

|  |
| --- |
| Client incident register user manual  Client incident management system |
|  |

|  |  |  |
| --- | --- | --- |
| Version | Date | Author |
| Version 2.1 | September 2020 | Operational Performance and Quality branch |
| Version 2.0 | August 2019 | CIMS Project |
| Version 1.2 | April 2019 | Operational Performance and Quality branch |
| Version 1.1 | August 2018 | Operational Performance and Quality branch |
| Version 1.0 | 1 December 2017 | Operations Performance and Quality branch |

|  |
| --- |
| To receive this publication in an accessible format phone 1300 024 863, using the National Relay Service 13 36 77 if required, or [email the client incident management system team](mailto:CIMS@dhhs.vic.gov.au) <CIMS@dhhs.vic.gov.au>  Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.  © State of Victoria, Department of Health and Human Services September 2020.  ISBN 9978-1-76069-531-6 (pdf/online/MS word)  Available at [client incident management system](https://providers.dhhs.vic.gov.au/cims) <https://providers.dhhs.vic.gov.au/cims> |
|  |

Contents

[1 Purpose and scope 5](#_Toc18053861)

[1.1 Overview 5](#_Toc18053862)

[1.2 Purpose 5](#_Toc18053863)

[1.3 Scope 5](#_Toc18053864)

[2 Client Incident Management System Users 6](#_Toc18053865)

[2.1 Unregistered users 6](#_Toc18053866)

[2.2 Registered users 6](#_Toc18053867)

[3 Client incident register 7](#_Toc18053868)

[3.1 The Manage incidents screen 7](#_Toc18053869)

[3.2 The manage follow-up screen 9](#_Toc18053870)

[3.3 The CIMS reports 9](#_Toc18053871)

[3.4 The manage users screen 9](#_Toc18053872)

[4 Review an incident 11](#_Toc18053873)

[4.1 Reviewing an incident 11](#_Toc18053874)

[4.2 Incident details 12](#_Toc18053875)

[5 Return an incident report for rework 22](#_Toc18053876)

[6 Service details - Response 23](#_Toc18053877)

[7 Non-major incident authorisation 26](#_Toc18053878)

[7.1 Authorisation 26](#_Toc18053880)

[7.2 Resubmitting using bulk submit 28](#_Toc18053881)

[8 Major incident authorisation 29](#_Toc18053883)

[8.1 Chief Executive Officer' or delegated authority's details 29](#_Toc18053884)

[8.2 Automated follow-up recommendations for major incidents 30](#_Toc18053885)

[8.3 Mandated investigation 31](#_Toc18053886)

[8.4 Mandated review 32](#_Toc18053887)

[8.5 Finalise and submit 34](#_Toc18053888)

[9 Additional follow-up recommendations 37](#_Toc18053889)

[9.1 Creating an additional follow-up recommendation 37](#_Toc18053890)

[10 Major impact – follow-up outcomes 43](#_Toc18053891)

[10.1 Add an investigation follow-up outcome 45](#_Toc18053892)

[10.2 Request an investigation or review extension 48](#_Toc18053893)

[10.3 Add a root cause analysis follow-up outcome 49](#_Toc18053895)

[10.4 Add a case review follow-up outcome 51](#_Toc18053896)

[10.5 Upload documents 52](#_Toc18053897)

[10.6 Download or remove documents 52](#_Toc18053899)

[10.7 Withdrawn outcomes 53](#_Toc18053903)

[10.8 Approved outcomes 53](#_Toc18053904)

[10.9 Completed outcomes 54](#_Toc18053905)

[11 Withdraw/Out of Scope function 55](#_Toc18053906)

[12 Download an incident report 57](#_Toc18053907)

[13 Generate reports 58](#_Toc18053908)

[14 Manage user profiles 60](#_Toc18053909)

[14.1 Add a new user profile 61](#_Toc18053911)

[14.2 Edit user profiles details 63](#_Toc18053912)

[14.3 Editing user profiles access 64](#_Toc18053913)

[14.4 Assigning existing user profiles to a team 65](#_Toc18053914)

[14.5 Deleting user access 67](#_Toc18053916)

[Appendix A: Department service area maps 70](#_Toc18053917)

[Appendix B: Service provider user roles 72](#_Toc18053918)

[Service provider user roles 72](#_Toc18053919)

[Appendix C: Service provider system status 74](#_Toc18053920)

[Status descriptions 74](#_Toc18053921)

[Appendix D: Department divisional office status 77](#_Toc18053922)

[Status descriptions 77](#_Toc18053923)

[Appendix E: Mandatory investigation criteria 79](#_Toc18053924)

[Appendix F: Non-major - bulk submissions 80](#_Toc18053925)

[Processing bulk submissions 80](#_Toc18053926)

[Selecting incidents for bulk submission 81](#_Toc18053927)

# Purpose and scope

## Overview

The Department of Health and Human Services (the department) has developed a client incident management system (CIMS) to strengthen processes to respond and manage incidents that occur during service delivery and result in harm to a client.

The CIMS aims to:

* ensure that timely and effective responses to client incidents address client safety and wellbeing
* ensure effective and appropriate investigation of client incidents
* ensure effective and appropriate review of client incidents
* learn from individual incidents and patterns of client incidents, to reduce the risk of harm to clients, and improve the quality of services and the service system
* ensure accountability of service providers to clients
* protect and maintain the personal and sensitive information of clients, service provider staff, carers and others from whom a service provider collects personal information for the purposes of client incident reporting.

The department has developed the Client Incident Management System as an end-to-end system for the management of client incidents and reporting to the department divisional offices.

There are there are two components to the information technology of the department-built client incident management system:

* CIMS incident report webform
* CIMS client incident register (CIR)

All service providers must own, manage and maintain a client incident register to capture all information regarding client incidents.

Some in scope service providers use their own systems to report client incidents before submitting to the department divisional offices via an application program interface to interact with CIMS.

## Purpose

The purpose of this document is to support service providers (i.e. in scope funded organisations and in scope department delivered services staff) using the **Client Incident Register (CIR)** component of the department-built CIMS, to assess, update, endorse and submit client incident information.

The service provider is responsible for keeping the client incident register up-to-date, and for monitoring trends and patterns.

## Scope

This document covers the management of a **client incident register** by **service providers**. It details the varying user groups and processes to managing client incidents in the CIR.

There are two processes for reporting a client incident, depending on whether the incident resulted in a major impact or non-major impact to the client. An assessment by the service provider of the impact on the client will determine the reporting process that must be followed.

# Client Incident Management System Users

There are two broad user categorisations in the CIMS; unregistered users and registered users.

## Unregistered users

Unregistered users are all staff that may be required to report a client incident under CIMS but are not registered users of a service provider’s client incident register. Unregistered users are limited to creating and submitting client incident reports via the CIMS incident report webform.

## Registered users

Registered users are service provider or department staff who are authorised users of the CIMS client incident register for managing incidents.

Registered users are responsible for reviewing and managing the incident report, follow-up and investigation or review process.

Registeredusers within the CIR are responsible for reviewing and ensuring the accuracy of incident reports and follow-up actions in the CIR before approving and submitting to the department divisional offices. Registered users may be the service provider or department staff at the time an incident has occurred or been disclosed during a department delivered service.

### Service Provider registered user roles

There are four user roles for service providers in the CIR. The four user roles for service providers are: Manager, Senior Delegate, Investigation manager/review manager and read-only.

Staff within the CIR are assigned one registered user role. Each user role varies in accessibility and authority to information held in the CIR. This variation ensures the person completing the task is at an appropriate level of authority in entering, reviewing and approving client incident information.

**Manager** user role – has limited access to the CIR. The primary task is reviewing the details of a client incident report and completing the service provider responses page before approving and escalating to a Senior Delegate user for endorsement and submission to the department divisional office. Manager users may be also be assigned responsibility to manage an investigation or review for a major impact incident.

**Senior Delegate** user role – has the highest level of access to CIR. A Senior Delegate user can undertake all functions within the CIR. Primary responsibilities for a senior delegate user is to endorse and submit client information to the department divisional office, determine follow-up action to be taken in response to a major impact incident and manage users provisioning.

**Investigation manager/review manager** user role– has access restricted to CIR. Access for an investigation/review manager user is only enabled when they are assigned to manage an investigation or review. No other incident related details will be visible to this level user.

**Read-only** user role – has limited access to CIR. The read-only user has full visibility and access to system but no workflow functionalities beyond the ability to view, print, extract and run reports.

**Note:** Appendix B (page 60) provides further clarification on service provider user roles.

# Client incident register

The client incident register has four screens: Incidents, Follow-ups, Reports and Users.

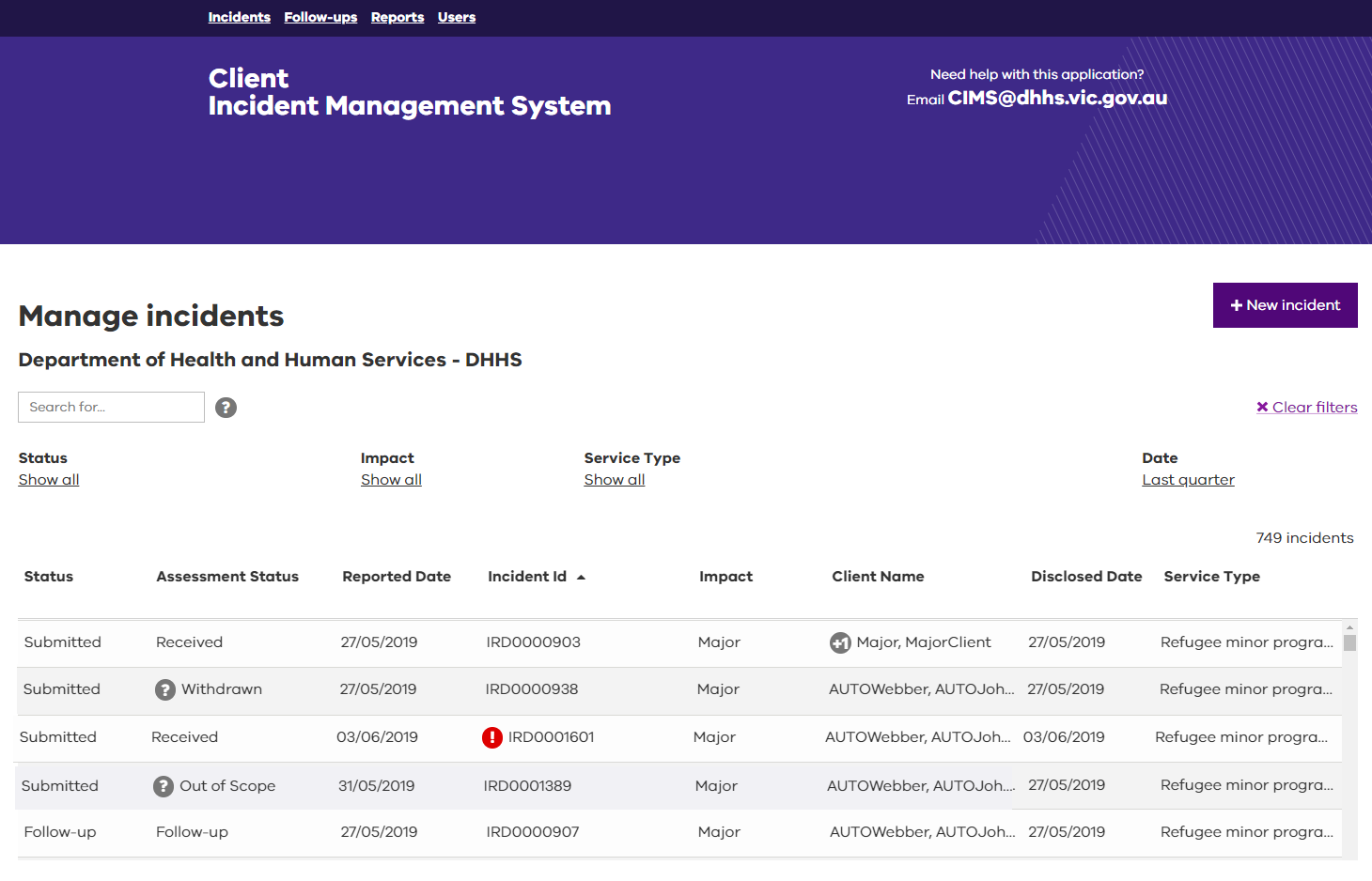
The accessibility of these four screens is dependent on the assigned user role.

The landing page is the Incidents (manage incidents) screen.

## The Manage incidents screen

The **Manage incidents** screen is available to all registered users and displays the incident reports within the team to which the logged in user belongs.

The **Manage incidents** screen displays all incidents in a matrix with the following details: Status, Assessment status, Reported date, Incident ID, Impact, Client name, Disclosed date, and Service type.



### Info Icons

* A number beside a client’s name indicates the number of additional clients involved in the incident beyond the first client. Selecting the number will reveal the names of the additional clients.
* A question mark beside an assessment status of Withdrawn or Out of Scope indicates that the incident has been Withdrawn or assessed as Out of Scope by the Department. Selecting the question mark will display further information about the withdrawal.
* Incident reports displayed with red exclamation marks indicate that the incident report details are restricted due to their highly sensitive or confidential nature and will only be visible to a user with Senior Delegate access. When you see this symbol, you can select it to view further information.

### Screen functions

Many functions have been embedded in the screen to make it easier to navigate.

* Refined searches using the search, filter, and sort tools
* Clear all filters
* Create a new incident

#### Refined searches using the search, filter, and sort tools

There are several search functions available in the Manage Incident screen to assist in quickly identifying an individual incident or group of incidents for actioning and reporting. They are:

* A ‘Search for’ field enables you to type search criteria into it.
* As you begin typing, the system begins identifying a match or partial match. An icon resembling a question mark sits beside the ‘Search for’ field. Selecting the icon provides additional tips and hints for using the search functions.
* Filter functions reduce the information displayed in the incident table.
* The filters are identified as a default of ‘show all’ beneath headings ‘status’, ‘impact’ and ‘service type’. Selecting any of the filters reveals a predefined list of options. The functions available will depend on the screen currently displayed. Select the option to filter the information in the incident table. These filters work individually or can reduce the incident view even further if more than one is selected.
* Column headings can be selected to sort the order of the table information to either ascending or descending.
* Select Clear Filters to return to the default page filter and sort options

|  |
| --- |
| Try using a combination of the search functions. For example, enter a name into the ‘Search for’ free text field, and then sort the results by Impact, then by Incident ID. |

#### New Incident

* New incident – this button opens a new client incident report form. Refer to the Client incident report webform user manual for more information on how to create an incident report using the CIMS incident report webform.

### The manage incident status descriptions

* Incident reports in the **Manage incidents** screen are classified by their status.
* Status descriptions in the **Manage incidents** screen reflect the current progress of the incident report managed by service providers. This varies from the assessment status description to reflect the current progress of the incident report within the department divisional offices once submitted.
* Refer to [Appendix C](#_Status_descriptions) for service provider status descriptions. A listing for department divisional office assessment status descriptions are provided at [Appendix D](#_Appendix_D:_Department).

### The manage incident action buttons

* Depending on the status description of the incident report, certain actions are available.
* Hover the mouse over the incident on the **Manage incidents** page to display the action buttons available according to the user profile of the logged in user, and the status of the incident report.



Action button selections can be made following their display. These are:

|  |  |
| --- | --- |
| Action | Description |
| View | This action enables the details of incident report to be opened and viewed. |
| Edit | This action enables the incident and its content to be viewed and changes made as required by the service provider user. |
| Follow-up | This action transfers to the summary page of the follow-up screen for the incident report (investigations, root cause analysis reviews and case reviews). For more information refer to [Major impact – follow-up recommendations.](#_5._Major_impact_1) |
| Withdraw | This action enables the withdrawal of an incident report from the reporting process where the incident report is determined to not be in-scope.  For more information refer to [Withdraw function](#_10._Withdraw_function_1). |
| Download | This function converts the incident report to a PDF that can be either saved or printed to a designated printer. See [Downloading an incident](#DownloadIncident) for more information.  Printing any document must comply with privacy regulations. |

## The manage follow-up screen

The manage follow-up screen displays major impact incidents that have progressed to follow-up (investigation, root cause analysis or case review) within the incident management process.

The incidents visible in this screen will be determined by the CIMS registered user role. A Senior Delegate level user will see all incidents that have progressed to follow-up within the team they are assigned whereas the Manager and Investigation/Review manager user roles will only be able to see the incidents they have been assigned to investigate.

## The CIMS reports

The reports screen is available to all registered users within a service provider and includes a list of predetermined reports that can be run. Each report has been built to meet a different reporting requirement with additional filters available in each to provide further flexibility based on the user requirements.

The data displayed within each report will be in line with the CIMS registered user role (Reports only display data for incident reports that a registered user has access too).

## The manage users screen

The manage users screen is available only to Senior Delegate level users and allows a service provider to manage their own CIMS registered users. This screen can be used for a range of functions including:

* Adding a new user
* Updating an existing users details
* Changing an existing users role to increase or decrease access
* Deactivating users

# Review an incident

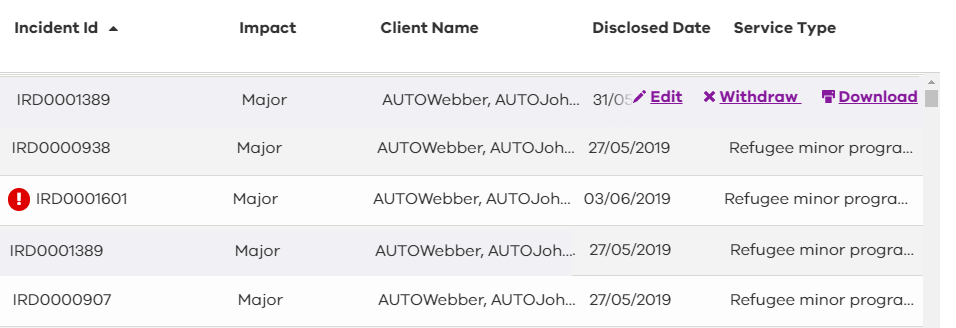
## Reviewing an incident

Both major and non-major impact incident reports are accessed from the **Manage incidents** screen and can be actioned by a Manager or Senior Delegate level user (where applicable). Incident reports when created that are awaiting review and approval will have a status of ‘New’.

