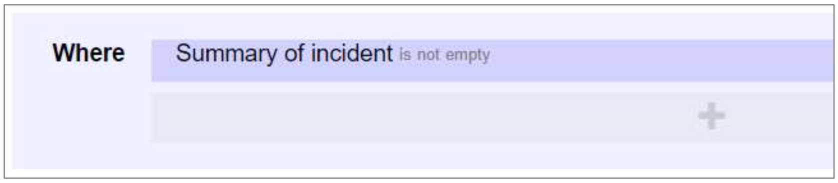
In this case, the Recipient will be set as the "Reporter's Manager":



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 <u>up</u> the reporting channel will have <u>permission</u> 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 inicidents will trigger this alert. In this case, we have chosen the **Summary** field:

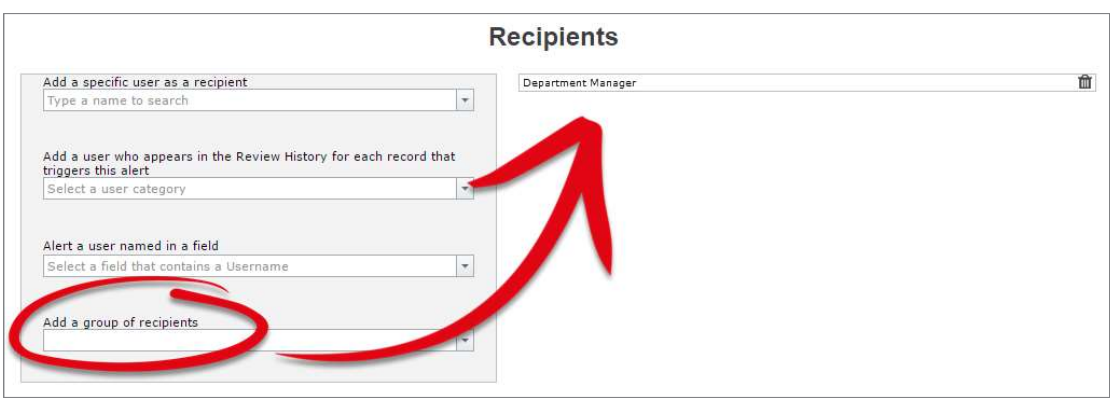


Notify a Department Manager of a new incident lodged in their department (uses Org Structure list)

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:



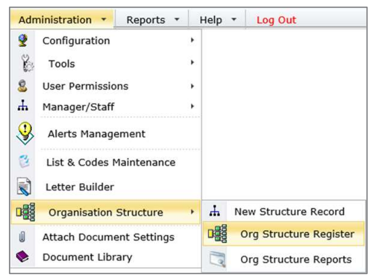
Remember that this kind of list allows you to target the responsible line manager in case a record is overdue for being followed up, or other similar situation.

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.

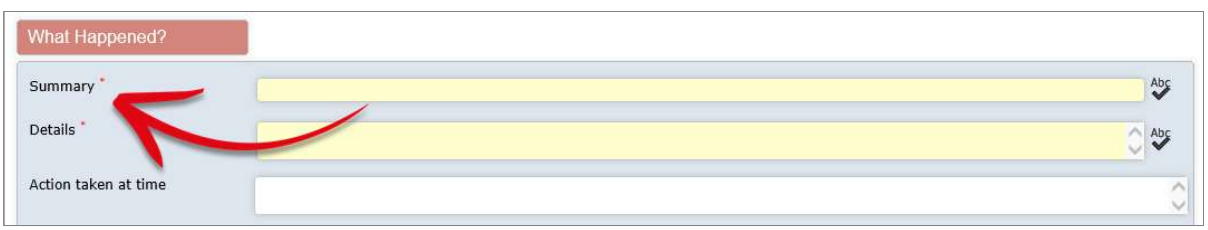
Notify a unit manager that a new incident has been lodged for their unit (uses Org Structure Register)



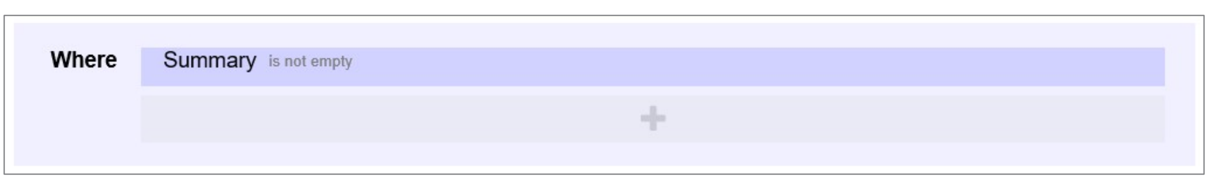
This is an example of an alert in a system that uses an Organisation Structure register in order to automatically assign the recipient.

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:

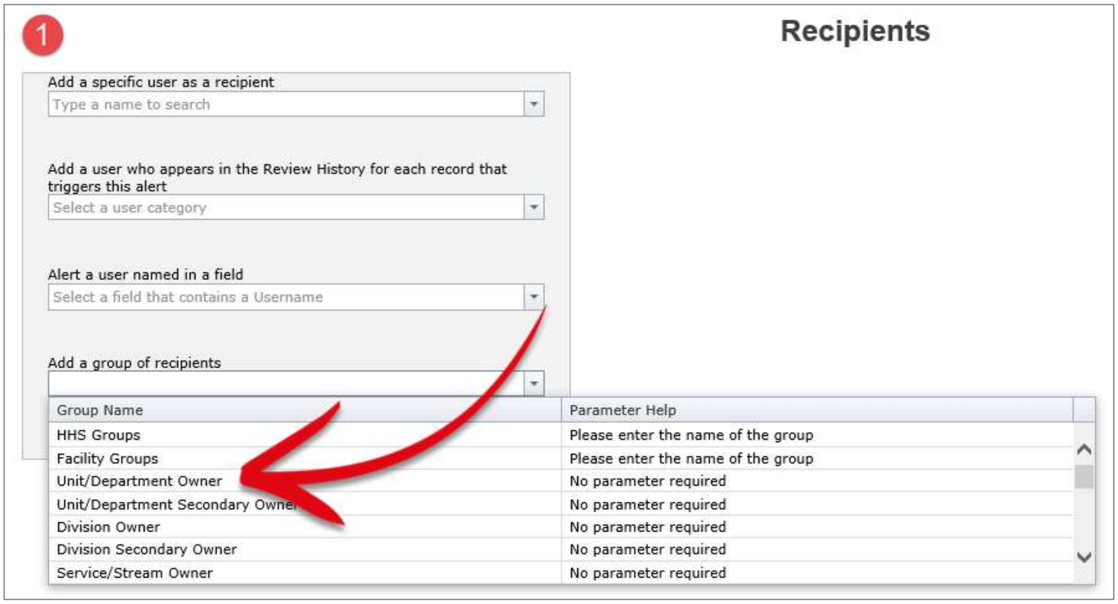


In this example system, we know that the **Summary** field is displayed for every incident, regardless of what type it is, and it is always mandatory. We will use this field as our condition to trigger the alert:

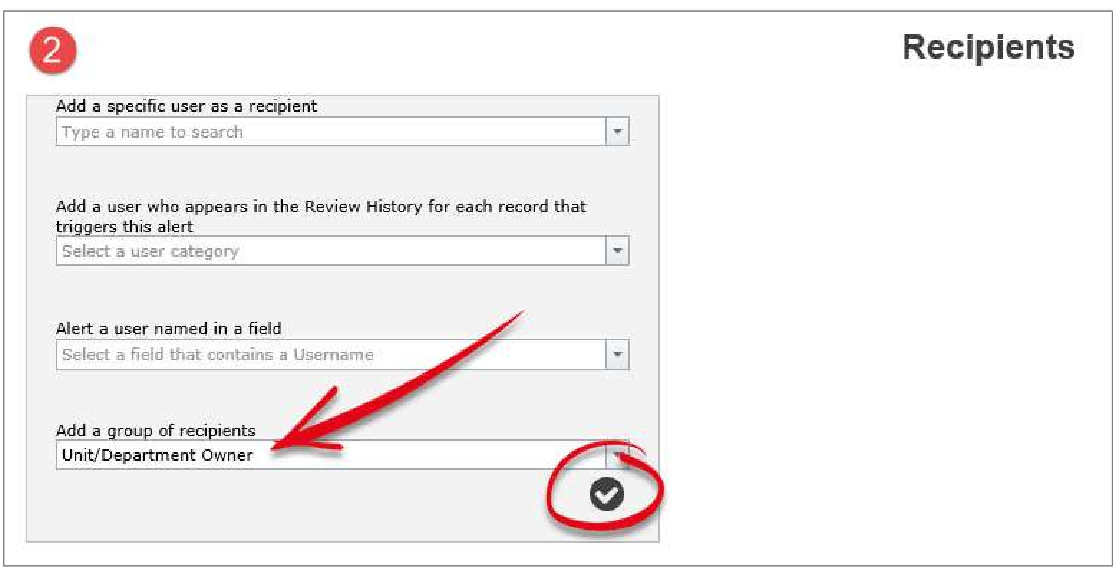


Recipient

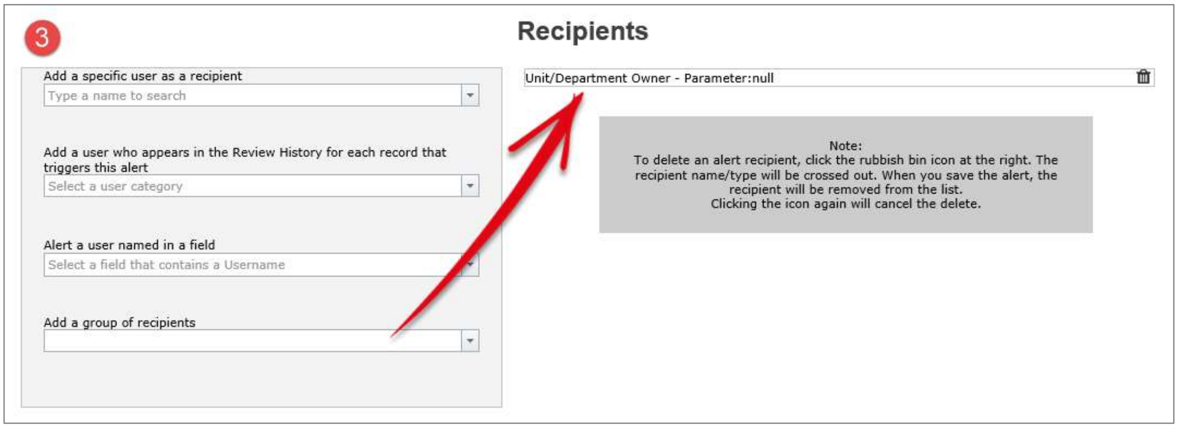
In this example, we will use the last option; Add group of recipients, and select **Unit/Department Owner**:



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:



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**.