**Note**: Once an incident report has been actioned by a user (escalated or submitted), then the incident report will no longer be editable by that user. Editable functionality will only be available after an incident has been actioned if the incident report is withdrawn or returned by the next user in the workflow.

The steps for reviewing the details of a major impact incident report by a service provider are as follows:

1. Locate the required major impact incident report. Refer to [the search, filter, and sort tools](#_Refined_searches_using) for assistance in locating the major impact incident report.
2. Hover the mouse over the major impact incident report to display the action buttons.



1. Select the Edit action button. This action will open the incident report and display the Incident details screen.
2. The Incident details screen has three stages; Incident, Response and Authorisation. The Manager user (or Senior Delegate user) will review all information in the Incident details screen in the incident stage and completes the Response stage for further approval within the organisation.
3. The Senior Delegate reviews information of the incident report in the incident and response stages. If satisfied, the Senior Delegate user will complete the Authorisation stage response before submitting to the department divisional office.

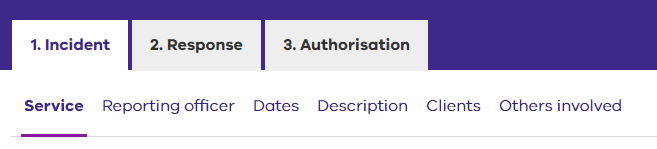
A number of function buttons are displayed on the bottom of the pages when working through the **Incident details** screens in reviewing the information within.

|  |  |
| --- | --- |
| Button | Description |
| Back | Select **Back** to return to a previously viewed page. |
| Return | Select **Return** if the incident needs to be returned for rework. This function is only available for Senior Delegate user roles. For further information refer [Returning an incident for rework](#ReturnIncident). |
| Withdraw | Select this option if the incident is out of scope and needs to be withdrawn from the reporting process. For more information refer to [Withdraw function](#_10._Withdraw_function_1). |
| Save | Select **Save** to make any changes to the incident. A message confirming the status of the save request is displayed. |
| Next | Select **Next** to move to the next page to continue the review.  The Declaration and acknowledgement screen will be displayed on the final stage for Senior Delegate users before concluding their involvement in the process and submitting to the department. |

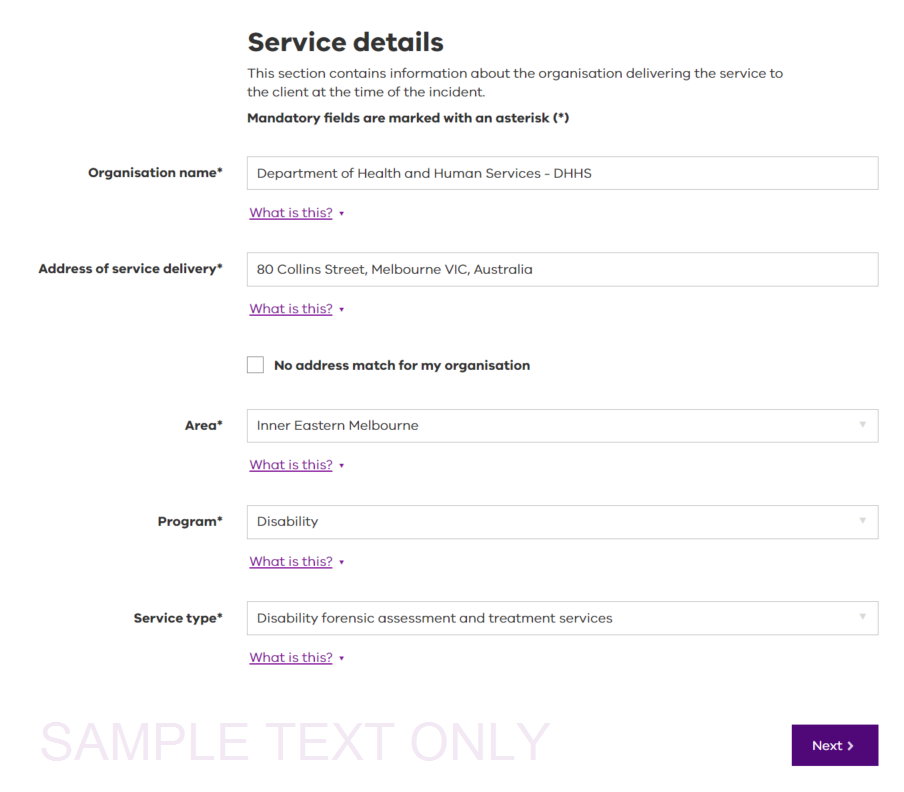
## Incident details

The **Incident details** screen captures and displays all incident details as created and submitted by a user the service provider.

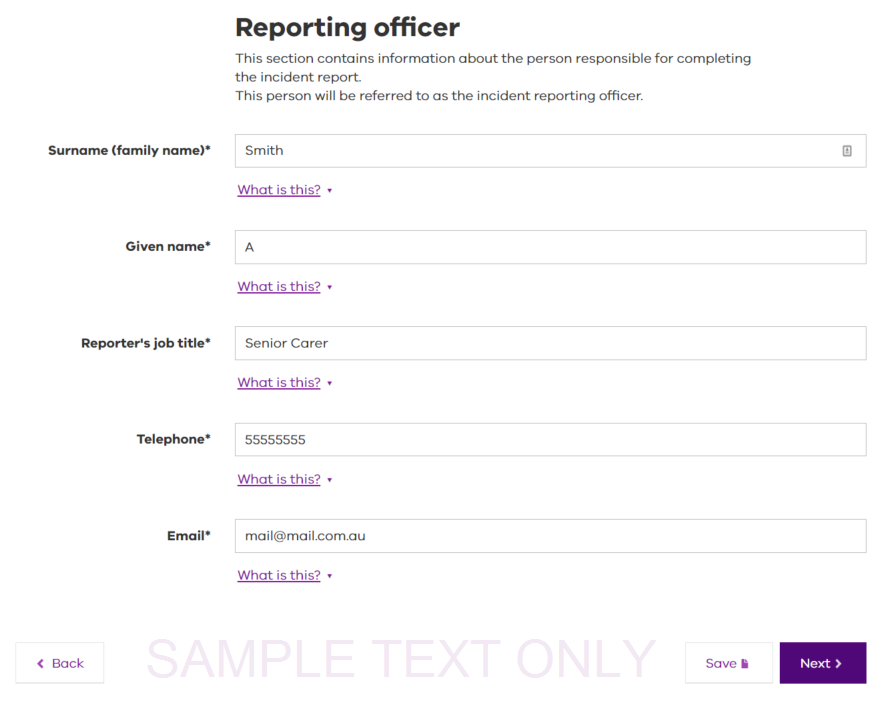
**Each of the** fields displayed across the pages within the **Incident details** screen; Service, Reporting Officer, Dates, Description, Clients and Others Involved, are to be reviewed to ensure the accuracy of information relating to the incident.



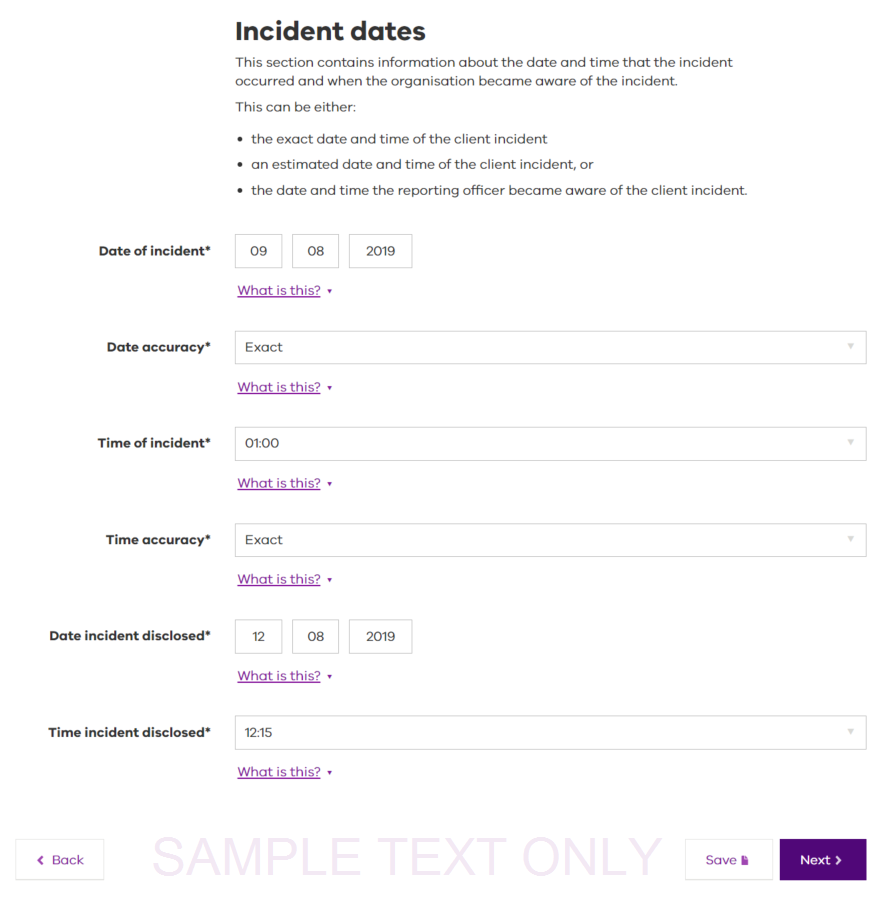
* 1. Commence the review from the **Service** **details** page.



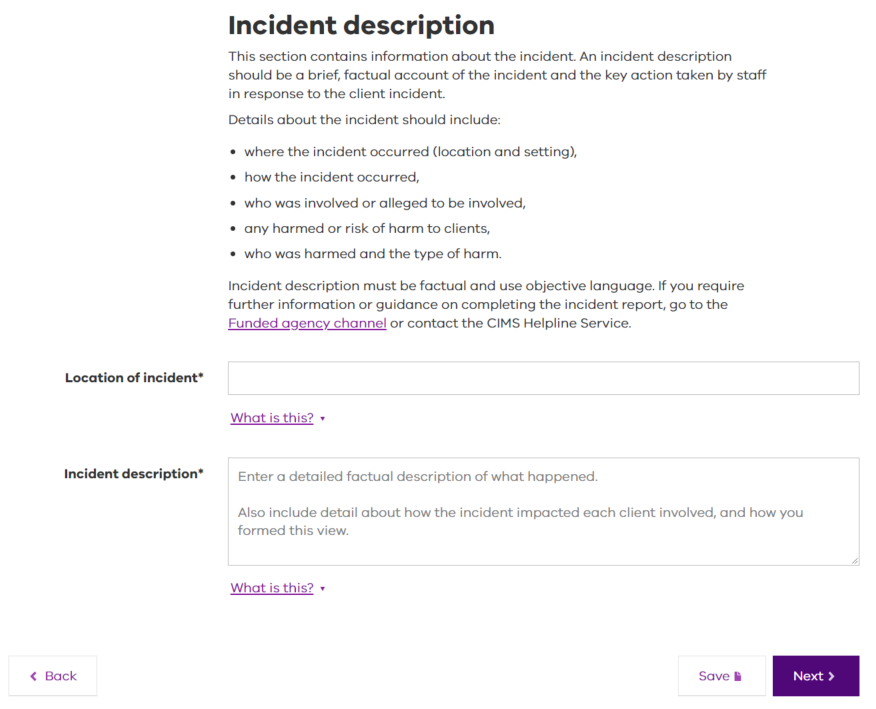
* 1. Select **Next** to review the **Reporting officer** page.



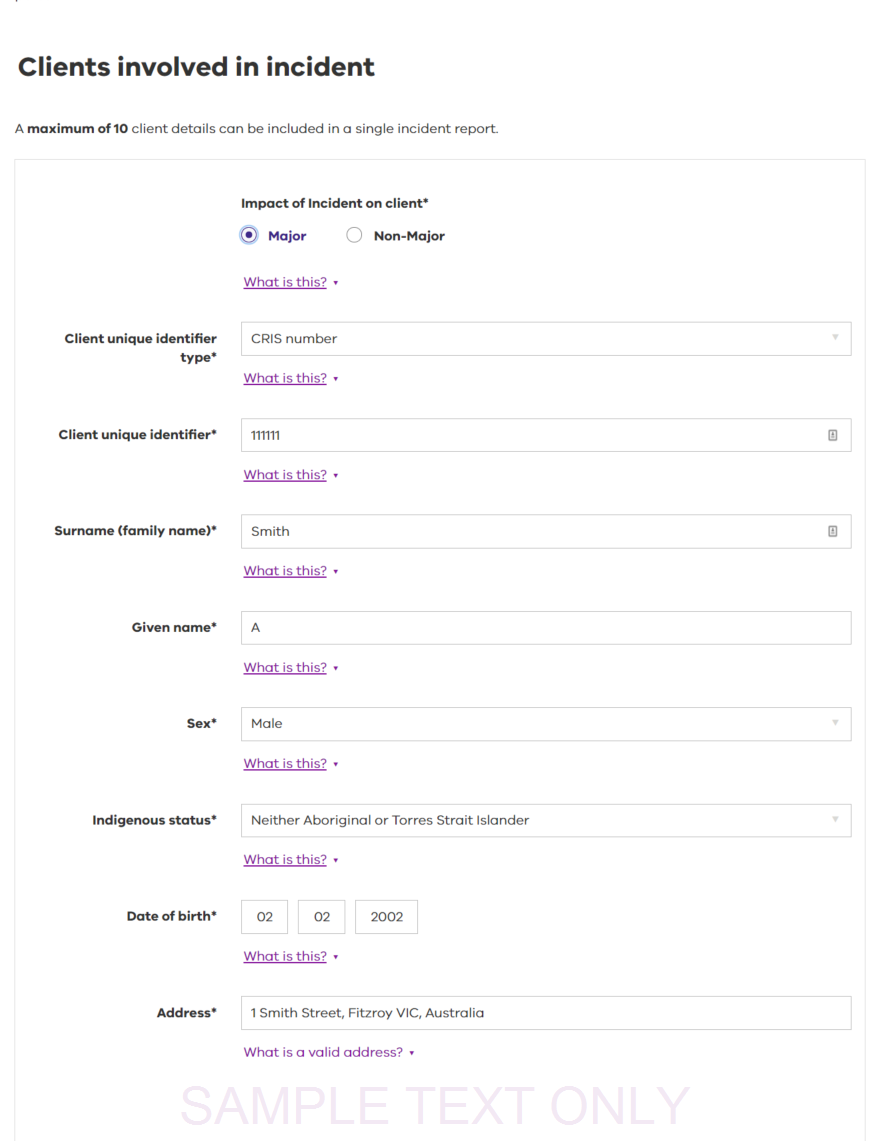
* 1. Select **Next** to review the **Dates (Incident dates)** page.



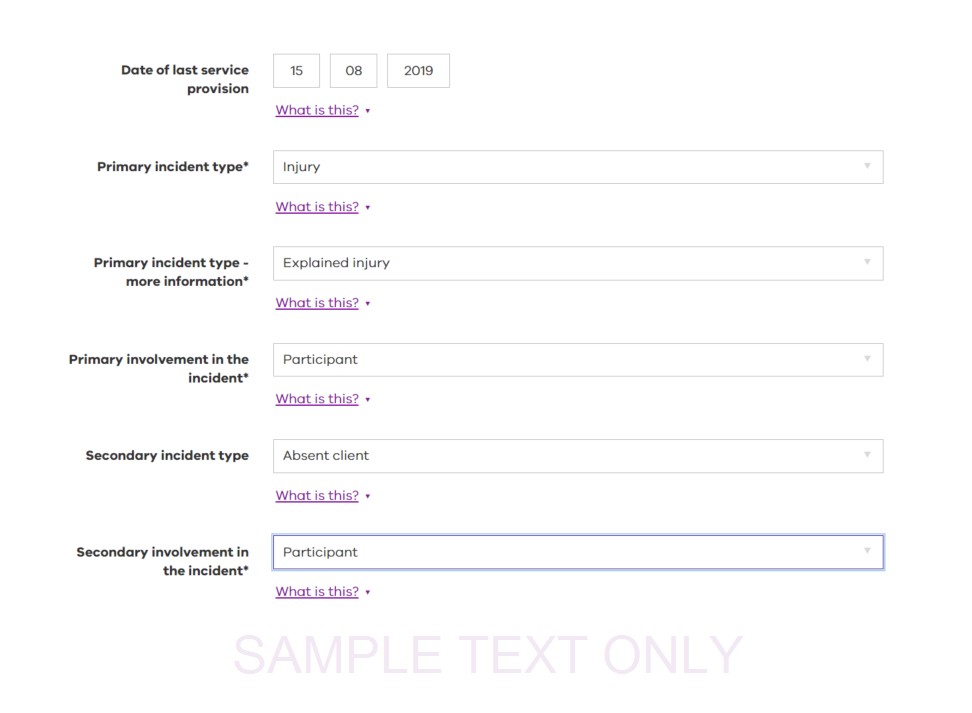
* 1. Select **Next** to review the **Description (Incident description)** page.

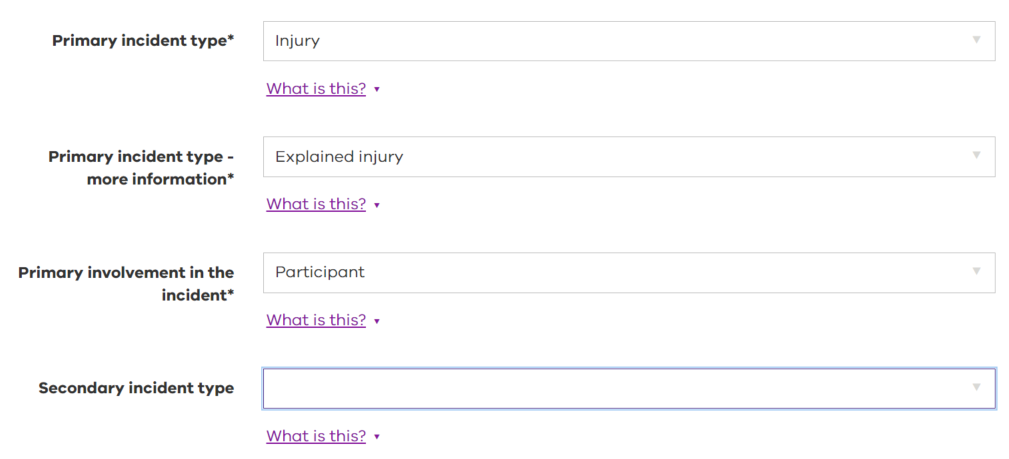


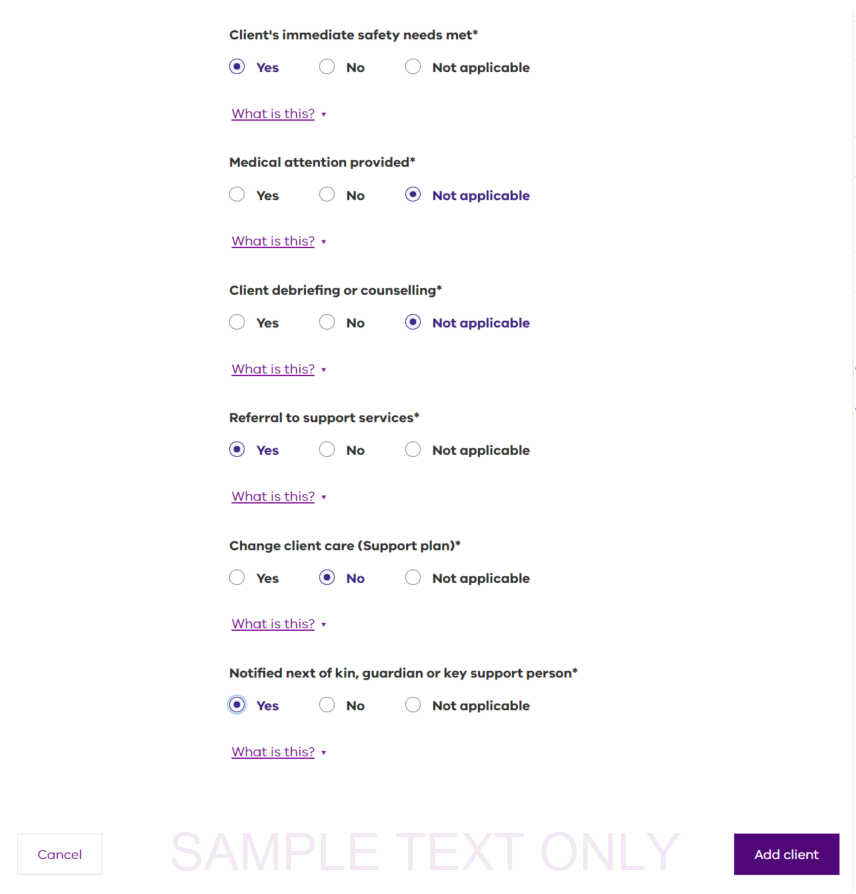
* 1. Select **Next** to review the **Clients (Clients involved in incident)** screen. A list of clients who are involved in the incident are displayed.



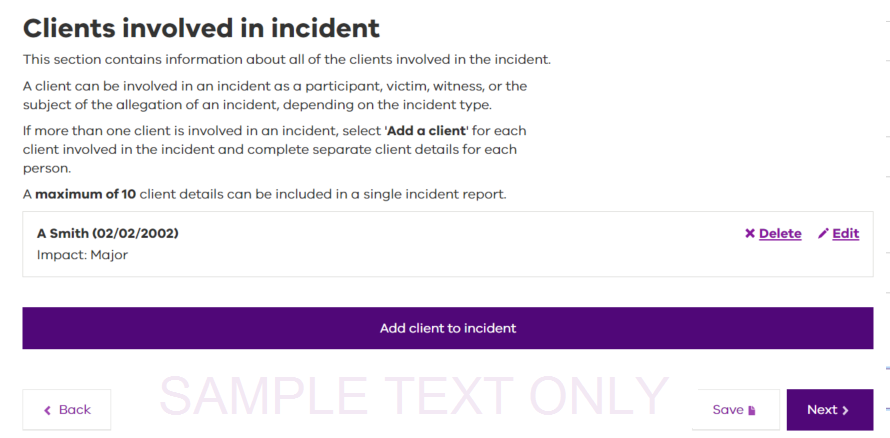
1. Select the **Edit** button beside the client to be reviewed. The specific details of the selected client are displayed and must be reviewed to ensure it is complete and accurate. **Note:** the delete button is available prior to the client record being open.







1. Select **Update client** to return to the **Clients (Clients involved in incident)** screen.



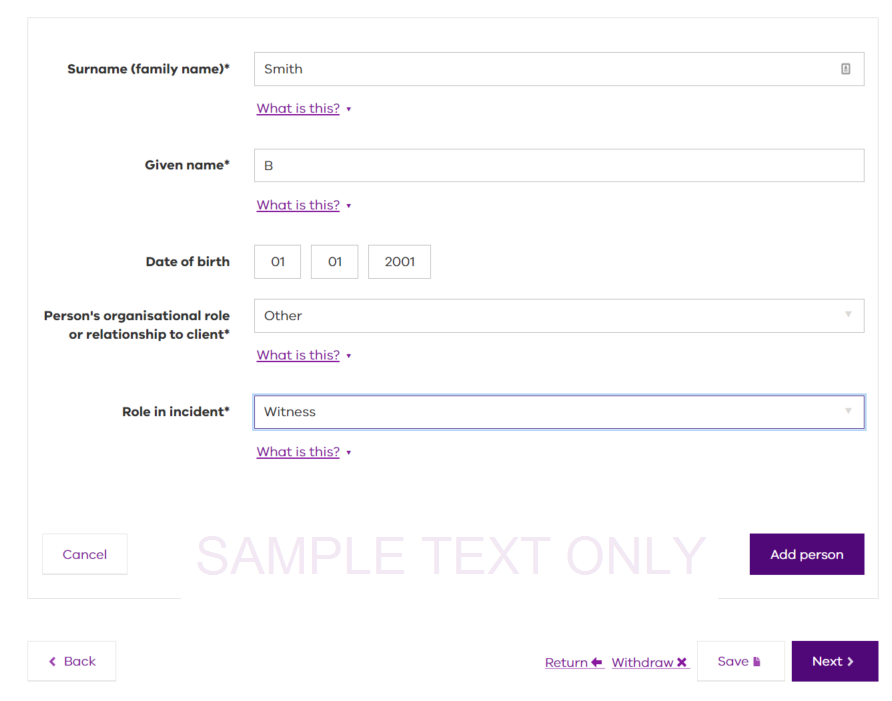
1. Return to Step 6 to review a different client (if more than one client) or continue by selecting **Next** to proceed with the review.

Selecting **Next** will display the **Others involved** screen. Details in the **Others involved** screen relate to persons that may have been involved in the incident that may include staff, volunteers or members of the general public and are not clients impacted during the delivery of service.

1. Select the **Edit** button beside the other person involved to display the specific details of the person to be reviewed for completeness and accuracy.



1. Select **Update client** to return to the **Others involved Clients** screen. Return to Step 9 to review a different other person (if more than one) or continue by selecting **Next**. The **Service provider’s response details** screen will display.



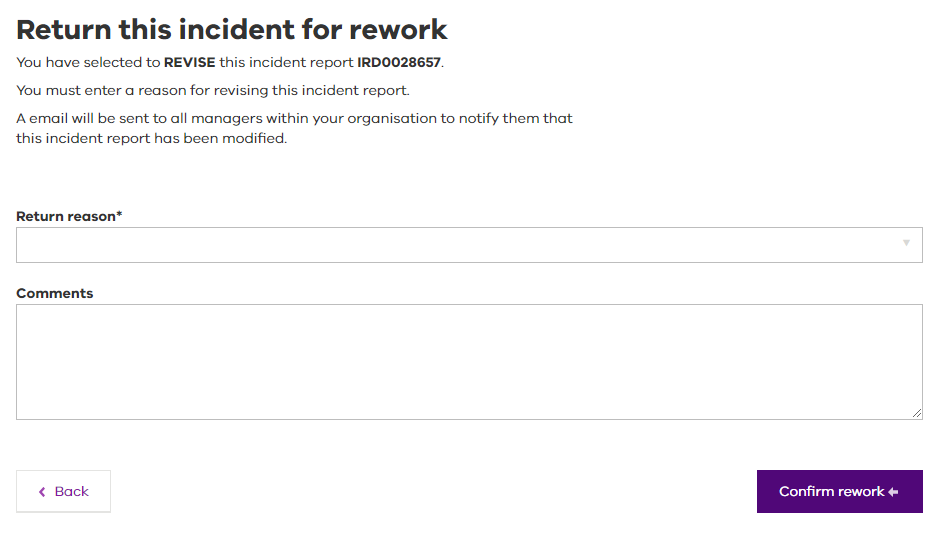
# Return an incident report for rework

Major and Non-major incidents with the status of ‘new’ can be returned by a Senior Delegate to the Manager or Investigation Manager/Review Manager user for reworking. The Senior Delegate processes this request by:

1. Identifying the major or non-major incident to be reworked.
2. Hovering the mouse over the required incident report for the **Edit** function to display.
3. Selecting **Edit will display t**he **Service details** screen.
4. Select **Return**.

* The **Return this incident for rework** screen is displayed.
* The Return link can be selected from any of the Incident, Response or Authorisation screens

1. Select the most appropriate reason for returning this incident for rework from the **Return reason** field.
2. Select **Confirm rework** to forward the non-major or major impact incident to the reporting officer with comments for rework to be completed.

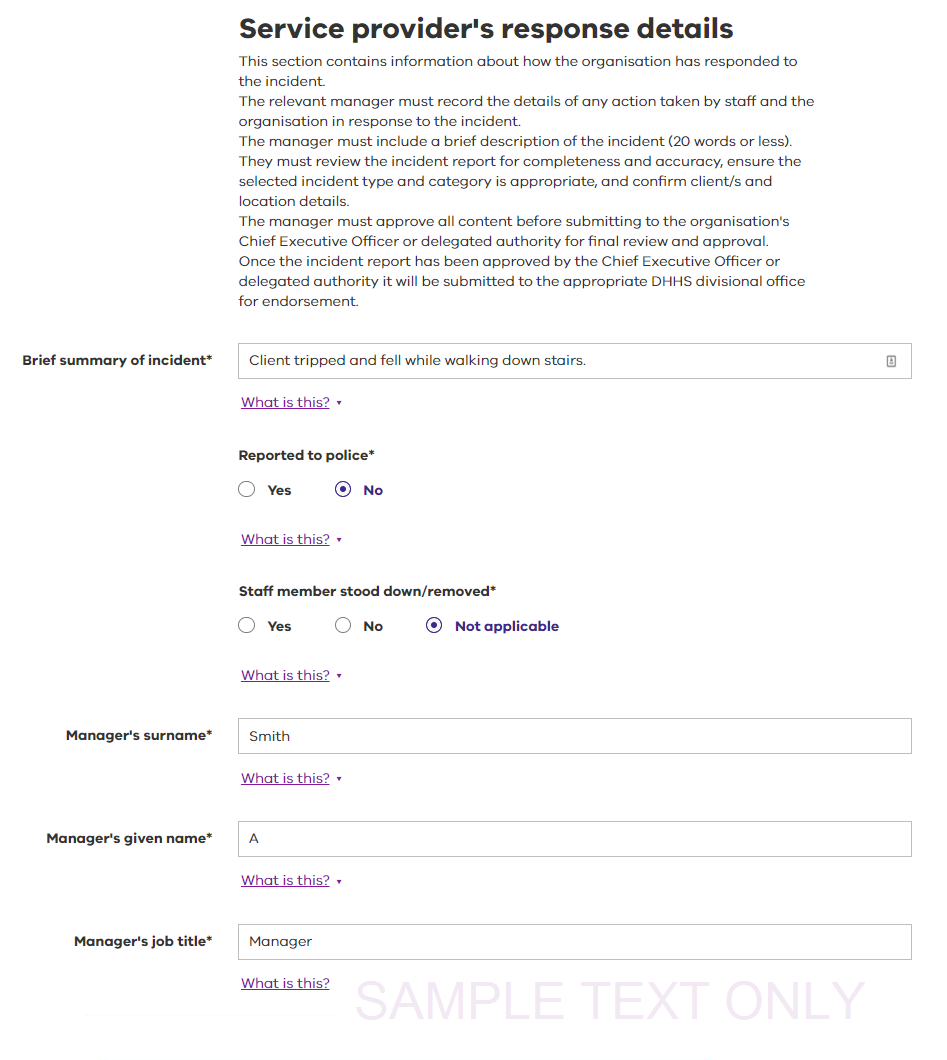


|  |
| --- |
| Managers are also able to **withdraw** incidents, if the incident is assessed as being out of scope. See [Withdraw function](#_10._Withdraw_function_1) for further information. |

# Service details - Response

The **Service provider’s response details** screen contains information about how the organisation has responded to the incident.

A Manager user (or Senior Delegate user) is required to record any action taken by staff and the organisation in response to the incident. The Manager user must review the information to ensure it is complete and accurate before approving and escalating to the Senior delegate user (which may be the CEO) for final review and approval.

To complete the service provider’s response details, the Manager user must:

1. Enter a **Brief summary of incident**.

* This should be a short description of the client incident – 20 words or fewer.

1. Indicate whether the incident was **reported to police**.

* If there was no need to report the incident to the police, select No. If No, go to step 5.
* If the incident was reported to police, select Yes. Additional fields will display. If Yes, continue to Step 3.

1. Enter the **Date reported to police**.

* This field is activated if Yes was indicated at Step 2. This is the date on which the police were notified.

1. Select a radio button to indicate whether **Police investigation initiated**.

* This field is activated if Yes was indicated at Step 2. Select Yes if the police are investigating the incident. Select No if they are not investigating the incident.

1. Select a **Staff member stood down/removed** radio button.

* Indicate here whether any of the organisation’s staff members have been stood down because of their involvement in the incident. This could include suspension or termination of employment and/or the staff member having no contact with the client.



1. Enter the **Manager’s surname**.

* This is the last name of the Manager user reviewing this incident report.

1. Enter the **Manager’s given name**.

* This is the first name of the Manager user reviewing this incident report.

1. Enter the **Manager’s job title**.

* This is the job title of the Manager user reviewing this incident report.

1. Enter the **Date completed**.

* This is the date that the Manager user reviewing this incident report reviewed it.

1. Enter **Telephone number**.

* This is the best telephone number on which to contact the Manager user reviewing this incident report.

1. Enter **Email**.

* This is the best business email address on which to contact the Manager user reviewing this incident report.

1. Select an **Access restricted** radio button.

* Select **Yes** if this incident report should only be visible to the organisation’s CEO or Senior Delegate user.

1. Enter the **Key actions** taken.

* Enter comments about the immediate actions taken by the organisation in response to the incident. This includes what the organisation has done to prevent similar incidents in future.

1. Select **Next**.

* A manager level user will receive a confirmation page stating that they are ready to escalate the incident to the Senior Delegate user for endorsement.
* A Senior Delegate user will progress to either the **Non-major** **incident authorisation** (see 5 Non-major incident authorisation) or the **Major incident authorisation** (see 6 Major incident Authorisation) screen.

# Non-major incident authorisation

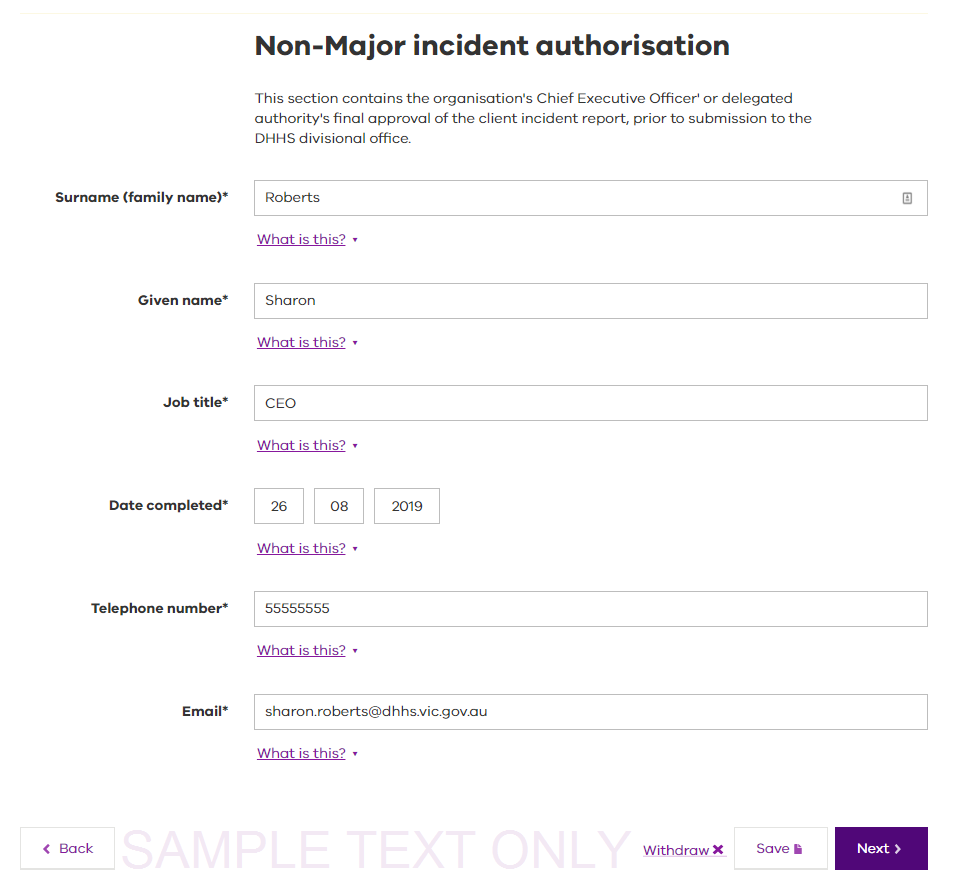
|  |
| --- |
| See [4](#_4._Major_impact_2) Major impact incidents - reviewing and submitting for the processes and information to assist with major impact incidents. |

Incidents reported are assessed as either major impact or non-major impact. The process for reporting non-major incidents is somewhat shorter than for major impact incidents, but is otherwise the same.