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

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

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

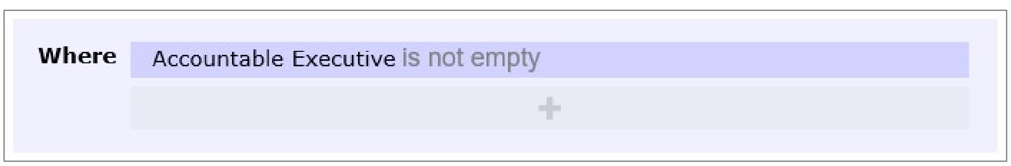
This example is the common method used to notify any user that they have been nominated as responsible for something. Although we are using the example of the executive accountable for a risk in the risk register, this is example is fairly universal and you can simply switch out the register and field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

Scenario

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

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:

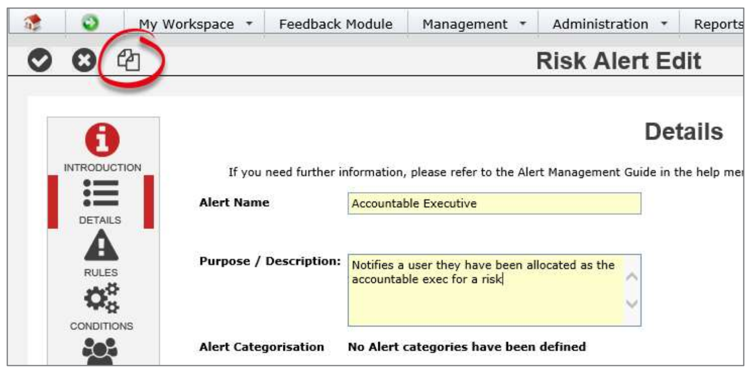


Recipient

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

Pro Tip 1: Alert Cloning

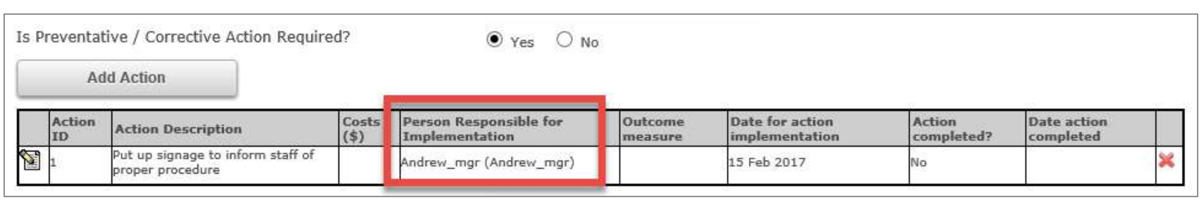
You will notice that in the example listed above, there were two fields where responsible users can be nominated; Accountable Executive, and Responsible Manager. Once you have saved the first alert, you can use the alert **Clone** button (as shown to the right here) to instantly create the alert that 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.



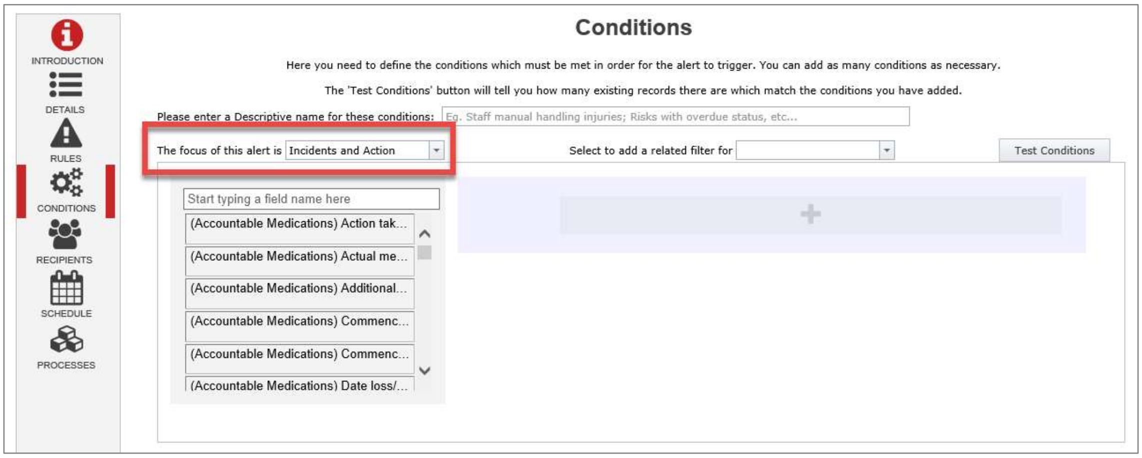
Pro Tip 2: When using this technique to notify users named in subforms

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.

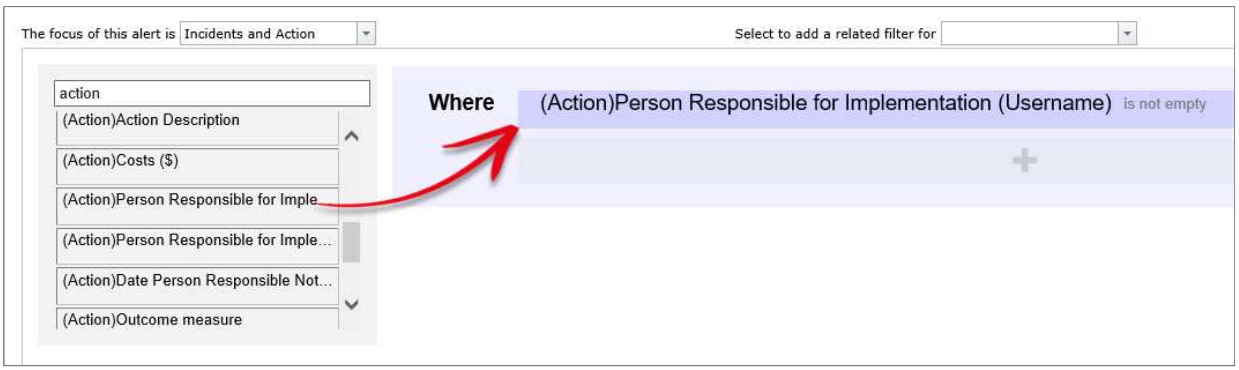
Let's suppose that we wanted to use this technique to notify a user that a preventative/corrective action has been assigned to them:



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:



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:



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

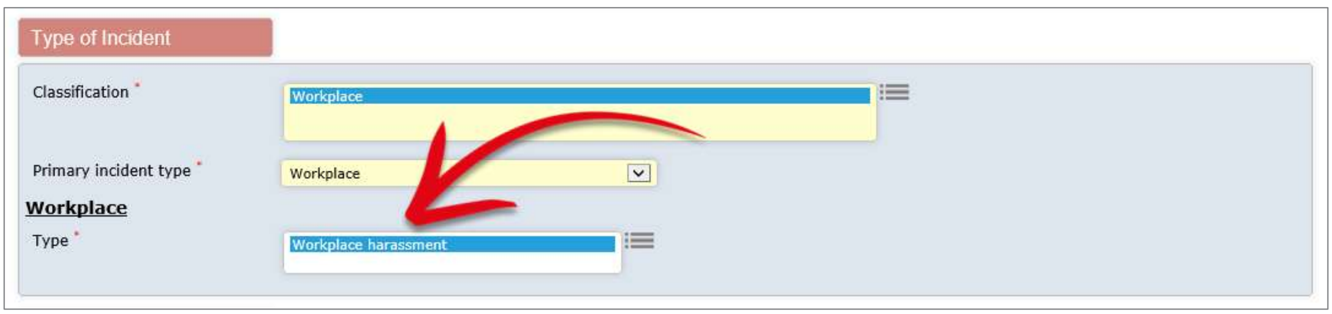
Create an exception which doesn’t sent workplace harassment incidents on to a user’s line manager; instead sends them to a certain HR user

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:

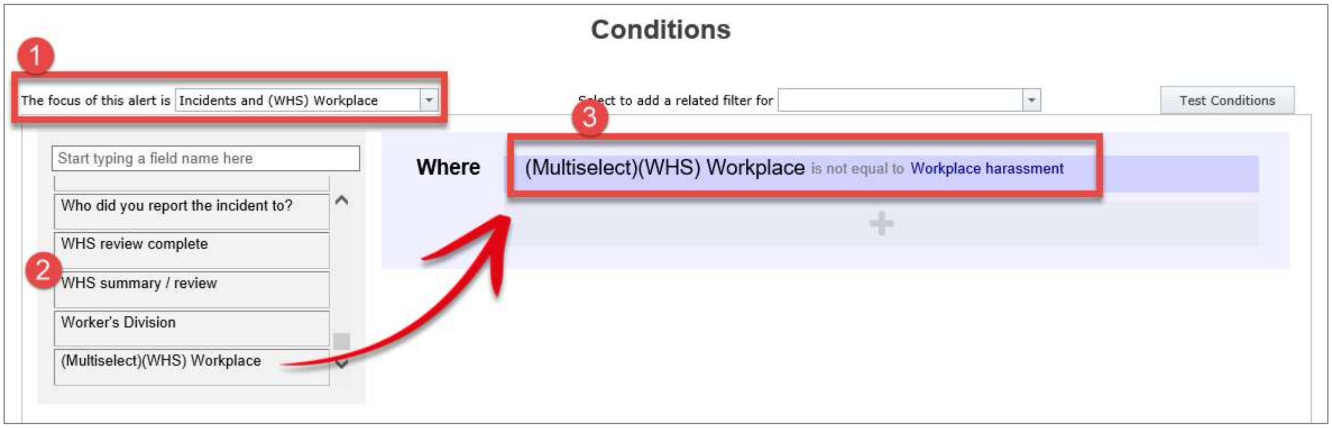


You will need to adjust the following example settings to suit your own system configuration. For example, your system might have a separate classification for workplace harassment (or similar).