## Authorisation

All non-major incident reports are required to be submitted to the department divisional office within three business days of the date and time the incident was disclosed.

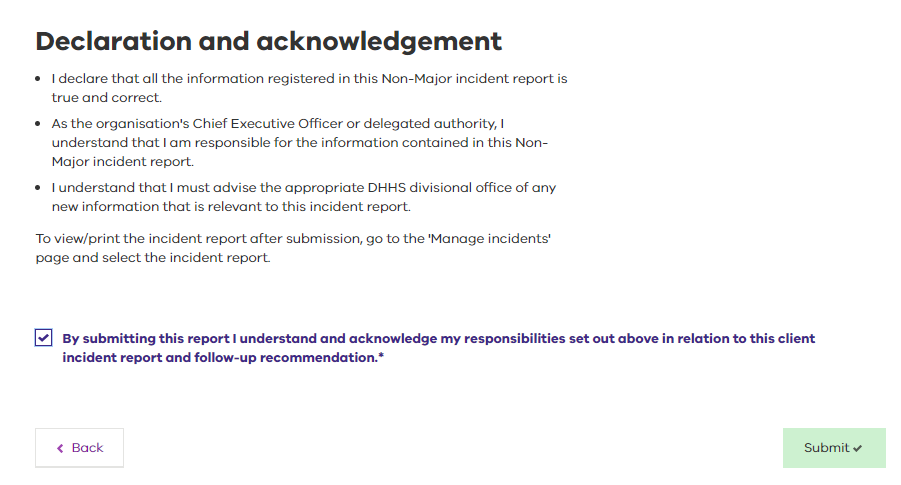
1. Select **Edit** to open the incident



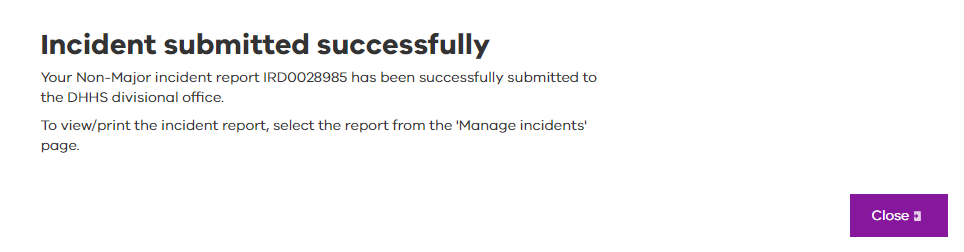
1. Review and update any details as necessary
2. Navigate to the **Incident Authorisation** tab
3. Enter the **Job title**

* All other details will pre-fill

1. Select **Next** to progress to the Declaration and acknowledgement screen



1. **Check** the acknowledgement box and select **Submit**

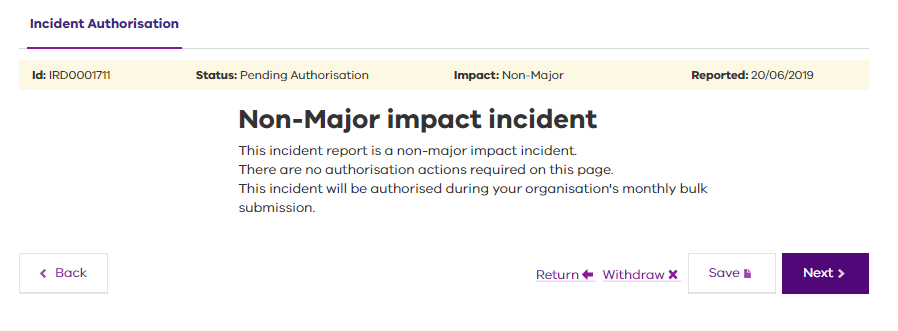


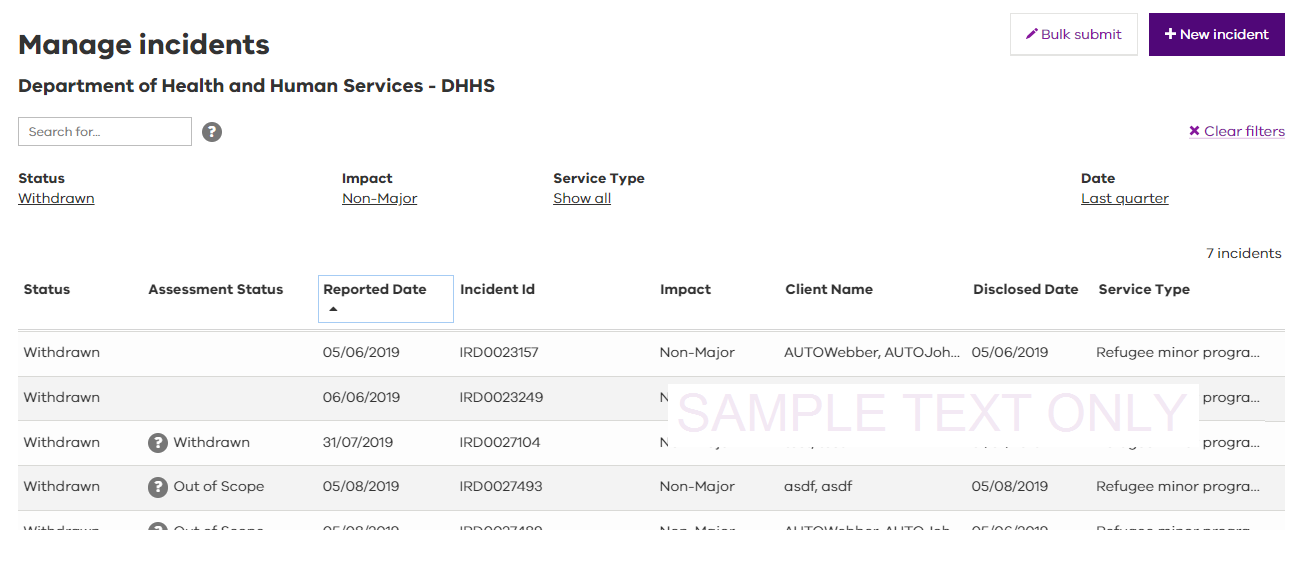
1. Select **Close** to return to the **Manage incidents** screen
2. The incident report shows a status of **Submitted** and an Assessment Status of **Received**



## Resubmitting using bulk submit

|  |
| --- |
| Non-major impact incidents, which have previously been submitted using the previous bulk submission process[[1]](#footnote-1), and which are withdrawn by the department divisional office, will require resubmission using the same bulk submit process. |

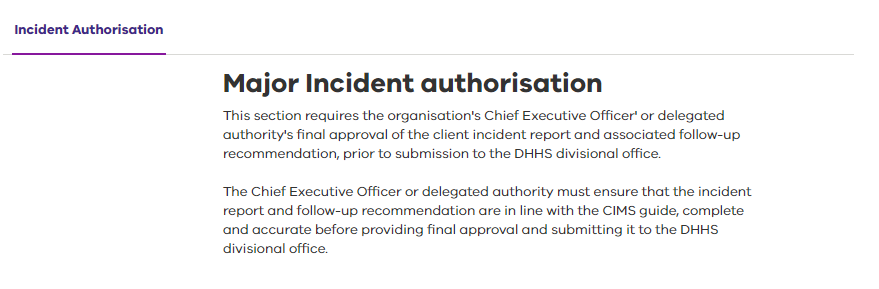


Any older non-major incidents, which have yet to be submitted, may also be required to use the bulk submission process. 

The bulk submission functionality will remain available where there are any non-major incidents that require submission using this process. Once all older non-major incidents have been submitted to the department, the bulk submission button will no longer be visible.

# Major incident authorisation

The **major incident authorisation** screen is for the organisation's Chief Executive Officer' or delegated authority's final approval of the client incident report and associated follow-up recommendation, prior to submission to the DHHS divisional office.



The Chief Executive Officer or delegated authority must ensure that the incident report and follow-up recommendation are in line with the CIMS guide, complete and accurate before providing final approval and submitting it to the DHHS divisional office.

Once the incident report has been approved by the Senior Delegate user, it will be submitted to the appropriate department divisional office for endorsement.

## Chief Executive Officer' or delegated authority's details

CIMS will automatically populate the details of the logged in Chief Executive Officer or delegated authority user for the following fields:

1. **Surname (family name)**.

* This is the last name of the user approving the incident report for submission to the department.

1. **Given name**.

* This is the first name of the user approving the incident report for submission to the department.

1. **Date completed**.

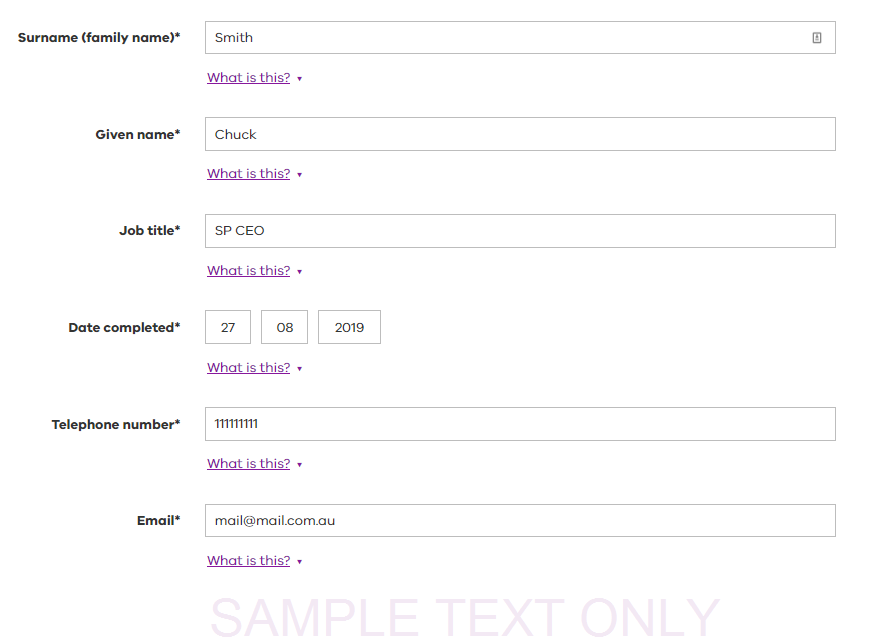
* This is the date that the major impact incident report was reviewed and submitted to the department.

1. **Telephone number**.

* This is the best telephone number on which to contact the user approving the incident report for submission to the department.

1. **Email**.

* This is the best business email address on which to contact the user approving the incident report for submission to the department.



|  |
| --- |
| The Senior Delegate user approving the incident report **may** edit each of the pre-populated fields, and **must** enter the **Job title**\* prior to submission to the department. |

1. Job title

* This is the job title of the user approving the incident report for submission to the department.

## Automated follow-up recommendations for major incidents

The release of the V2.0 upgrade to CIMS saw the incorporation of business rules driven follow-up recommendations for major impact incidents, as part of the incident authorisation step.

|  |
| --- |
| As part of this change, follow-up recommendations no longer need to be reviewed and endorsed by the department, and move from a status of **Recommendation** **in Progress** – when first submitted as part of a major incident submission – to **Recommendation Completed** – when the assessment of the incident is completed by the department. |

Based on the information detailed within the incident report, CIMS will specify that either an investigation or a review (by Root Cause Analysis or Case Review) is carried out for each major impact incident as follows:

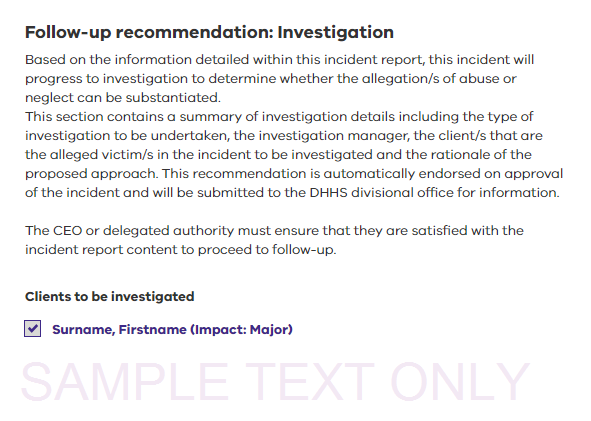
* When any client involvement in a primary or secondary incident meets the mandatory investigation criteria[[2]](#footnote-2), an Investigation is required.
* When the mandatory investigation criteria are not met, a review is required.

## Mandated investigation

When any client involvement in a primary or secondary incident meets the mandatory investigation criteria, CIMS will display the Follow-up recommendation: Investigation details:

1. Clients to be investigated

* CIMS will automatically include all clients whose involvement in the incident meets the mandatory investigation criteria1



1. Select the Investigation type radio button.

* This is the type of investigation to be undertaken for this incident. Select the button to indicate whether the investigation is to be managed internally, externally or jointly with the department divisional office.

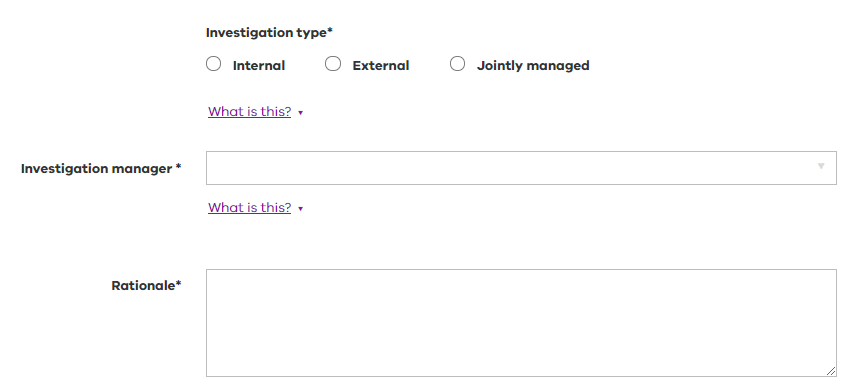
1. Select in the Investigation manager field to select from the list.

* This is the person to whom the incident will be assigned to manage the investigation and the contact details for the Investigation manager will be automatically populated.

1. Enter the rationale for the choice of investigation type

* This provides any additional relevant information regarding the choice of investigation type.

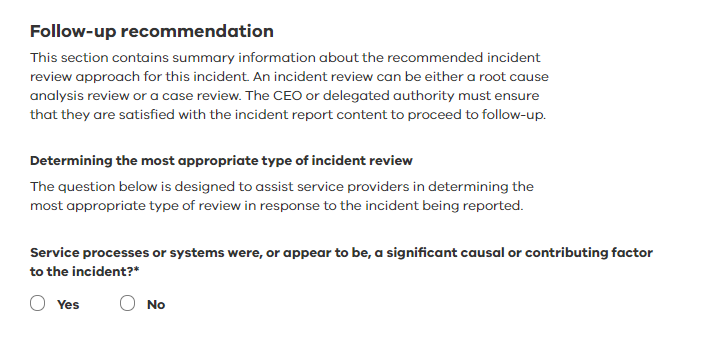
|  |
| --- |
| The **investigation/review manager** will only have access to the investigation or review outcome for client incident they are assigned. |



## Mandated review

Where the mandatory investigation criteria are not met, a review is required.

CIMS will use information provided during incident review and authorisation to determine the most appropriate type of incident review in response to the incident being reported.



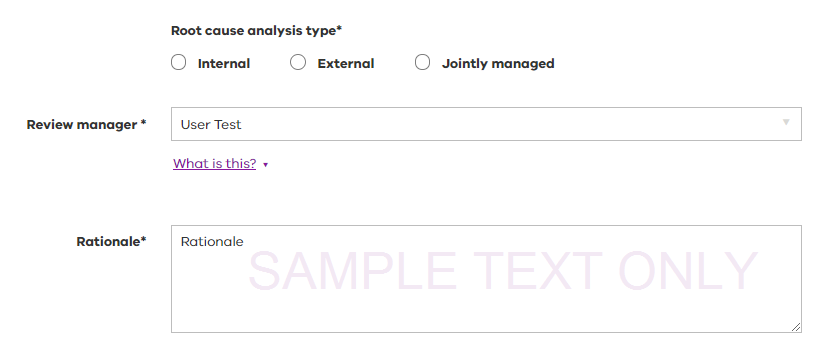
Select **Yes** or **No** to answer whether service processes or systems were a significant causal or contributing factor to the incident.

### Review by Root Cause Analysis

### Proposed root cause analysis review where service processes or systems were determined to be a significant causal or contributing factor

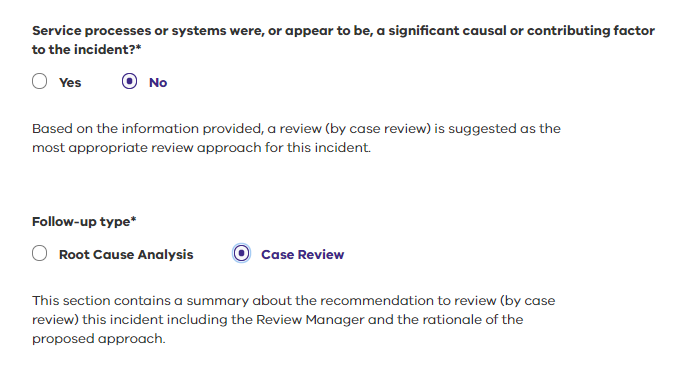
Where service processes or systems were determined to be a significant causal or contributing factor to the incident, CIMS will suggest that a Root Cause Analysis is the most appropriate review approach

|  |
| --- |
| Where Root Cause Analysis is recommended the user **may choose to select Case Review.** |



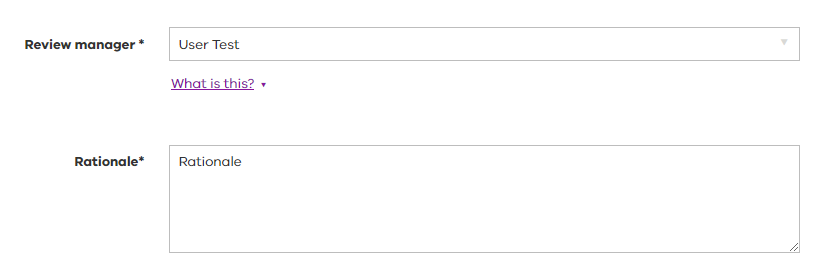
1. Select the **type of review** to be undertaken
2. Choose the **review manager** from the dropdown list
3. Enter the **rationale** of the proposed approach.

### Review by Case Review



Where service processes or systems were not determined to be a significant causal or contributing factor to the incident, CIMS will suggest that a Case Review is the most appropriate review approach

|  |
| --- |
| Where Case Review is recommended the user **may choose to select Root Cause Analysis.** |



1. Choose the **review manager** from the dropdown list
2. Enter the **rationale** of the proposed approach.

## Finalise and submit

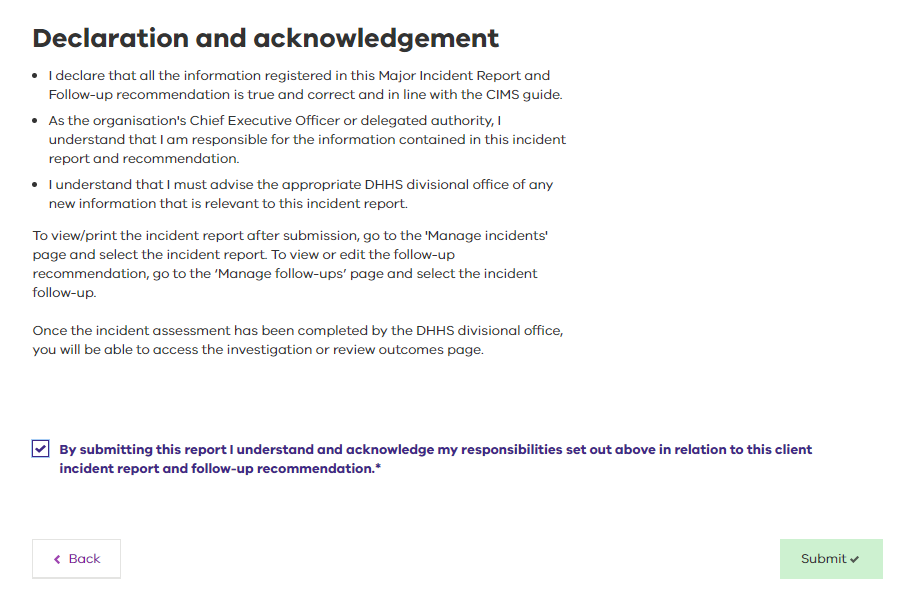
The function buttons are available at the bottom of the **major incident authorisation** screen.

|  |  |
| --- | --- |
| Button | Description |
| Return | Select **Return** if the incident needs to be returned for rework. This function is only available for Senior Delegate user roles. For further information refer [Returning an incident for rework](#ReturnIncident). |
| Withdraw | Select this option if the incident is out of scope and needs to be withdrawn from the reporting process. For more information refer to [Withdraw function](#_10._Withdraw_function_1). |
| Save | Select **Save** to make any changes to the incident. A message confirming the status of the save request is displayed. |
| Back | Select **Back** to return to a previously viewed page. |
| Next | Select **Next** to move to the next page to continue completing the response.  The **Declaration and acknowledgement** screen will be displayed. |

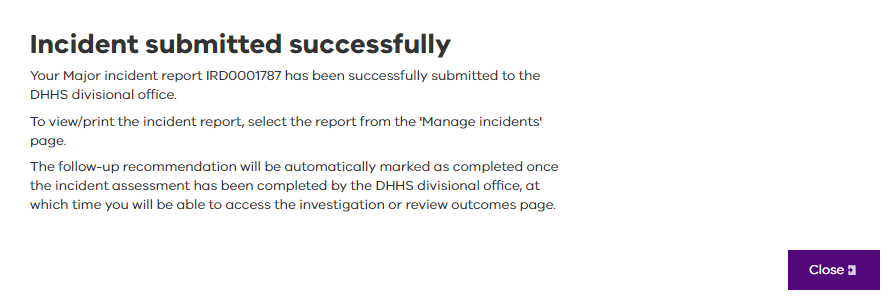
Selecting the **Declaration and acknowledgement** statement ‘by submitting this report I understand and acknowledge my responsibilities set out above in relation to this client incident report’ confirms that the organisation’s CEO or Senior Delegate user understands that:

* All the information registered in the major impact incident report is true and correct.
* They are responsible for the information contained in the major incident report.
* They will advise the appropriate department divisional office of any new information that arises relevant to the incident.

1. Select **Submit**.



The **Incident submitted successfully** message will be displayed. This confirms that the incident report has been forwarded to the department divisional office with CEO’s or Senior Delegates approval on their responsibilities and confirmation of a thorough review being completed.



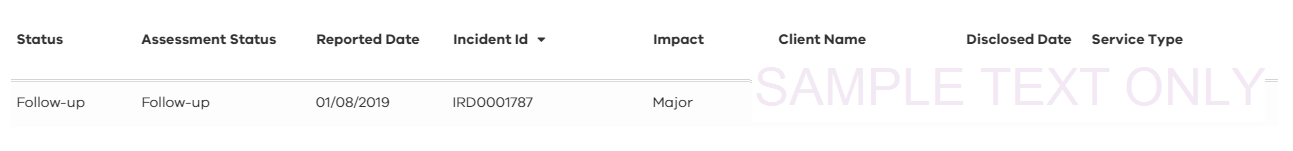
1. Select **Close**.

The **Manage incidents** screen will display. The major impact incident report will now reflect changes to incidents status and assessment status:

* **Status**: Submitted
* **Assessment Status**: Received

Once the incident assessment has been completed by the department, the incident will show:

* **Status**: Follow-up
* **Assessment Status**: Follow-up



# Additional **follow-up recommendations**

Initial follow-up recommendations are completed as part of major incident submission and approval. Following completion of the incident assessment by the department, subsequent follow-up recommendations may be added to the incident at the discretion of the service provider.

Follow-up recommendations can be added from the **Incidents (Manage Incidents) screen and from the Follow-ups (Manage Follow-up) screen.**

**Monitoring and actioning the follow-up recommendations is conducted from the Follow-ups (Manage Follow-up) screen.**

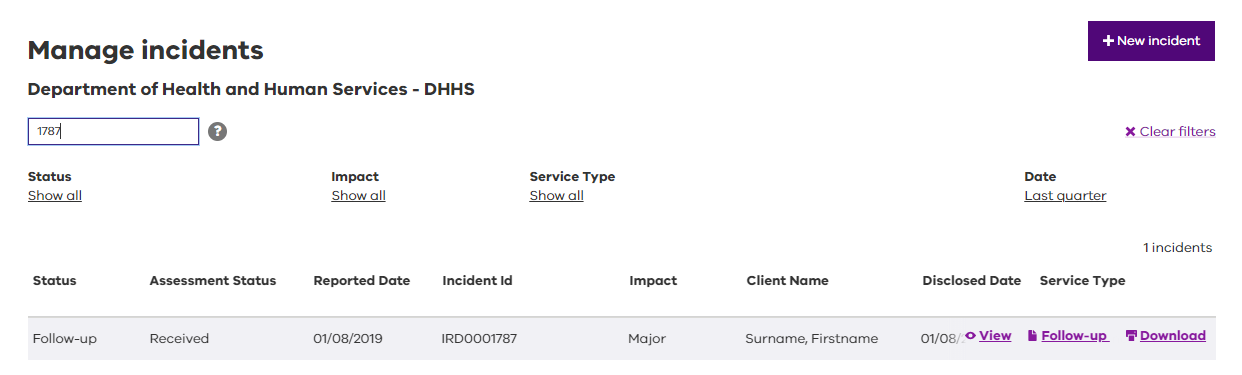
**Note: only a Senior Delegate user can create a follow-up recommendation for investigation or review of a major impact client incident.**

## **Creating an additional follow-up recommendation**

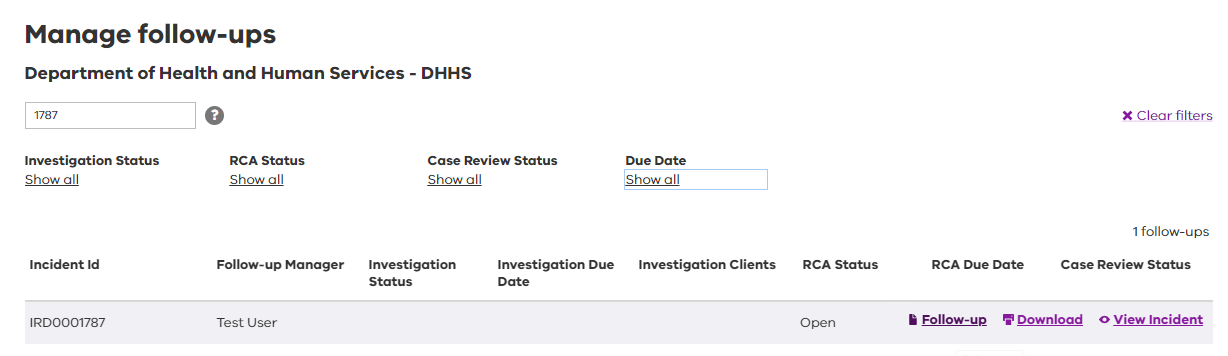
|  |
| --- |
| The primary (or initial) follow-up recommendation is created as part of major incident authorisation, any subsequent recommendation can only be created and submitted to the department divisional office after the incident report has been submitted. |

### From the manage Incidents screen

1. Locate the incident report from the **Manage incidents** screen. Refer to [Using the filter, search and sort tools](#Navigation) for assistance.



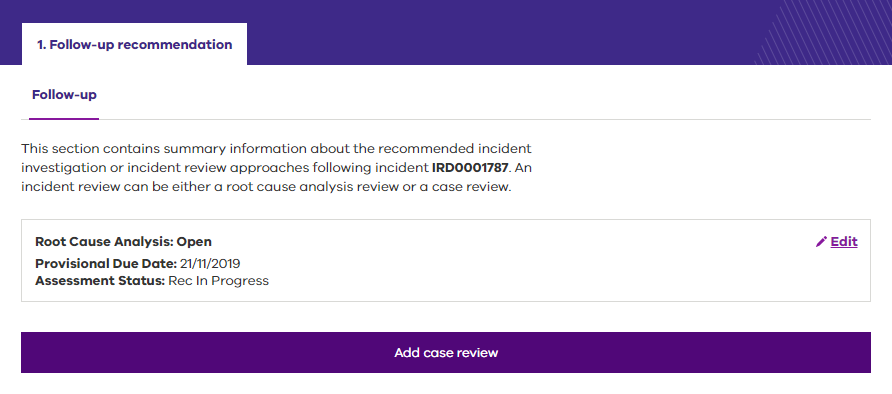
1. Alternatively, you can locate the incident report from the **Manage follow-ups** screen. Refer to [Using the filter, search and sort tools](#Navigation) for assistance.



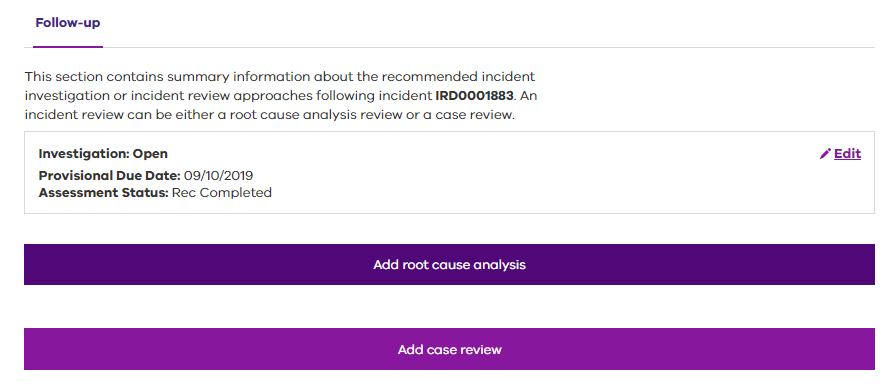
1. Hover the mouse over the incident report and select the **Follow-up** action button. The **Follow-up recommendation** screen will display.

|  |
| --- |
| **When the mandatory investigation criteria are met,** and an Investigation is created as part of the incident submission process, additional Root Cause Analysis and Case Review recommendations may be created.  **When the mandatory investigation criteria are not met,** no subsequent Investigation recommendation may be created, however a subsequent further review by either Root Cause Analysis or Case Review may also be created. |

The **Follow-up recommendation** screen displays a summary of the incident’s review history. In this example, a Root Cause Analysis follow‑up recommendation has already been made as part of the incident submission process; this means that only an additional review by Case Review may be created.



In this example, an Investigation follow‑up recommendation has already been made as part of the incident submission process; this means that additional reviews by Root Cause Analysis and Case Review may be created.

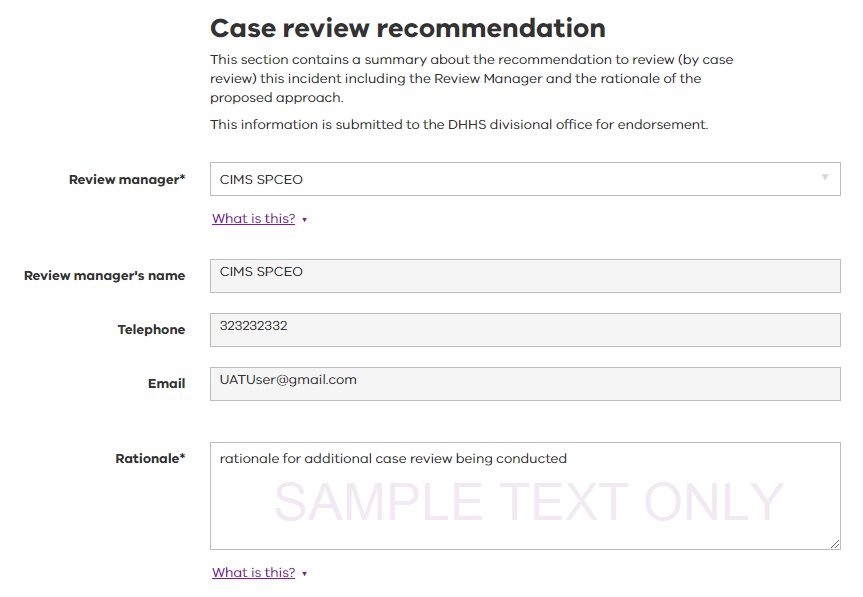


### Add a case review

1. Select **Add case review**
2. Select the **Review Manager** from the dropdown box.

* The Review manager details will automatically populate

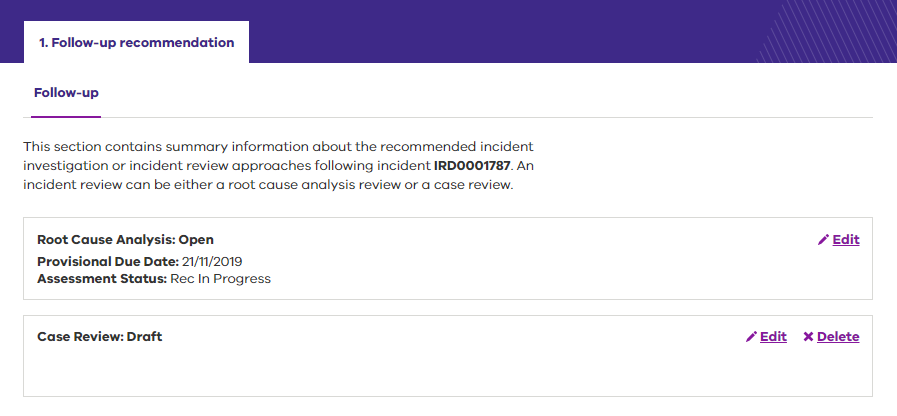
1. Enter the **rationale** for creating an additional review



There are three option buttons available at the completion of entering all information for the investigation. These are:

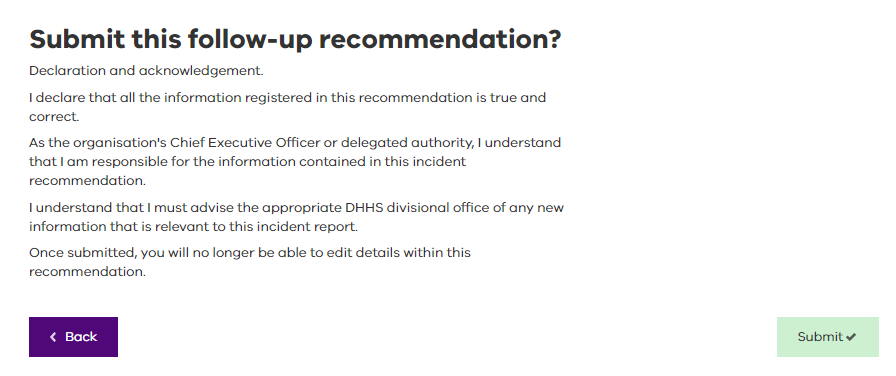
|  |  |
| --- | --- |
| Button | Description |
| Submit | This button prepares the incident investigation for submission to the department for endorsement. |
| Save & close | This button saves and closes the investigation recommendation. It has not been submitted to the investigation manager and can be returned to at a later time. |
| Back | Select **Back** to return to a previously viewed page without saving the recommendation. |

1. Select **Save** to return to the Follow-up summary screen. The saved recommendation is shown with a **Draft** status and can be edited and completed, or deleted, as appropriate.