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:

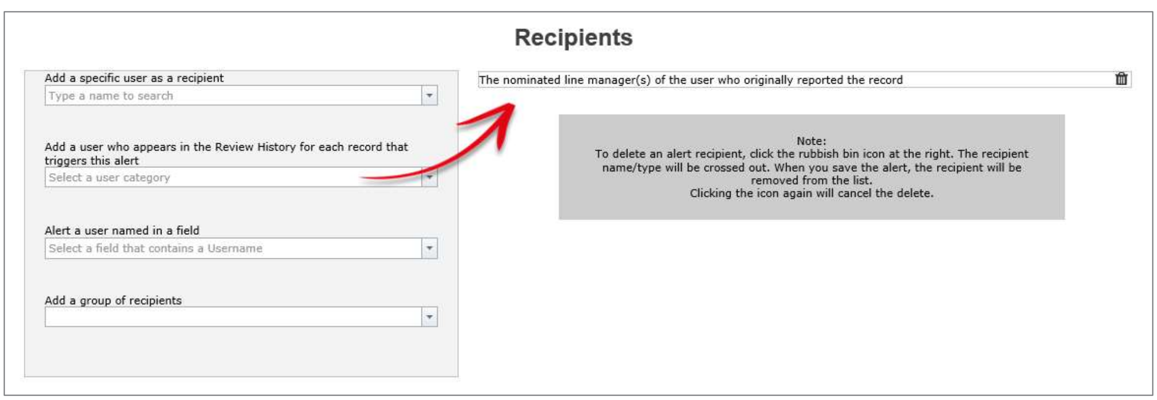


We can then see ❷ the **(WHS) Workplace** field in the list of available fields.

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

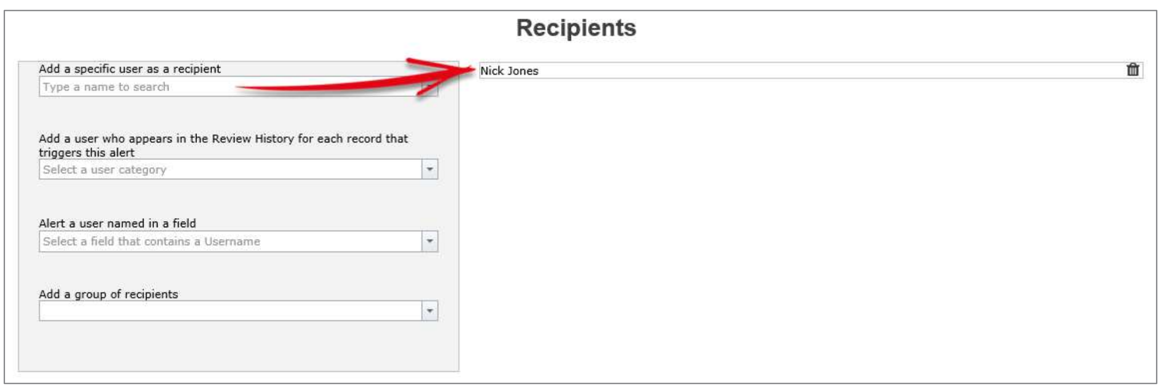
Conditions

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:

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:

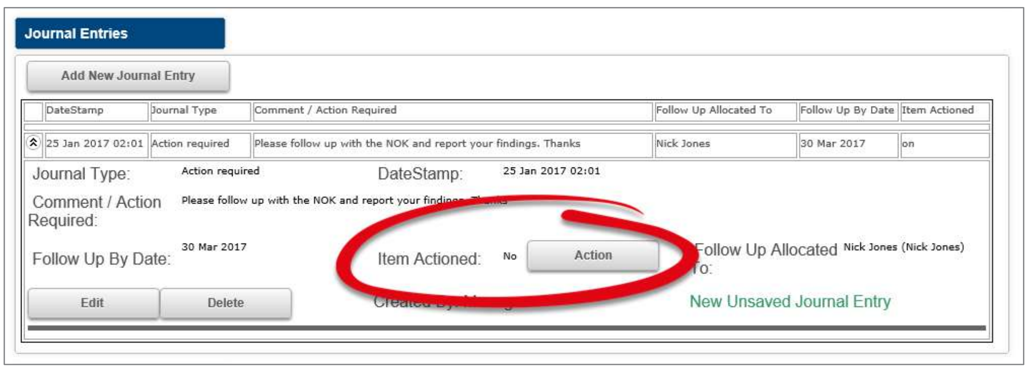


Notify a user who created a journal task that it has been marked as complete

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:

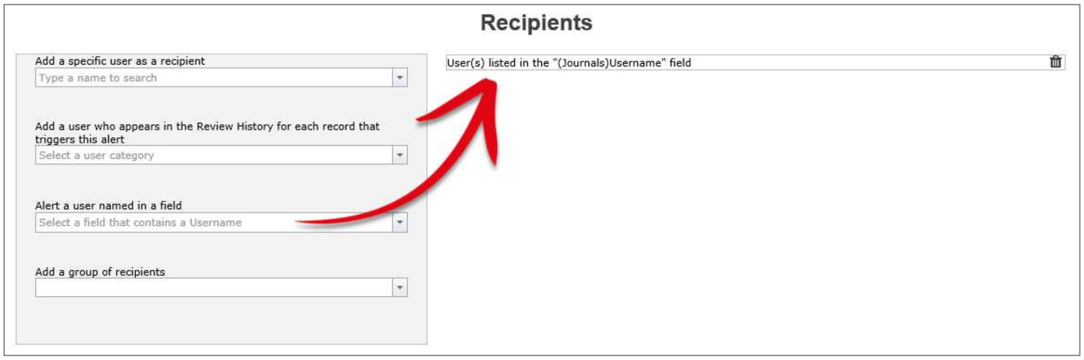


Conditions

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

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.



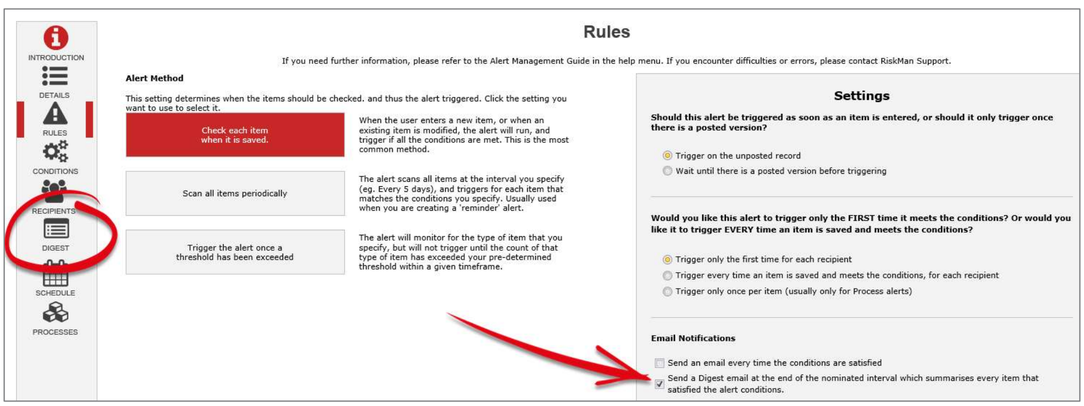
Notify the CEO of all the serious patient incidents that happened in the previous 7 days via a digest alert

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

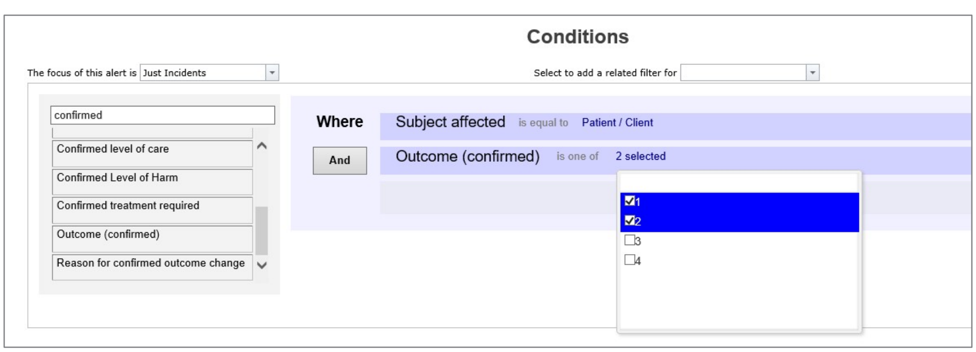
In order for the settings for a Digest Email to appear, you must have selected that you want to send a digest email in the Rules section:



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

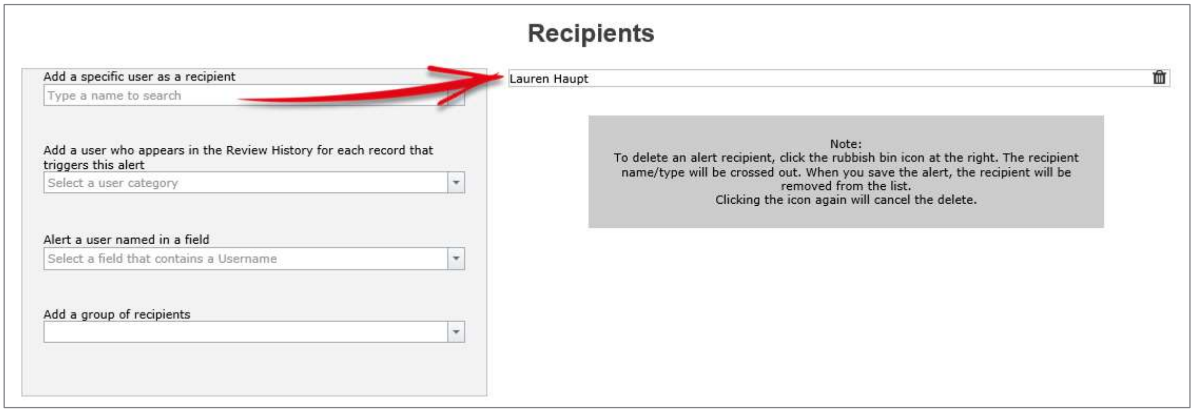
Conditions

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

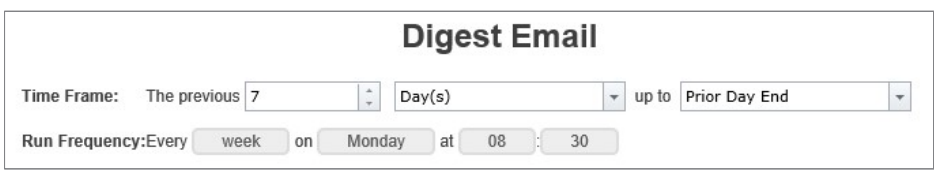
We have selected our CEO manually as the intended recipient. Remember that digest alerts will only work when you select a specific user as the recipient, as opposed to the dynamic methods.



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.

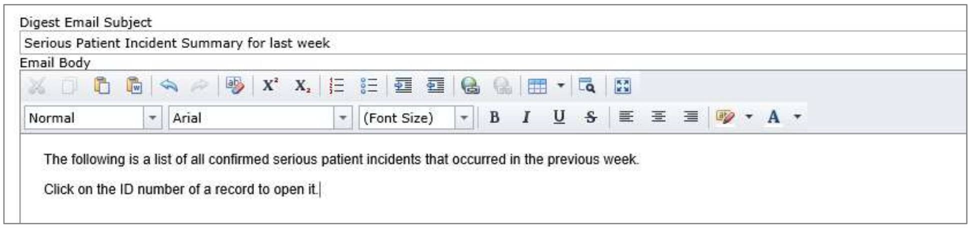
In our example, we have said that we want the digest email to be delivered every Monday morning at 8:30am, and it should include the previous 7 days from the day prior to the run date as the time frame:



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

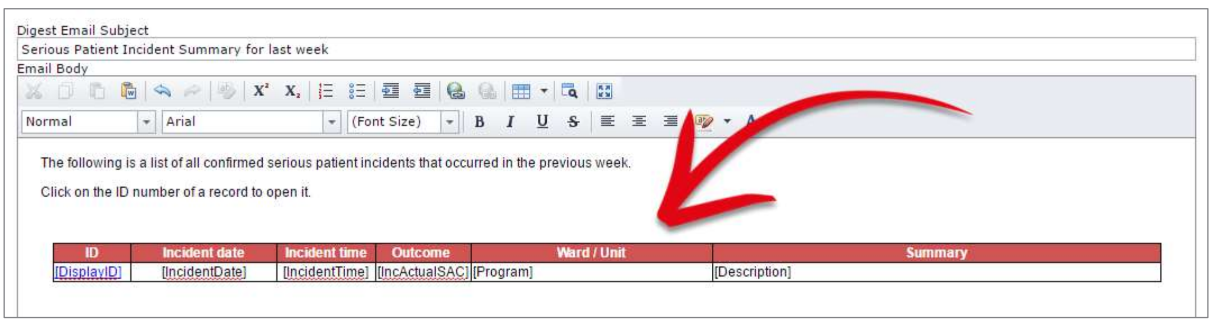
Add the static content of the email as required. Our example is as follows:



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.

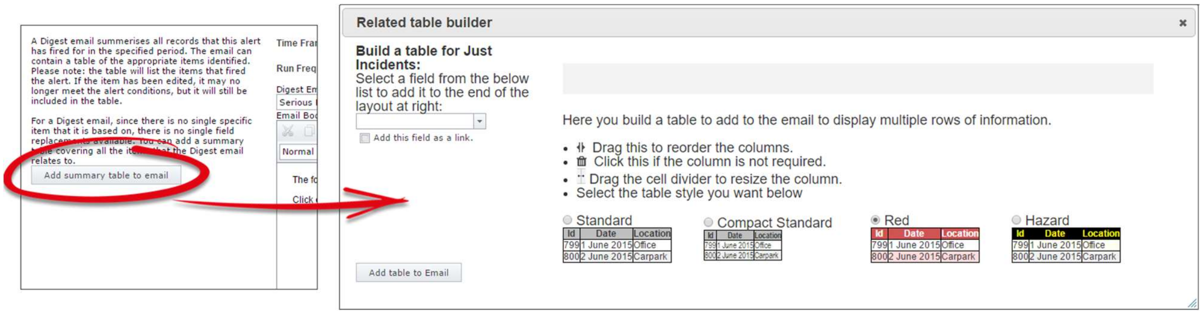
Here is what our end point looks like. We will then examine how we arrived at the end point.



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

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**:



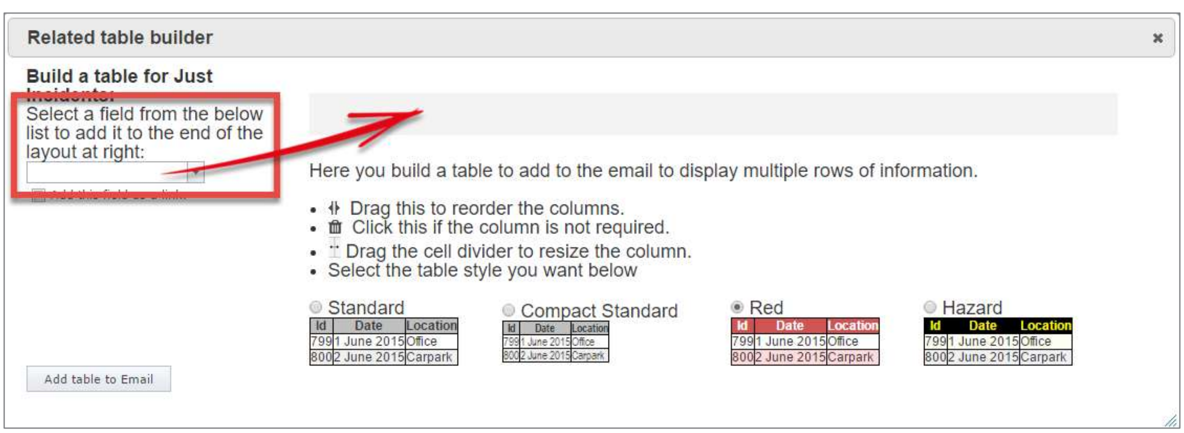
The idea of the related table builder is to:

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

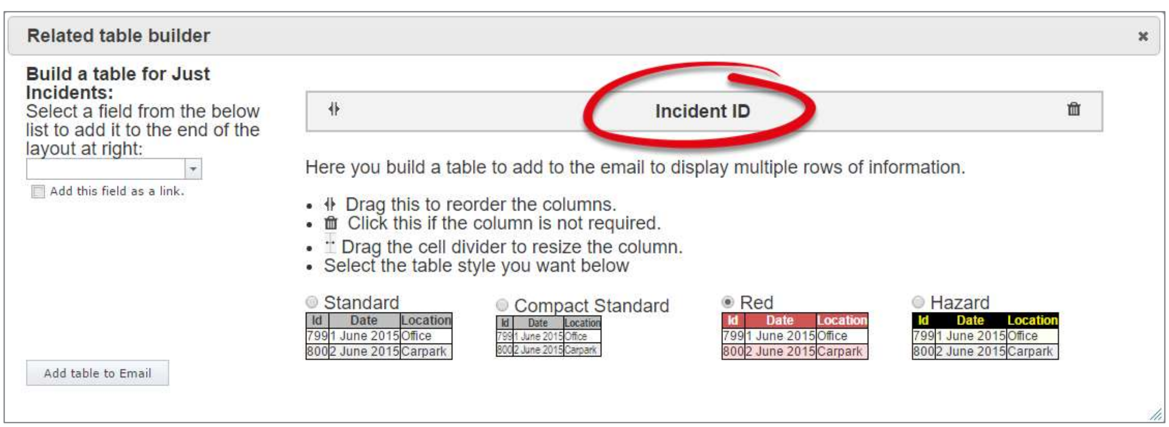
From the drop down field on the left, find each field you wish to add to the table. As you click on a field, it will be added to the table as a column header, in the grey area marked below:



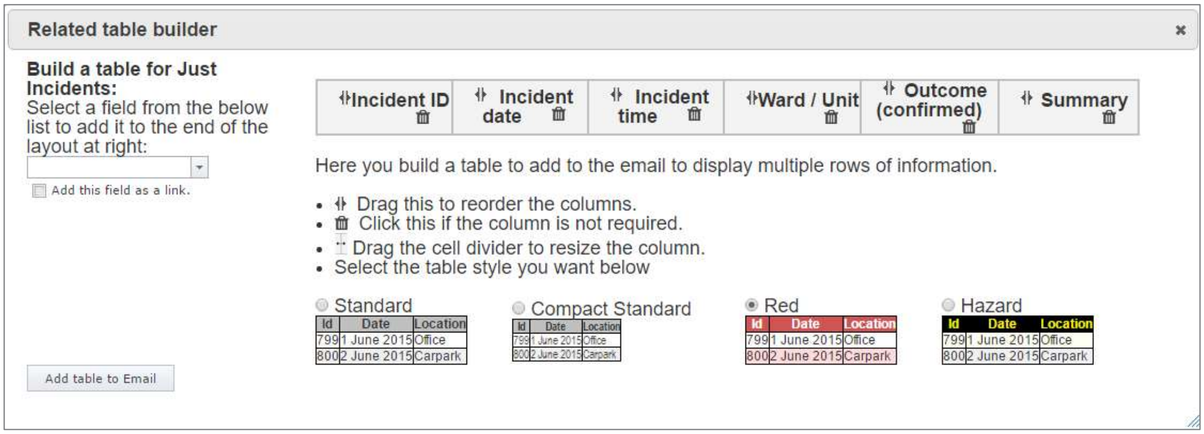
The first field we will add is **Incident ID.** Because we want Incident ID to be the clickable link to open each record in the table, **before** we add it to the table, we will ❶ select the **Add this field as a link** check box:

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

The field is added to the table column header area:



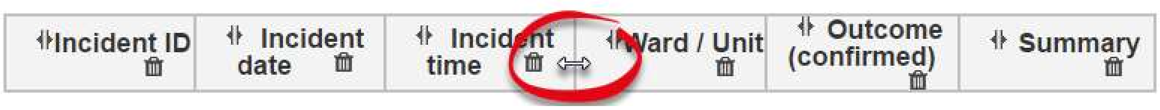
Repeat to add the other fields you wish to add as columns in your table:



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.