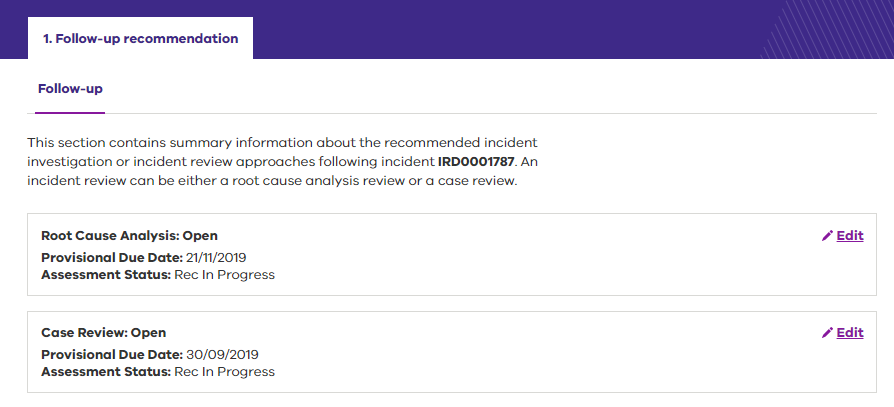


1. Select Submit to complete the recommendation and submit to the department divisional office.

* It is important to read and understand the responsibilities of submitting a follow-up recommendation particularly that the information is confirmed to be true and correct and will no longer be editable by the Senior Delegate once submitted.

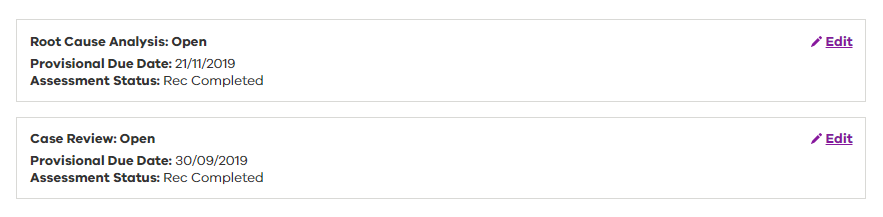


1. Select **Back** to return to the previous screen or select Submit to confirm the recommendation and return to the Follow-up summary screen.



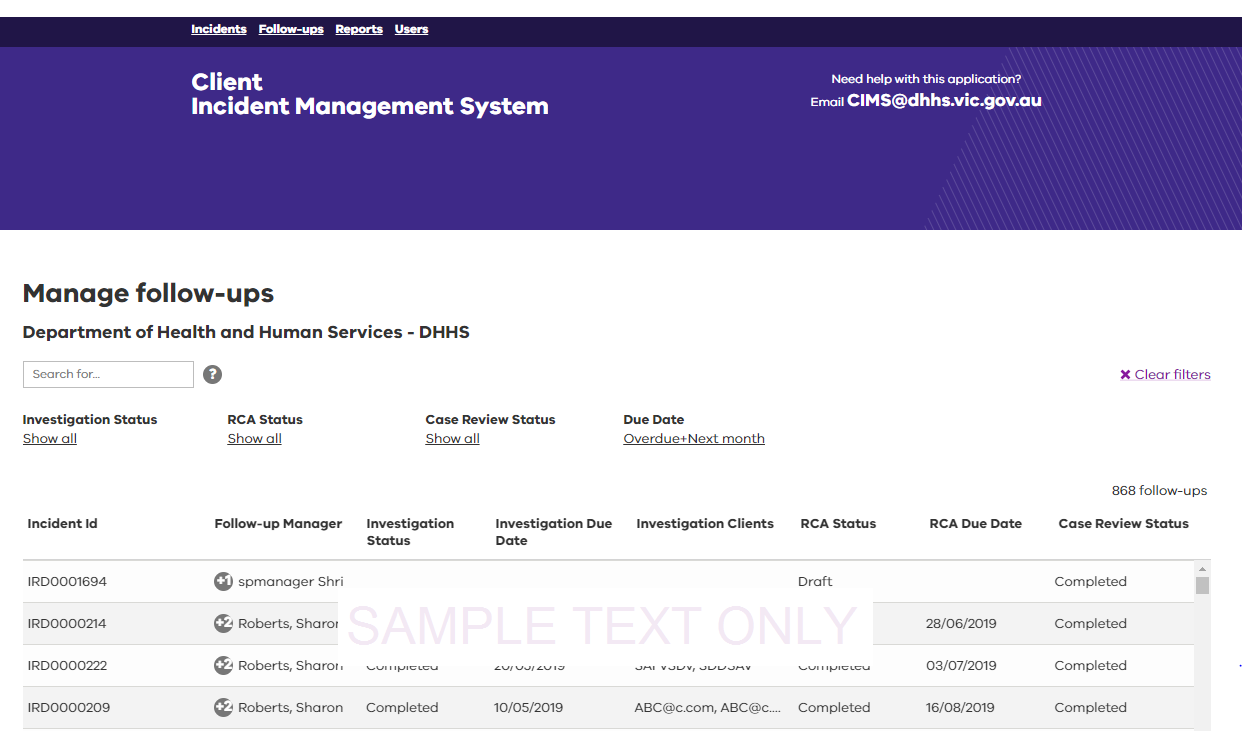
While the incident assessment is in progress, any associated follow-up recommendations will remain in **Recommendation in progress** status.

Once the department has completed the incident assessment, these recommendations will automatically progress to **Recommendation Completed** status.



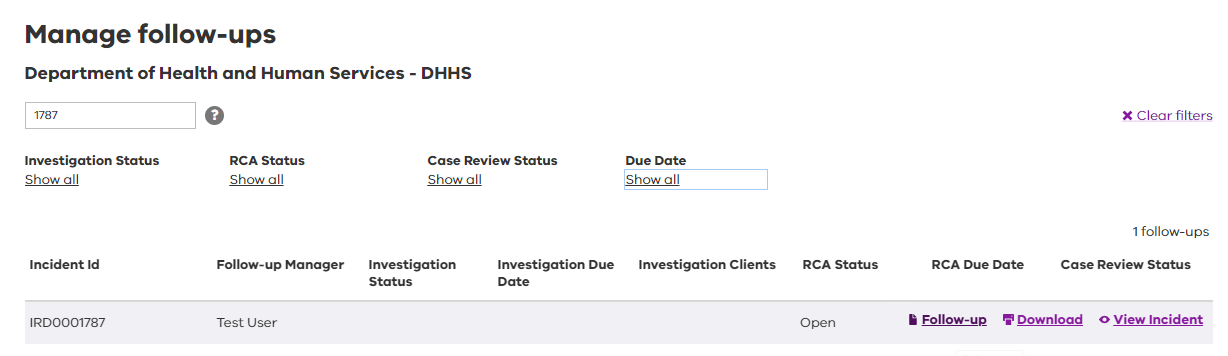
# Major impact – follow-up outcomes

The **Manage follow-ups** screen is used for viewing and completing follow-up outcomes; follow-ups can be accessed directly from this screen, as well as from the **Manage incidents** screen. See [Using the filter, search and sort tools](#Navigation) for assistance.



Access to follow-up recommendations and outcomes within the **Manage follow-ups** screen is restricted to Senior Delegate users, and assigned Investigation/Review Managers.

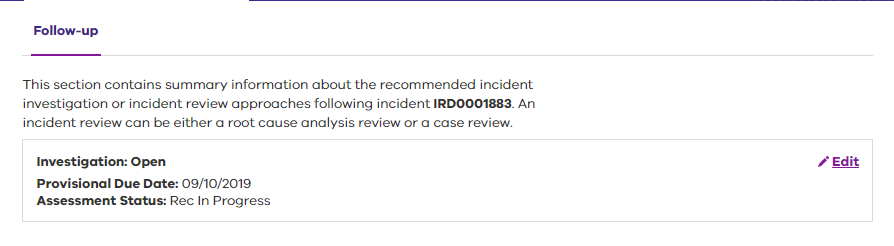
Investigations, root cause analysis reviews and case reviews once added in the system are escalated to the Senior Delegate user for endorsement. This screen provides a list of client incident reports that have been allocated to the manager or senior delegate for review and action.



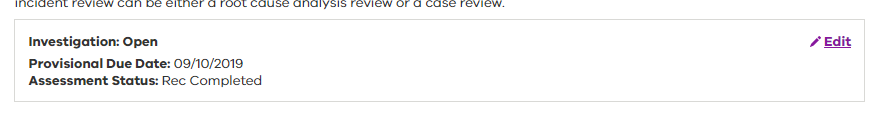
Hover the mouse over any of the incident reports on the **Manage follow-ups** screen to display available action buttons.

|  |  |
| --- | --- |
| Action button | Description |
| Follow-up | This function displays the follow-up summary screen for an incident report.  See 5.6 Additional follow-up recommendations |
| Download | This function enables the incident report to be exported or saved in a pdf document. |
| View incident | This function enables the incident report to be opened and the details viewed. |

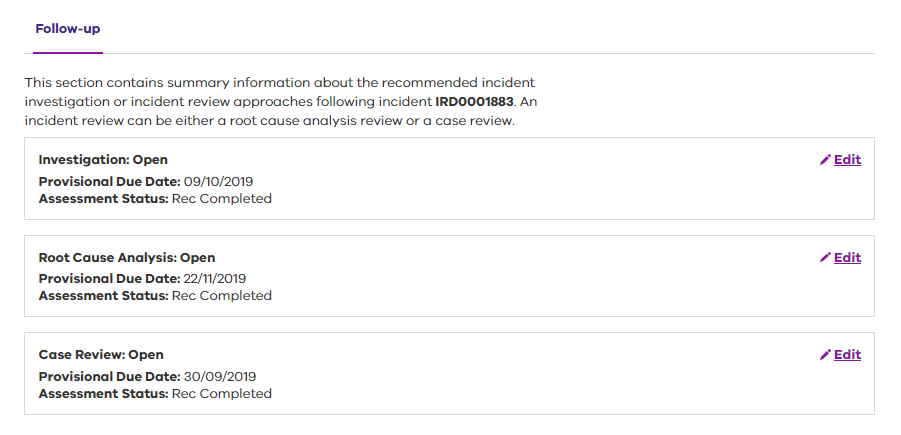
The **Follow-up recommendation** screen displays a summary of the incident’s review history. In this example, an Investigation recommendation has been made as part of incident submission. As the incident assessment is not yet complete, the status is **Recommendation in Progress**.



Once the assessment has been completed, the status will progress to **Recommendation Completed**, and at this stage an **Investigation Outcome** can be added.



|  |  |
| --- | --- |
| Action button | Description |
| Edit | This function opens the follow-up to either view or edit its content. |
| View | This function allows the follow-up recommendations and any outcomes to be viewed. |



|  |
| --- |
| The **status** of the follow-up recommendation (Investigation, Root Cause Analysis and Case Review) is from the perspective of the service provider.  The **provisional due date** is the system generated due date specific to the follow-up recommendation.  The **assessment** **status** is from the perspective of the department divisional office. |

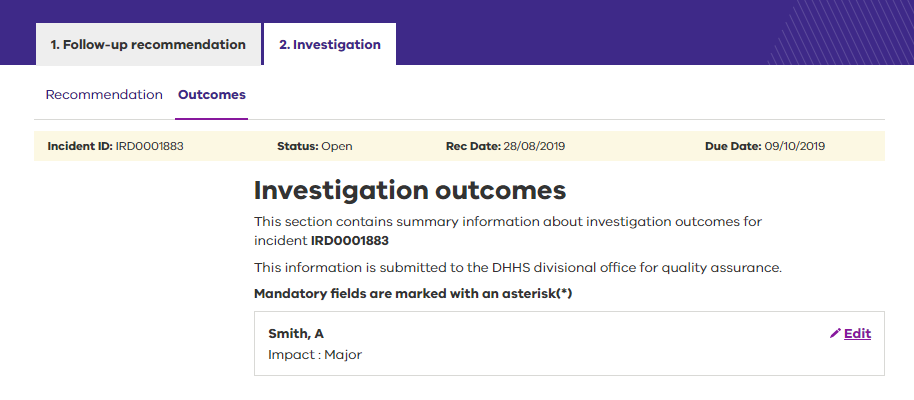
See [Appendix C: Service Provider system status](#_Status_descriptions) and [Appendix D: Department divisional office status](#_Appendix_D:_Department) for further information.

## Add an investigation follow-up outcome

1. Select **Edit**

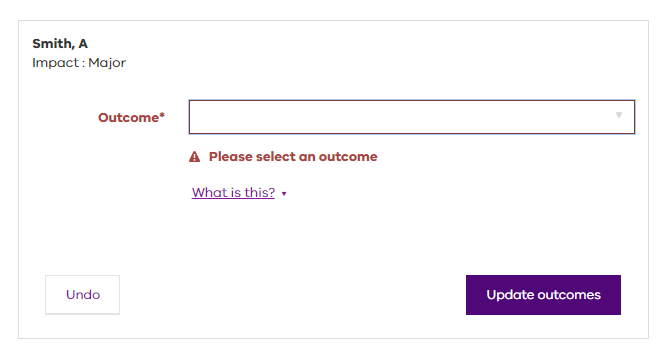
* This action will display a summary of the follow-up recommendation to review prior to adding the follow-up outcome.
* The Investigation Manager may be edited at this stage.

1. Navigate to the Outcomes screen by selecting either the **Outcomes** link at the top of the screen or the **Next** button at the bottom of the screen.
2. For each client impact to be investigated, select **Edit** to add an outcome.



1. Select the **Outcome** dropdown to select an outcome from the listing generated.

* This refers to the primary investigation outcome that best describes the investigation findings in relation to that client.



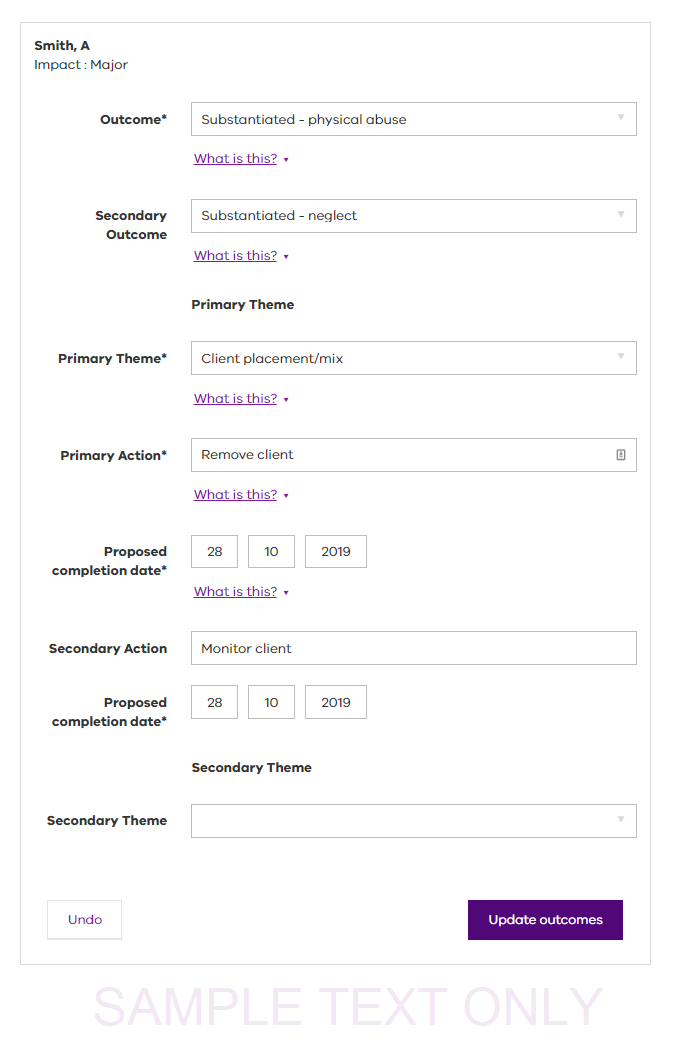
### Outcome options

* Substantiated – physical abuse
* Substantiated – sexual abuse
* Substantiated – emotional/psychological abuse
* Substantiated – financial abuse
* Substantiated – neglect
* Not substantiated – further action required
* Not substantiated – no further action required
* Pending

### Pending outcomes

Outcomes of ‘Pending’ are only applicable when the inability to continue an investigation is outside of department control. An example of this would be if the incident involved a police investigation and further instructions were awaited.

Prior to submission, the user must complete and attach the **Incident investigation/review on hold request** using the template provided and detailing the rationale for the incident investigation/review being on hold, and providing the proposed new due date for completion. See 6.2 Requesting an investigation or review extension.



1. Select the **Secondary Outcome** field if necessary.

* If applicable, select a secondary outcome if the findings from the investigation determine there is a secondary outcome in relation to the client.

1. Select in the **Primary Theme** field to select a primary theme if required.

* This is the theme that best describes the primary action to be undertaken in response to the investigation.

|  |
| --- |
| There are a number of fields where a theme is required. A theme is best described as a category. For example, several incidents occurring where investigation has revealed that the underlying cause was lack of staff training. Staff training would be considered the theme as it is a common thread linking the incidents. |

1. Enter the **Primary Action**.

* Enter the summary details of the primary action to be undertaken in response to the investigation.

1. Enter the **Proposed completion date**.

* This is the date by which the primary action will be completed.

1. Enter the **Secondary Action**.

* Enter the summary details of the secondary action to be undertaken, if necessary, in response to the investigation.

1. Select in the **Secondary Theme** field to select a secondary theme if necessary.

* This is the theme that best describes the secondary action to be undertaken in response to the investigation.

1. Select **Update outcomes** to save changes.

* The **Investigation outcomes** screen displays.

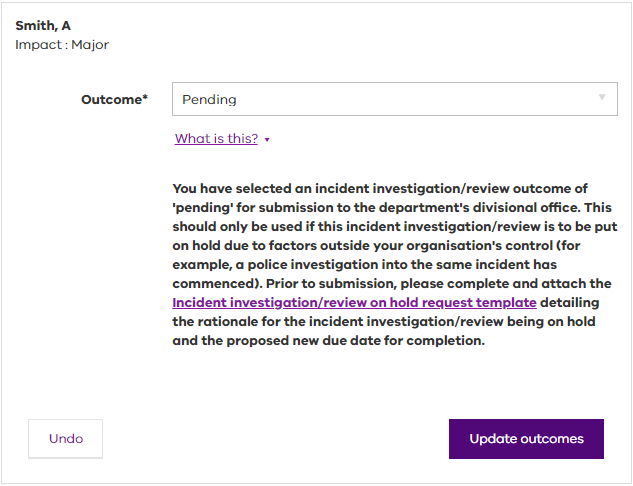
Select **Edit** for other clients, if necessary, and repeat from Step 2.