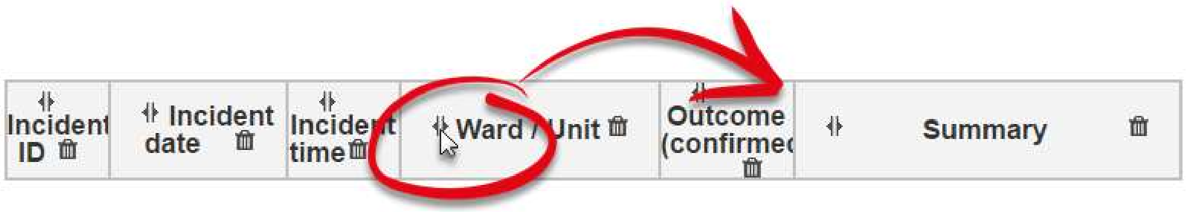
Adjust column widths, and the order in which they appear in the table

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:

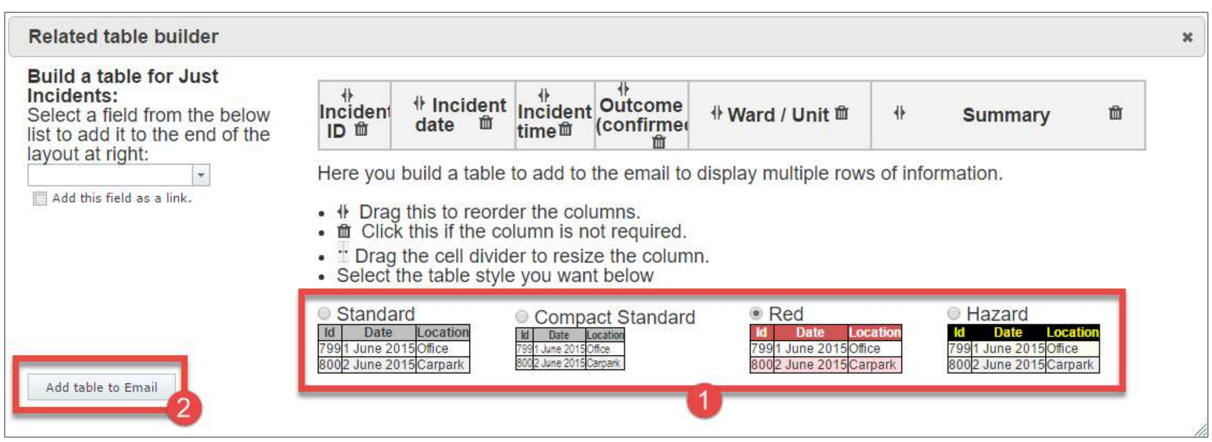
The next step to change the order of the columns as desired. To do this, click on the icon of a column header, and drag it to the desired position:

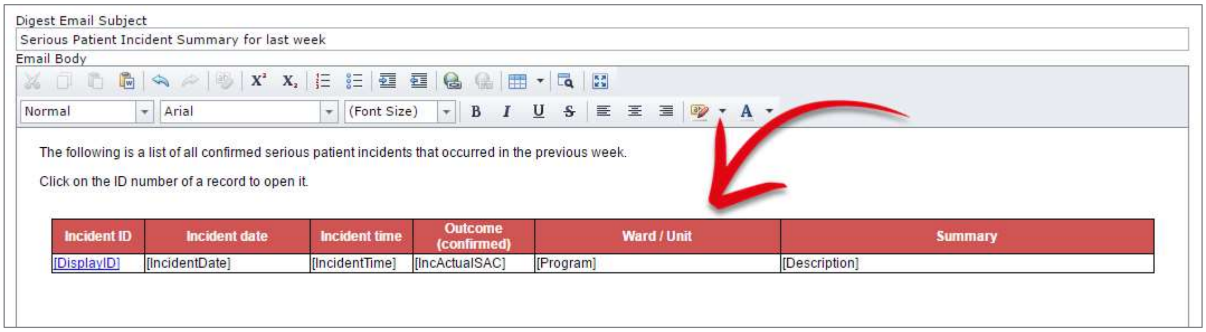


Our final column header setup is as follows:

Choose a pre-defined table format

❶ Choose from one of the table formats at the bottom of the related table builder dialogue. ❷ 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.





Apply finishing touches once you have added the table to your email body

We have decided to make the following formatting changes to our table:

Incident ID	Incident date	Incident time	Outcome (confirmed)	Ward / Unit	Summary
[DisplayID]	[IncidentDate]	[IncidentTime]	[IncActualSAC]	[Program]	[Description]
1	2	3	4		5

❶ Change the column header to just say "ID". Centre the actual display ID number, and format it as bold.

❷ Centre actual date value

❸ Centre the actual time value

❹ Change the column header to just say "Outcome". Centre the Outcome value.

❺ Format the actual summary value to be in italics.

Our finished table now looks like this:

ID	Incident date	Incident time	Outcome	Ward / Unit	Summary
[DisplayID]	[IncidentDate]	[IncidentTime]	[IncActualSAC]	[Program]	*[Description]*

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.

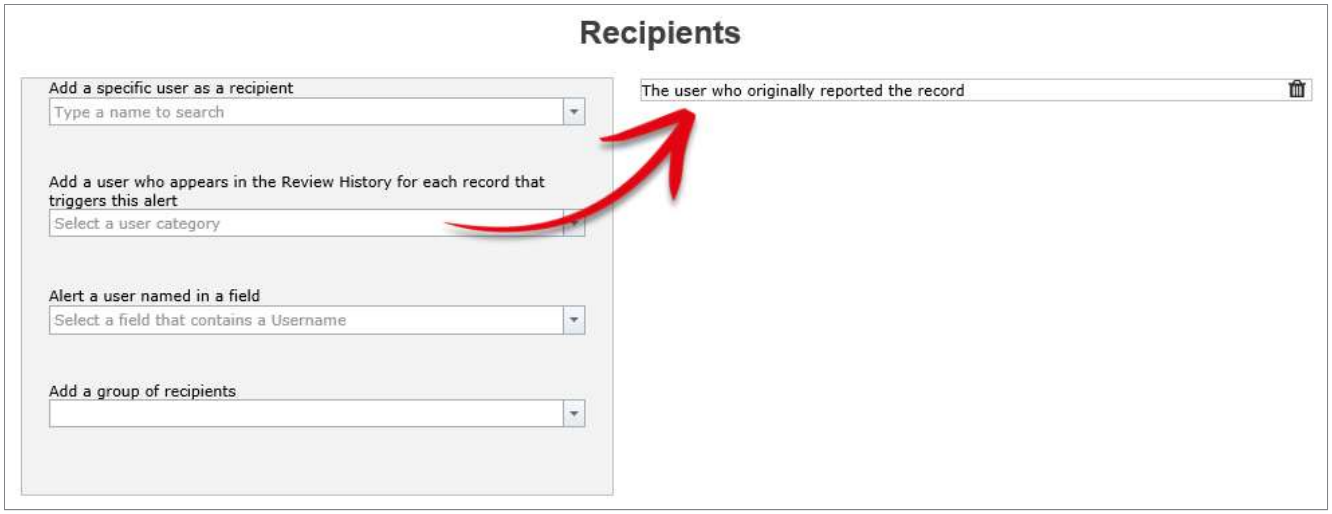
Granted, in many organisations, there may be a significant percentage of users who do not have a company email address. However, having an alert in place like this can really assist with getting buy-in with a new (or even existing) system.

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:

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

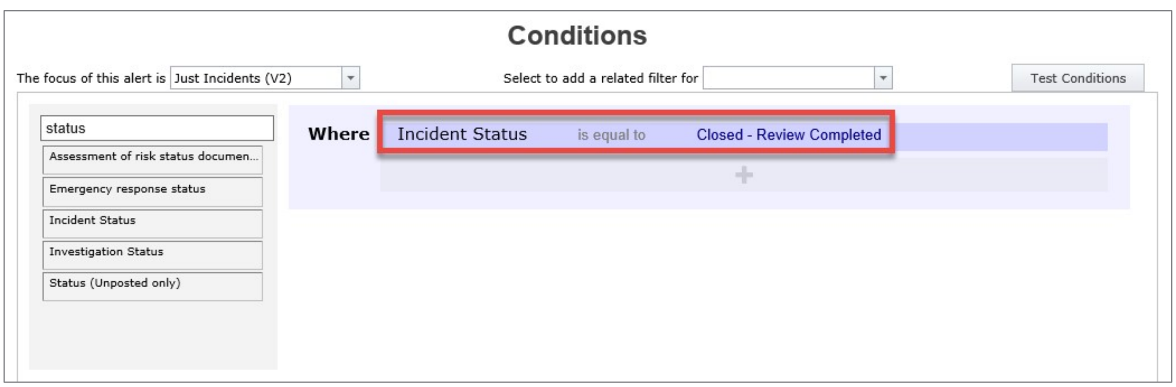
This example is obviously going to be very similar to the previous one. Again, the aim is to close the feedback loop and include the original reporter in the overall process.