## Request an investigation or review extension

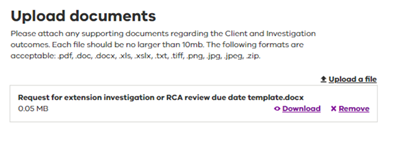
Under specific circumstances, it may be necessary to place an investigation on hold. In these cases, the outcome should be shown as ‘Pending’.

To place an investigation on hold, go to the **Review outcomes** screen and follow these steps:

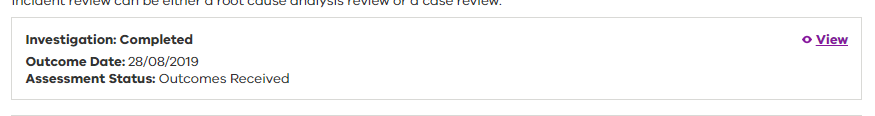
1. Select in the **Outcome** field to select ‘Pending’ from the dropdown list. Further information is displayed, along with a link to a template.



1. Select the **Incident investigation/review on hold request template** link. The template is available on the CIMS website.
2. Complete the template and return to the **Investigation outcome** screen.
3. Select **Update outcomes**.
4. Attach the completed **Incident investigation/review on hold request template in the Upload documents attachments section.**

****

1. **Submit and Confirm when completed and return to the Follow-up summary screen.**



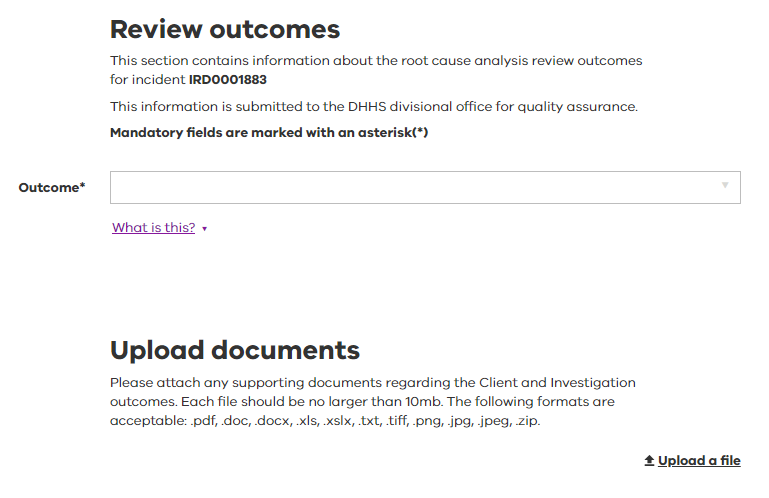
## Add a root cause analysis follow-up outcome

1. From the Follow-up summary screen, select Edit

* This action will display a summary of the follow-up recommendation to review prior to adding the follow-up outcome.
* The Review Manager may be edited at this stage.



1. Navigate to the Outcomes screen by selecting either the Outcomes link at the top of the screen or the Next button at the bottom of the screen.
2. Select Edit
3. Navigate to the Outcomes screen by selecting either the **Review** **outcomes** link at the top of the screen or the **Next** button at the bottom of the screen.



1. Select in the Outcome field to display the outcome options.

* If no further action is required, proceed to Step 8. If further action is required, continue to the next step.

1. Select Further action required. The Theme 1 field is displayed.
2. Select in the Theme 1 field to select a theme from the list. The Theme 2 field is displayed.

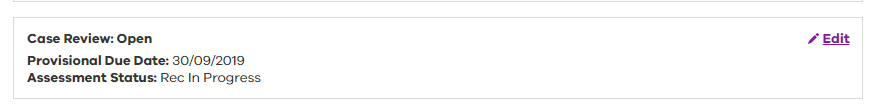
* The Theme 2 field is not mandatory but can be completed if necessary by Selecting in the field to reveal a list of options. Select the most appropriate option. If you complete the Theme 2 field, a third theme field is displayed. Repeat the Theme 2 procedure to complete this field.

1. Select the Upload a file link. A browse screen is displayed, enabling you to locate and select the files to be uploaded to the review.

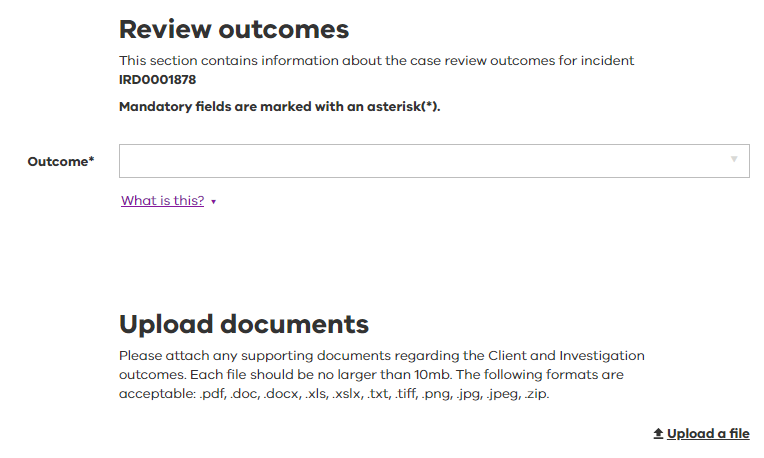
## Add a case review follow-up outcome

1. From the Follow-up summary screen, select **Edit**

* This action will display a summary of the follow-up recommendation to review prior to adding the follow-up outcome.
* The Review Manager may be edited at this stage.



1. Navigate to the Outcomes screen by selecting either the **Review** **outcomes** link at the top of the screen or the **Next** button at the bottom of the screen.



1. Select in the Outcome field to display the outcome options.

* If no further action is required, proceed to Step 8. If further action is required, continue to the next step.

1. Select **Further action required**. The Theme 1 field is displayed.
2. Select in the Theme 1 field to select a theme from the list. The Theme 2 field is displayed.

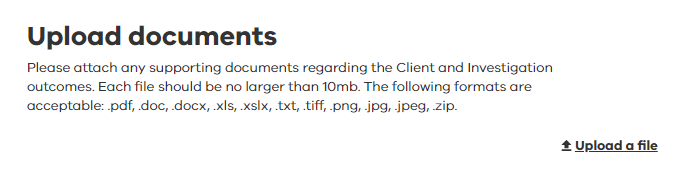
* The Theme 2 field is not mandatory but can be completed if necessary by Selecting in the field to reveal a list of options. Select the most appropriate option. If you complete the Theme 2 field, a third theme field is displayed. Repeat the Theme 2 procedure to complete this field.

1. Select the Upload a file link. A browse screen is displayed, enabling you to locate and select the files to be uploaded to the review.

## Upload documents

Documents that record and support the investigation process and the outcomes of the investigation into a client incident can be attached to the incident. This includes substantiating documents when an investigation is placed on hold with a status of ‘Pending’.

Uploaded files should be no larger than 10 MB. The following formats are acceptable: pdf, doc, docx, xls, xlsx, txt, tiff, png, jpg, jpeg, zip.

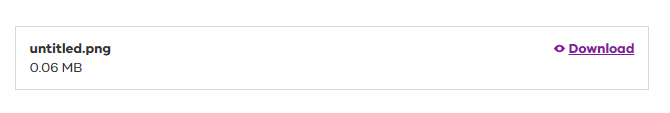


1. For an outcome (investigation, root cause analysis, case review) select the **Upload a file** link.
2. Navigate to the folder containing the files to be uploaded.
3. Select to highlight the file to be uploaded.
4. Select **Open**. The file is not actually being opened, it is being uploaded to the investigation record. The name of the file attached will be displayed under the **Upload documents** heading.
5. To upload more files, repeat from Step 1. Alternatively, continue to the next step.
6. Select **Save & close**.

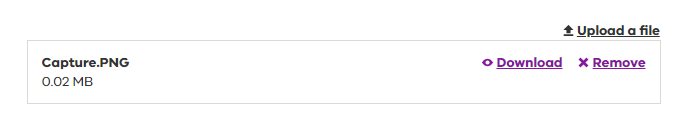
|  |
| --- |
| Case review outcomes do not require endorsement and cannot be withdrawn by the department.  Case review outcomes progress to **Outcomes completed** status automatically on submission. |

## Download or remove documents

Where an outcome has a document attached, that document can be downloaded by selecting the **Download** link



Where a saved outcome has a document attached, that document can be removed by selecting the **Remove** link, and a replacement document uploaded.



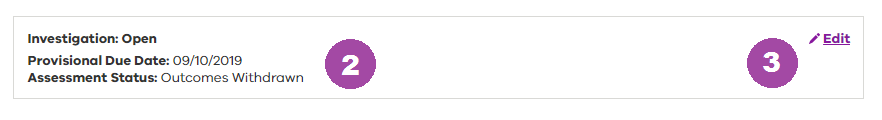
## Withdrawn outcomes

Where a follow-up outcome (investigation or root cause analysis) is withdrawn by the department, the investigation will display as:

1. **Open** on the Manage follow-ups screen; and as
2. **Outcomes Withdrawn** on the Follow-up summary screen.



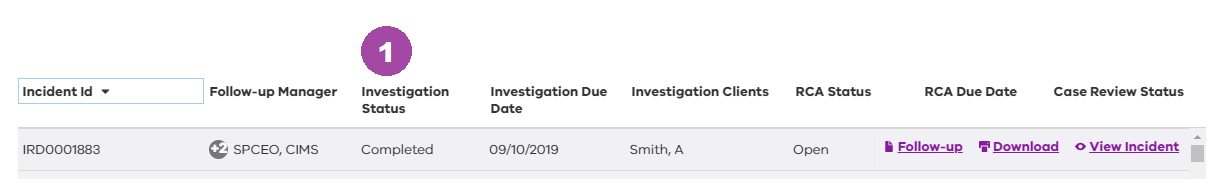
1. From the Follow-up summary screen, select **Edit** to revise and resubmit the outcome.

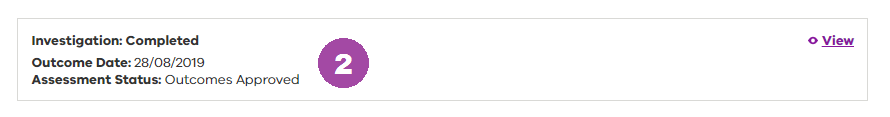


## Approved outcomes

Once an outcome (investigation or root cause analysis) has been accepted and endorsed by the department the investigation will display as:

1. **Completed** on the Manage follow-ups screen; and as
2. **Outcomes Approved** on the Follow-up summary screen.

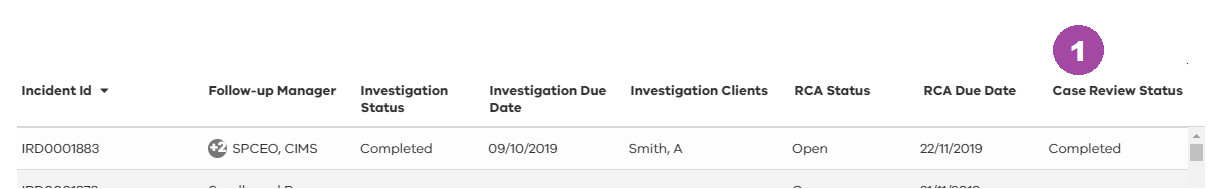


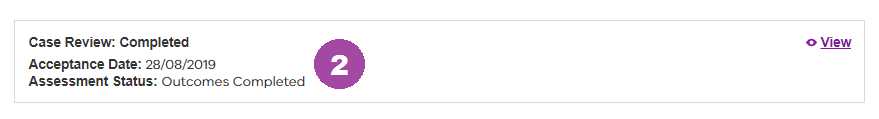


## Completed outcomes

Case review outcomes do not require endorsement and cannot be withdrawn by the department. On acceptance of the outcome by the Senior Delegate, the case review outcome is automatically Completed and displays as:

1. **Completed** on the Manage follow-ups screen; and as
2. **Outcomes Completed** on the Follow-up summary screen





# Withdraw/Out of Scope function

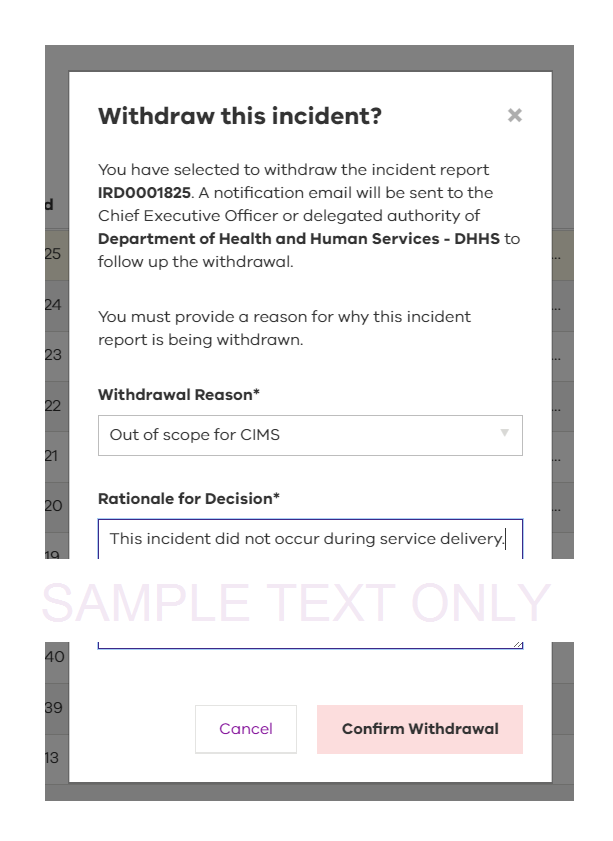
Non-major impact incidents are out of scope if they did not occur during service delivery or they did not cause harm to the client despite having the potential to.

**Note:** a request from the department divisional office for an incident report is not a request for the incident report to be withdrawn.

If an incident is out of scope, a manager or Senior Delegate user can withdraw it. A client incident report withdrawal commences at the **Manage incidents** screen. Use the sort and search functions to help locate the incident report.

Refer to [Using the filter, search and sort tools](#Navigation) for assistance.

1. Hover the mouse over the required incident report for the **Withdraw** beside the incident to be withdrawn. The **Withdraw this incident?** screen is displayed.



1. Select a **Withdrawal Reason** from the list that most accurately reflects the reason for the withdrawal. Options available are:
   * + Out of scope for CIMS
     + Review address details
     + Review assessment of impact on client/s
     + Review client/s details
     + Review immediate responses
     + Review incident description
     + Review incident type/s
     + Review staff/other details.
2. Enter a **Rationale for Decision**.
3. Select **Confirm Withdrawal**. The **Manage incidents** screen is displayed.

|  |
| --- |
| To cancel the withdraw request, Select **Cancel** to be returned to the **Manage incidents** screen.  Note: Only incident reports that are out of scope of CIMS and do not require submission to the department divisional office should be withdrawn.  Once an incident has been withdrawn, it will no longer be available for editing or resubmission. |

# Download an incident report

Individual client incidents reports can be downloaded for saving or printing.

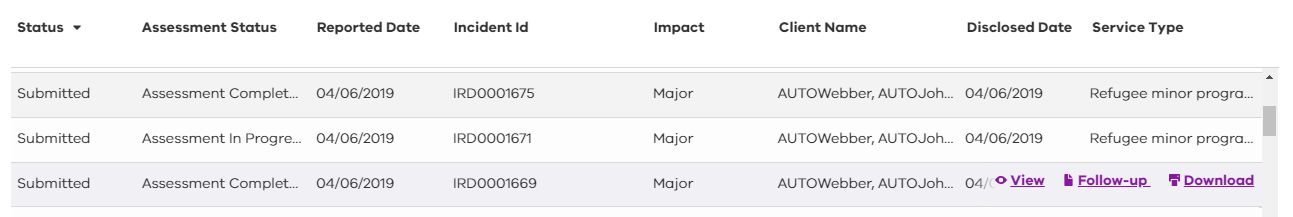
|  |
| --- |
| Downloading, saving or printing any document must comply with privacy regulations. |

A client incident report can be downloaded from either the **Manage incidents or Manage follow-ups** screens.

Use the sort and search functions to help locate the incident. Refer to [Using the filter, search and sort tools](#Navigation) for assistance.

### Saving and printing a downloaded client incident report:

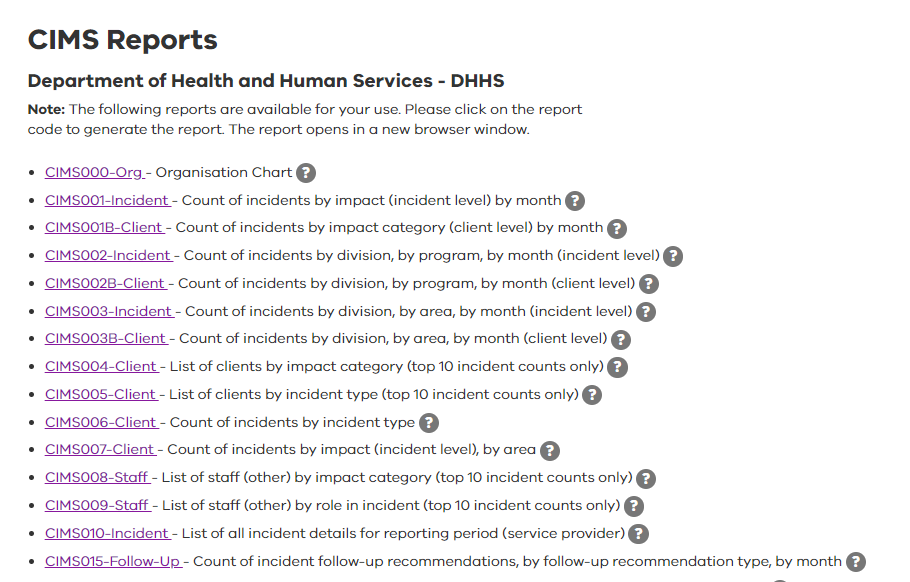
1. Hover the mouse over the client incident report required and select **Download action button**.



1. The client incident report is automatically converted to a PDF document at the bottom of the screen.
2. Selecting the client incident report from the bottom of the screen will enable the PDF document to be viewed.
3. To **Save** the viewed PDF document, select the drop-down arrow available at the top right hand side of the viewed document and follow the prompts.
4. To **Print** the file, select the printer icon to the top right-hand side of the viewed document.