Conditions

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

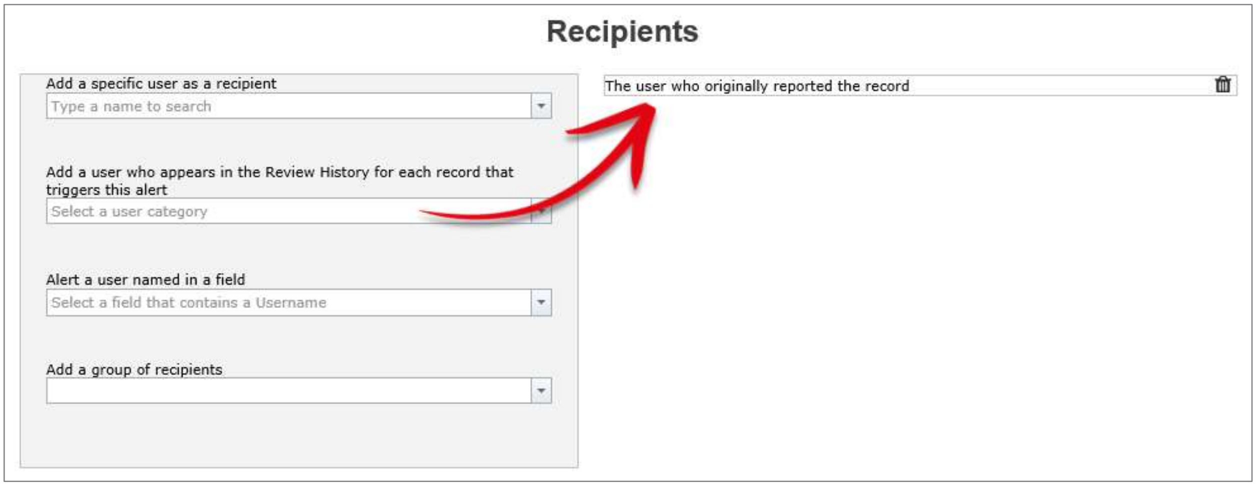
- Investigations completed date has been filled in
- Investigation status = complete
- Incident Closed on date has been filled in
- Incident status = closed

This is our example:



Recipients

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



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.

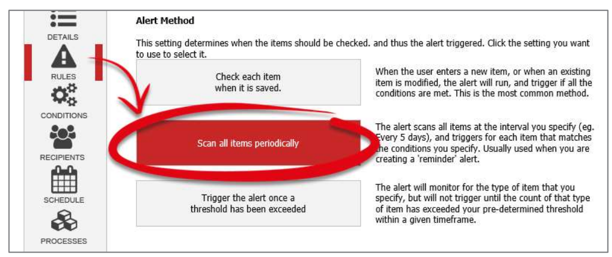
Situation

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

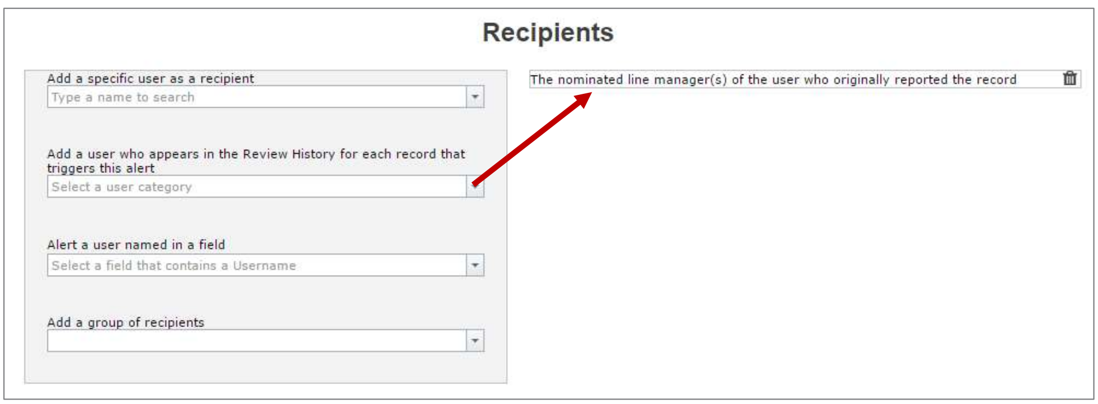
We will check if anything has been entered into the investigations/findings field. We will also check to see how long since the incident was entered - greater than 7 days, and fewer than 21 days:

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, is 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.

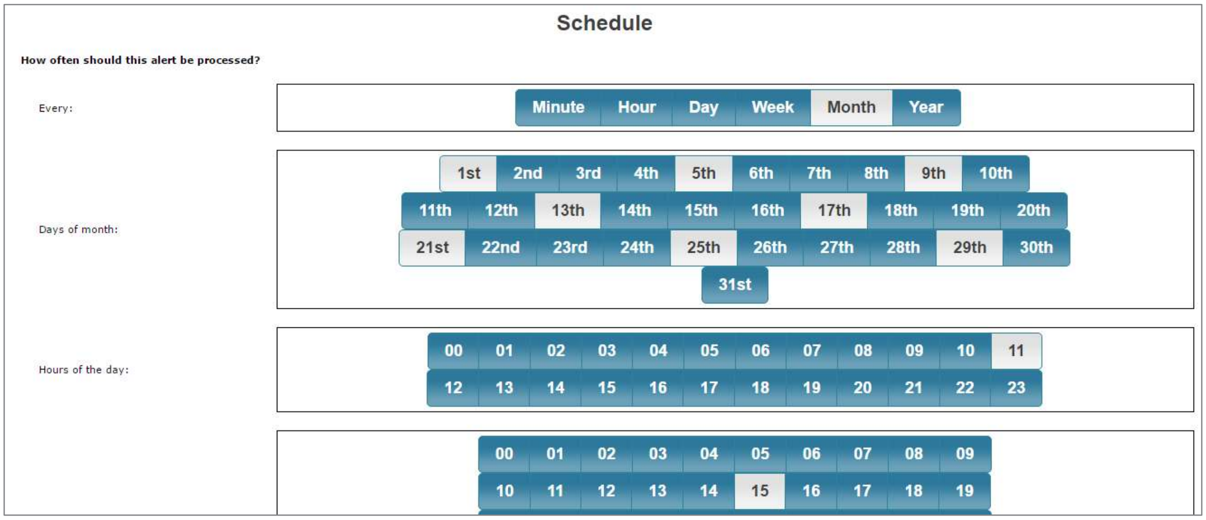
Recipients

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.



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:



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.

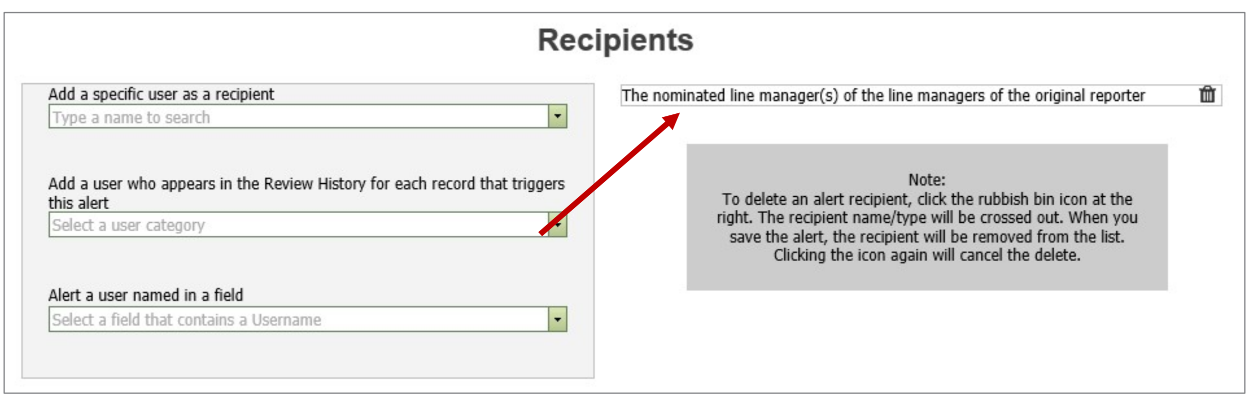
Conditions

The conditions for the escalation alert will look like this:

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.

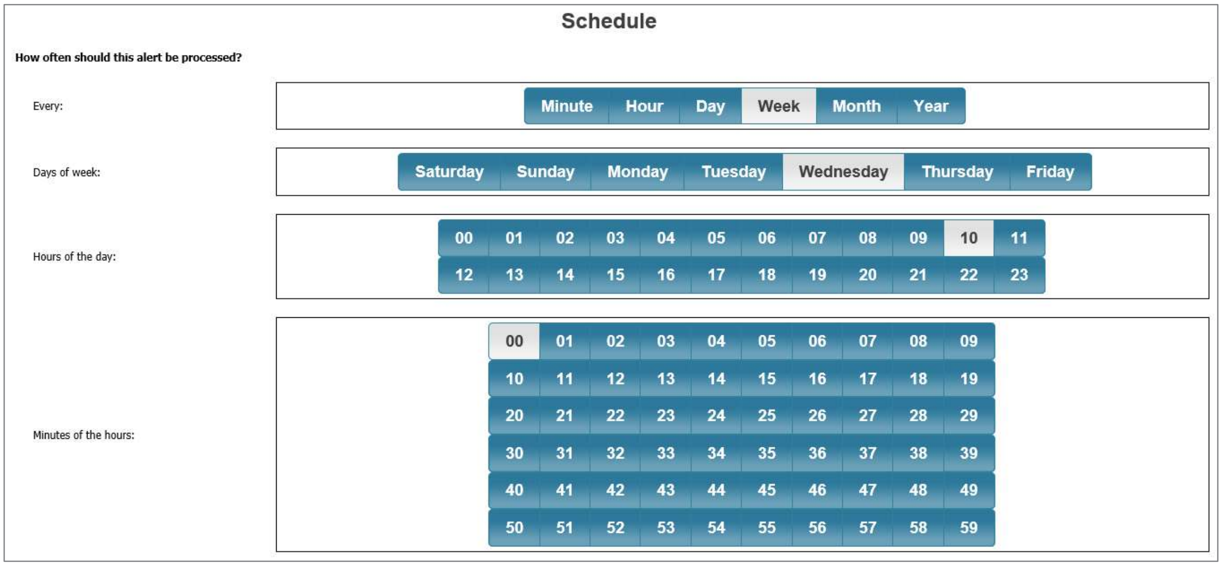
Recipient

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:



Schedule

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



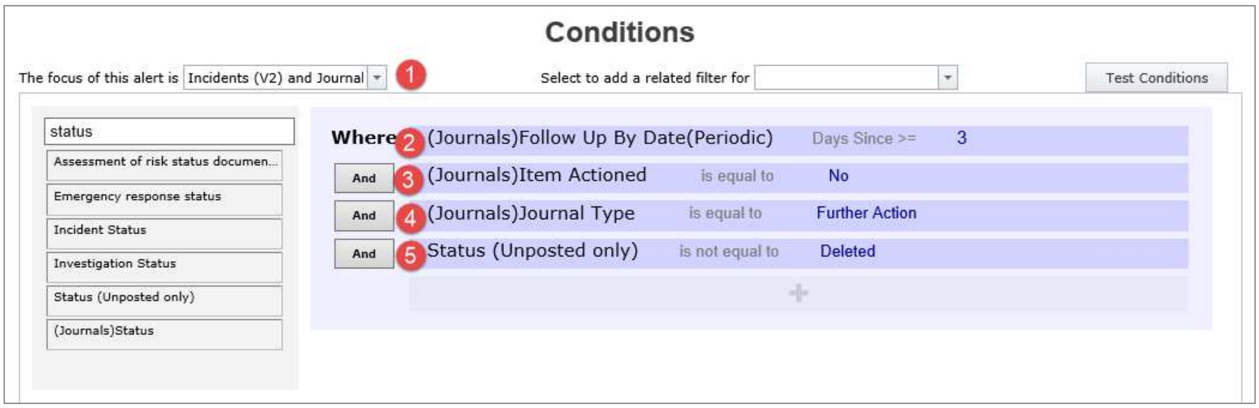
Remind a user that a journal task assigned to them is now overdue, and has not been actioned

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:



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 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:

Optional: You could also notify the user who <u>created</u> 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 <u>**overdue**</u>.

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 **[JournalDateStamp]**

The original due date of the task was **[JournalFollowUp]**

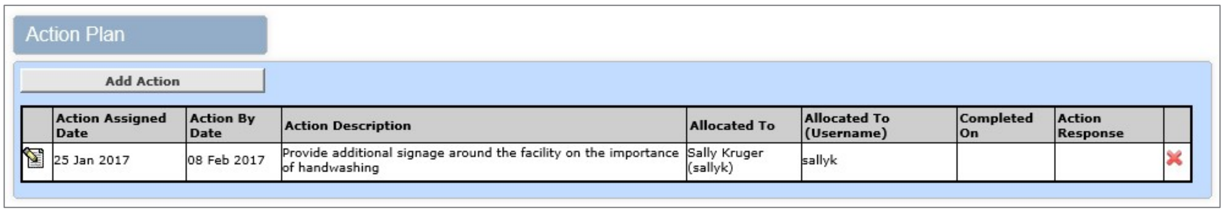
Task Description:

[JournalDescription]

<u>Click Here</u> 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:



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:

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:

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'

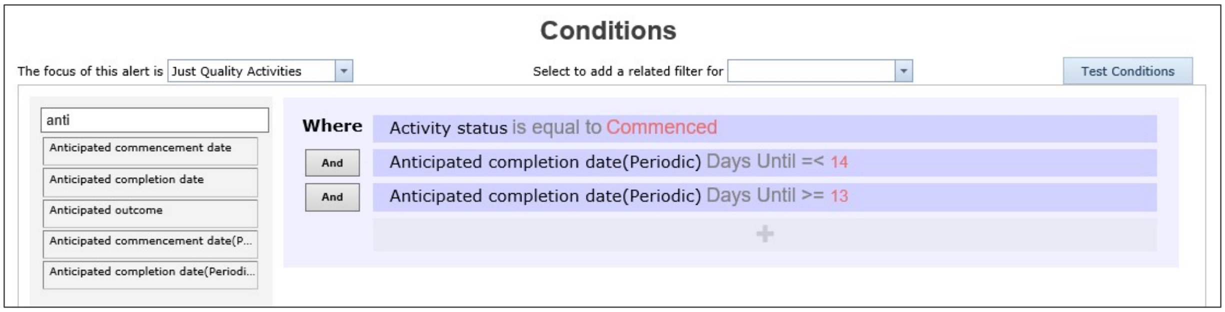
Here is an example of a reminder alert that notifies users that a key date is approaching, rather than past.

Scenario

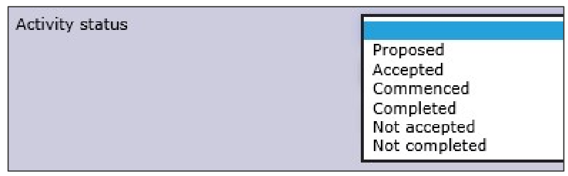
We will have 3 recipients for this alert; **key person 1 & 2**, and also the person who **approved** the quality activity.

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



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

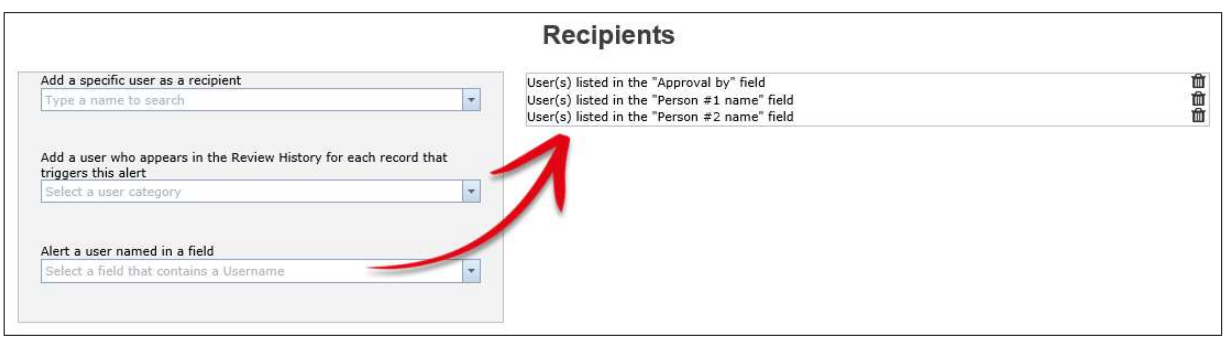


- The alert should only trigger on quality activities which have a status of **Commenced**. This eliminates the chance that the alert will trigger for activities which were not accepted, or have already been completed, or are just proposed at this stage, etc.
- The way we have added the periodic date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

Recipients

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

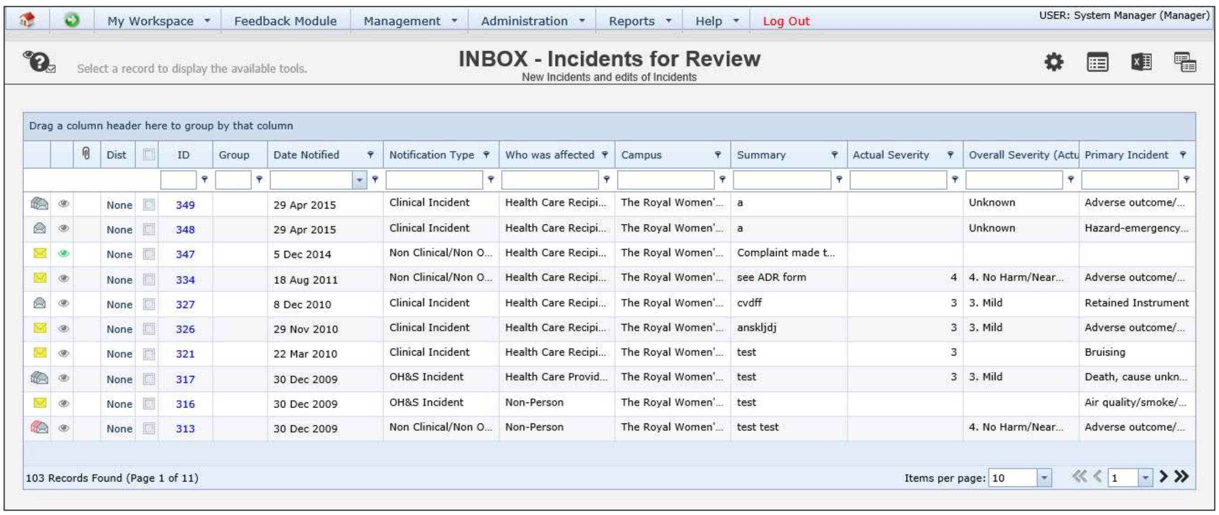
- Person #1 name
- Person #2 name, and
- Approval by



RESTRICTION ALERTS

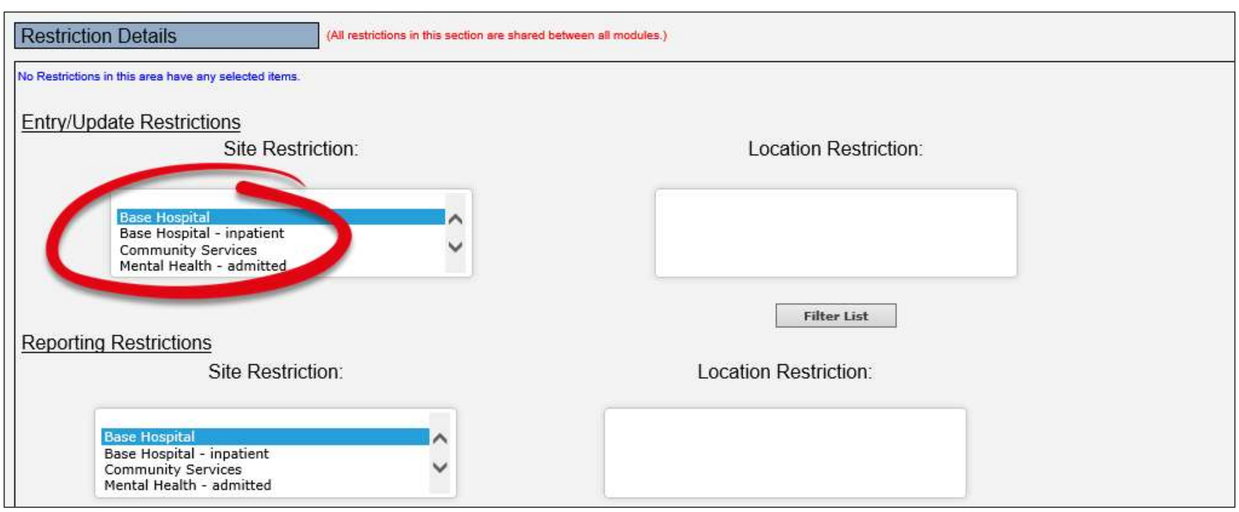
Allow a user to see only records of a certain type in a register

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

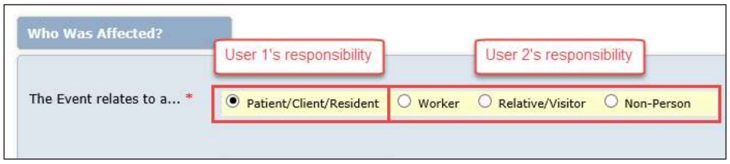


Now, if a user has permission to see the Inbox, then unless you place any additional restrictions on that user, then they will see **all records in the Inbox** across the entire organisation.

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



Adding the site restriction shown above will allows 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 incidents; and the other, responsible for posting all other incidents, including WHS, non-person, etc.

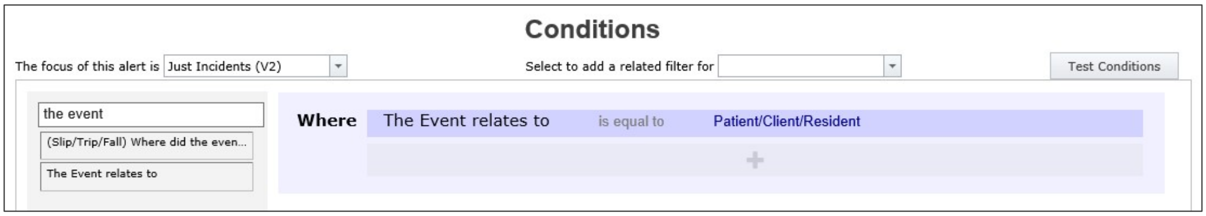
The good news is that you can further restrict the records that a user can see using alerts (also, note that this same technique applies to any register accessed via the Management menu).

Part 1: Create the requisite alerts

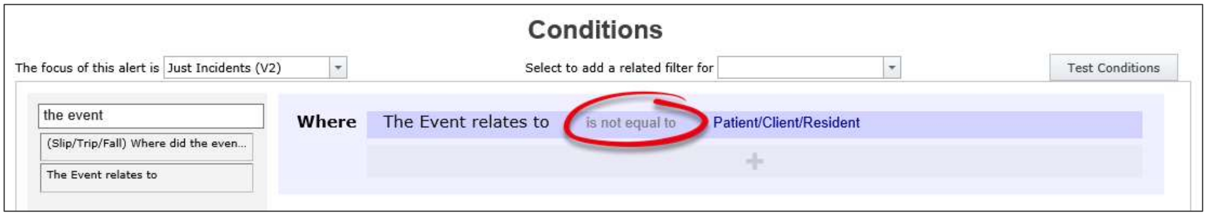
In our example we will need to have 2 alerts configured; one for each user.

Conditions

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

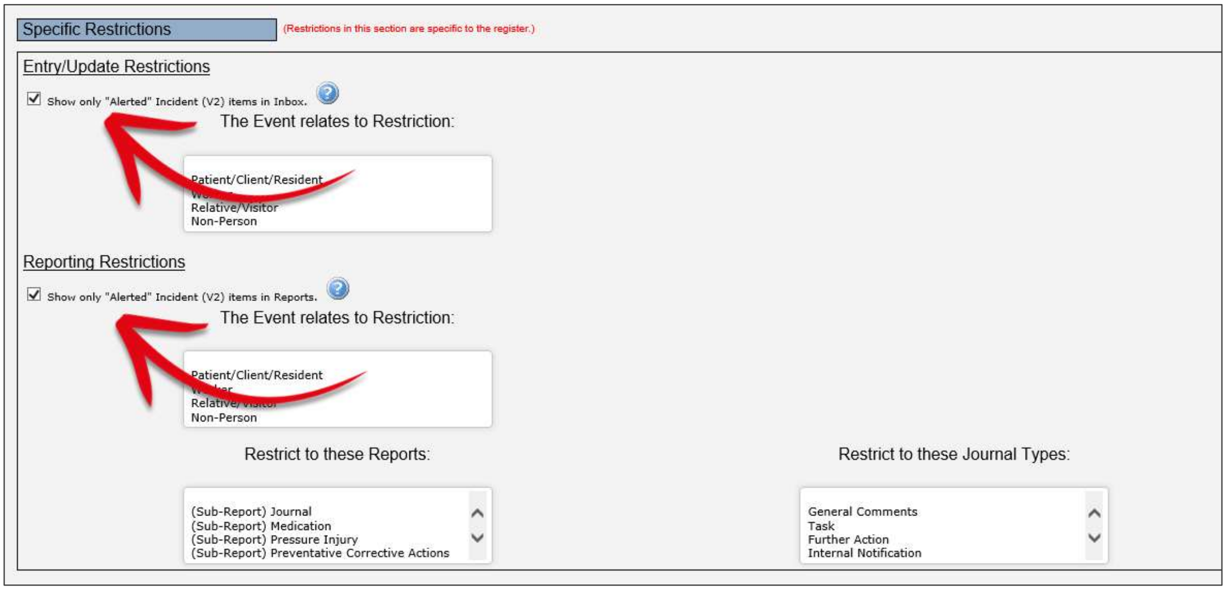


The second alert will be the opposite:



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:



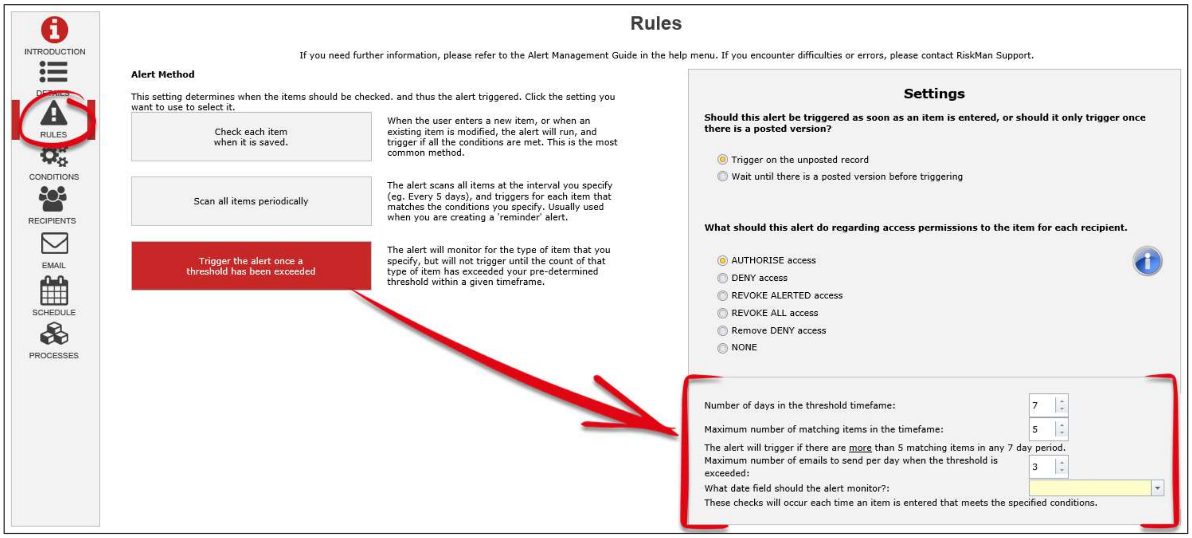
Enabling the two options shown above will ensure the users can only see incidents in the Inbox that their respective alert has given them permission to see. This setting overrides all other methods of defining what a user can see.

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:



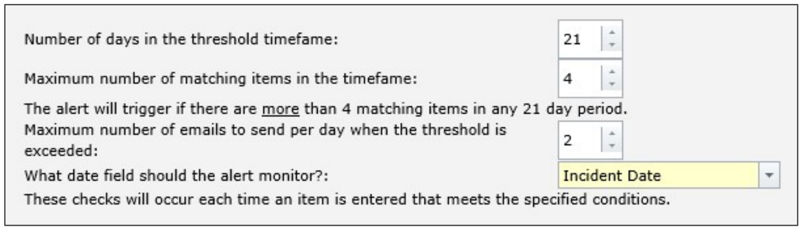
The last two settings control the following:

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

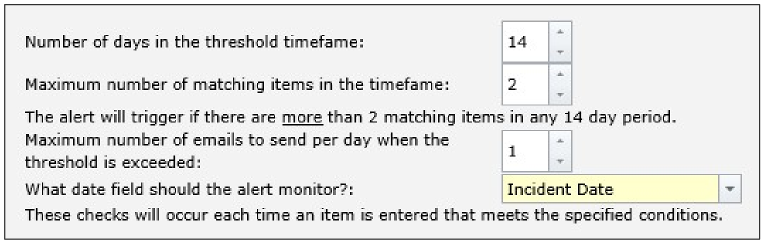


Conditions

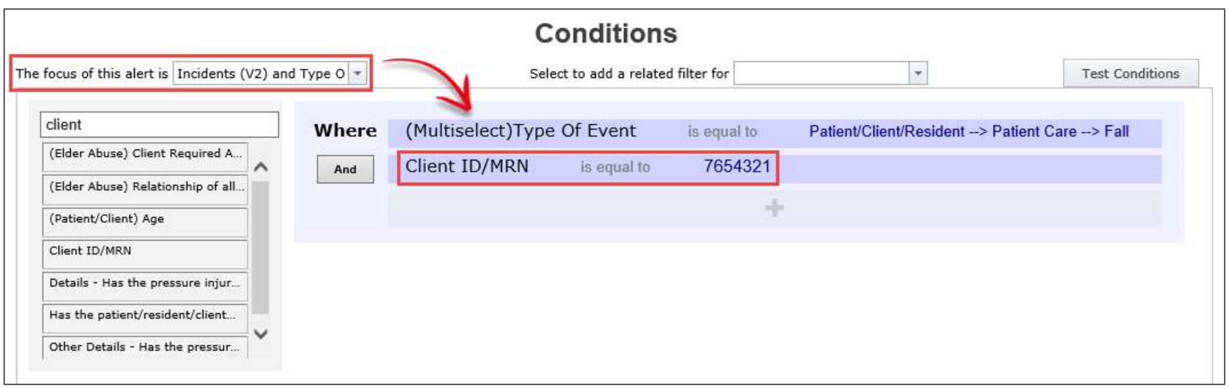
In the system that we made this example, “Type of Event” is a multi-select field. Subsequently, we had to ensure we chose “Type of Event” as the alert focus, so that we could add a condition for that field.

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

Threshold Settings



Conditions



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/MRN. 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.