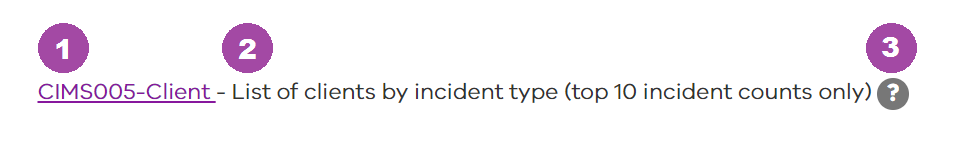
# Generate reports

The **CIMS Reports** menu provides a list of reports available to registered users dependent on their user’s provisioning.



For each report:

1. The underlined text is the heading of the report and acts as link to the report when selected.
2. The plain text is a short description of the report.
3. Selecting the question mark icon reveals further information about the report. Select the question mark icon a second time to close the information section.



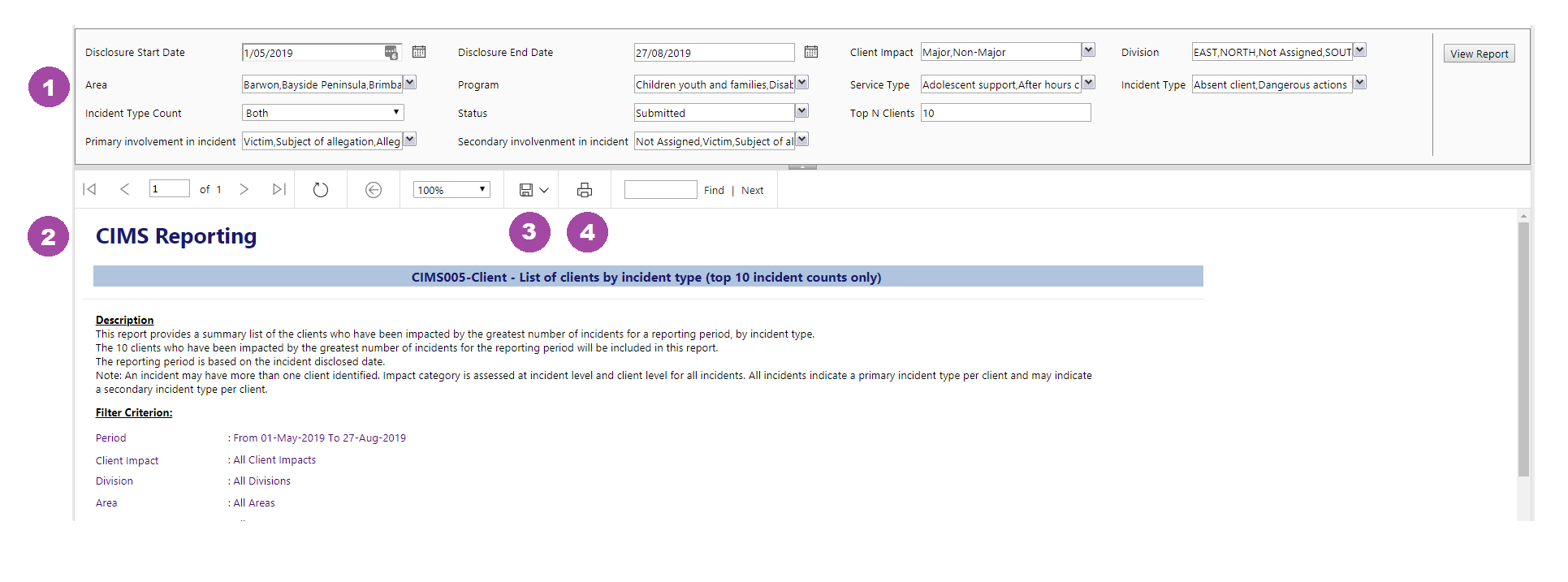
Select the heading of the required CIMS report. Once selected, the CIMS report will open in a new browser window.

This screen is divided into two sections.

1. The top section contains a number of editable fields that enable you to filter the information to be included and displayed in the report.
   * + All report templates have these filter fields although the fields will differ depending on the type of report being generated.

The lower section of the screen displays:

1. Report details
2. Save icon
3. Print icon.



### To generate a report:

1. Find the report to be generated.
2. Select the link for the chosen report. The report template is displayed as shown above.
3. Work through each of the editable fields to define the details of the report.
4. Select **View Report**. The lower section on the report displays the details of the report based on the defined filters.
5. Select the **Save** icon to save the report, or the **Print** icon to send the report directly to the printer.

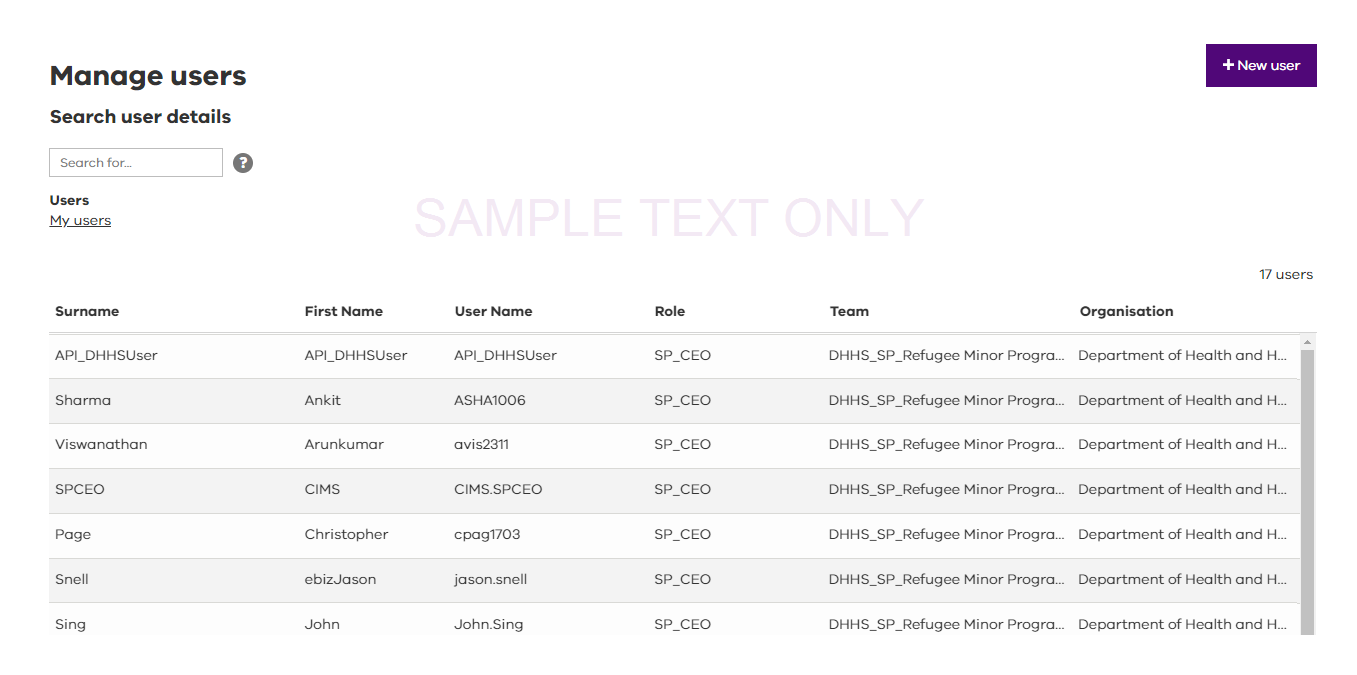
# Manage user profiles

Senior Delegate users have the added functionality of managing user profiles within their assigned teams within CIR. Assigned teams are workflow structure of users.

From the **Manage users** screen, Senior Delegate users can create, edit and remove registered users to CIR; Manager, Investigation manager/review manager and Read-only.

The **Manage users** screen displays the list of registered users with access to CIR and the following information:

* Surname
* First Name
* User Name
* Role
* Team
* Organisation

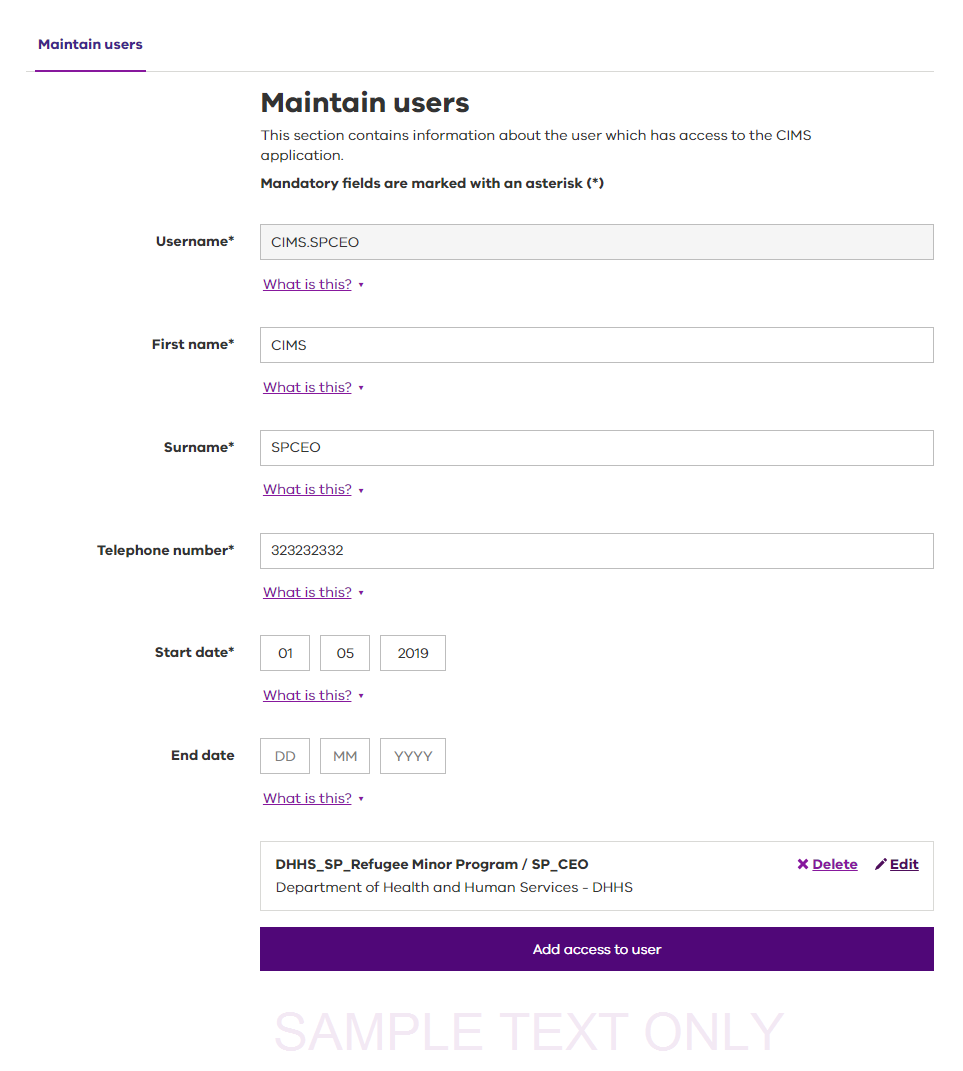


|  |  |
| --- | --- |
| Function | Description |
| Search for… | This field enables a search from all of the columns displayed in the **Manage users** table. The system begins identifying a match once the search criteria is entered. A search is not able to be completed on the Role column. |
| Question mark icon | Select this icon to view what is allowed by the free text search. |
| Users | Select on the **Users** heading to sort the users by following:   * my users – active users within your team * deactivated users – former users who no longer have provisioning within your team * show all – all users (regardless of active status) within the organsation. |
| Column headings | Column headings can be selected to change the view order of the table information to either ascending or descending. |

## Add a new user profile

Creating new users, with associated functionalities, within CIR is completed by Senior Delegate level users.

1. Conduct a quick search before starting to ensure a record of the user has not already been created.
2. Select the **+New user** button. The **Maintain users** screen is displayed.



1. Enter the **Username**.

* This is the name by which CIMS IT will know the user. For department users, this could be the HSNetID. For all other users, this will be the eBusiness ID.
* The HSNetID should be in the format **JTho1212**
* The eBusiness ID is normally **Firstname.Surname.**

1. Enter the **First name**

* This is the first (given) name of the person to be added as a user in CIMS IT.

1. Enter the **Surname**

* This is the surname (family or last) name of the person to be added as a user in CIMS IT.

1. Enter the **Telephone number**

* Enter the best telephone number on which to contact the user. It should be all numbers with no spaces.

1. Enter the **Start date**

* This is the date from which the user has access to allocated functions within CIMS IT.

1. Enter the **End date**

* This is the date to which the user has access to CIMS IT. After this date, the user will no longer be able to access CIMS IT.
* Do not complete this section if there is no end date.

1. Select in the **Organisation** field to choose the required organisation from the activated drop-down list.

* This is the organisation that the user belongs to.

1. Select in the **Role** field to choose the required role from the activated drop-down list.

* The role reflects the user’s level of access to client incident details and available functions the user can perform in CIMS IT. Refer to [Appendix B: Service provider user roles](#_Appendix_B:_Service).

1. Select in the **Team name** field to choose the required team name from the activated drop-down list.

* The team name refers to the team the user will belong to in respect of the organisation identified earlier. A team that does not exist can be added via the Manage teams page.

1. Enter an email address in **Email**.

* The email address should be the best business email address to contact the user on.

1. Select **Add access**. The user’s details are recorded and the level of access.
2. Select **Save & close**. A message confirming the successful addition of the user will be displayed.

## Edit user profiles details

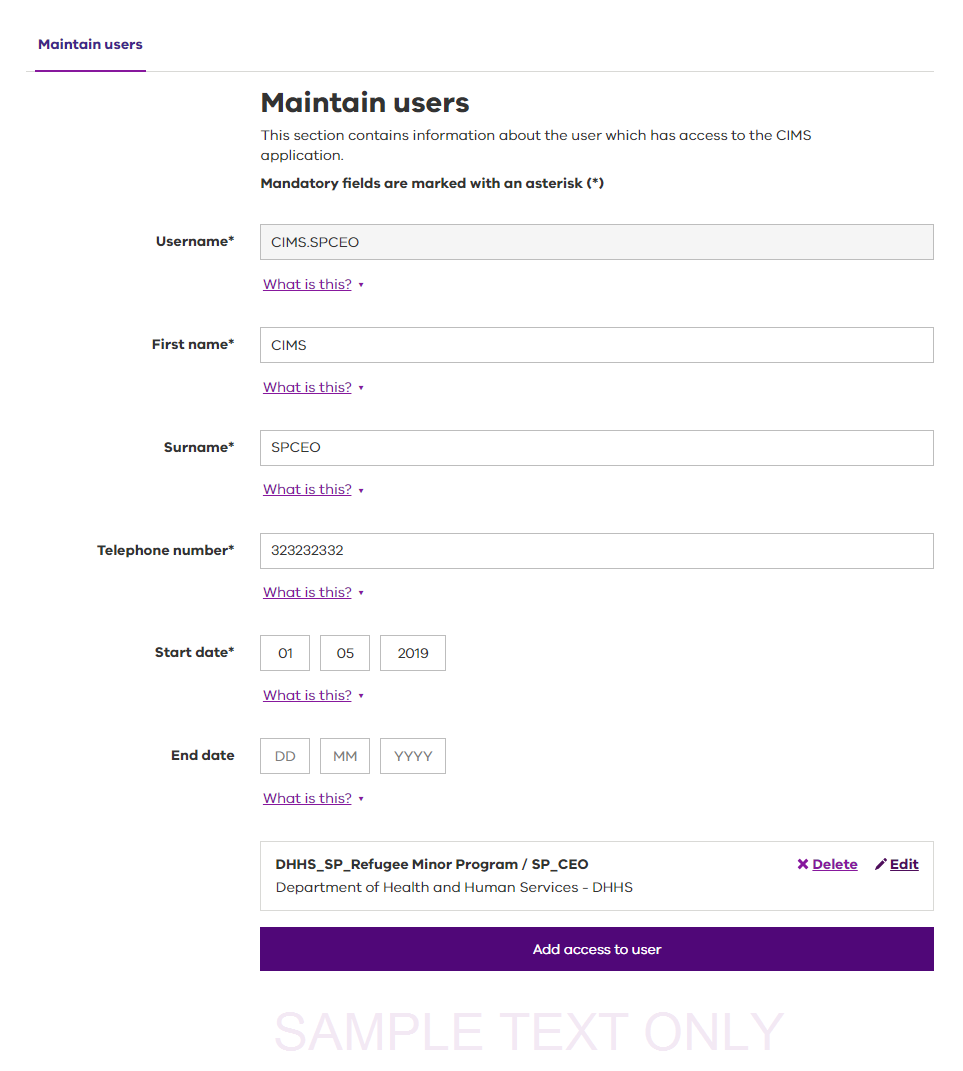
Editing existing user profile details within CIR is completed by Senior Delegate level users. User profile details include the CIMS nominated user name, first name, surname, telephone number, start and end date of using CIMS.

1. Search for the user profile required. Refer to [Refined searches using the search, filter and sort tools](#_Refined_searches_using) for further information.
2. Select the **Edit** action button.



The user profile details can be edited directly.

To add or change user access levels select



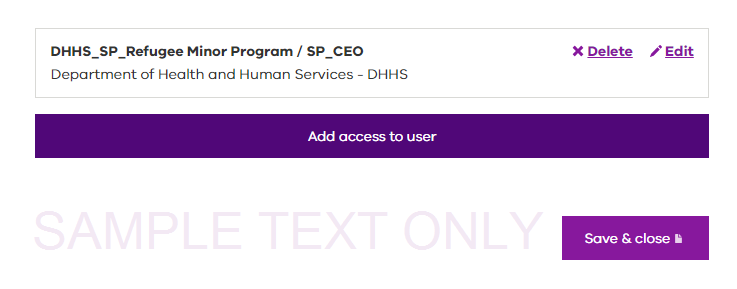
1. Changes to the user profile registered in CIMS can be made here.

Note: deactivating a user that is assigned to an investigation or review as the manager will require the investigation or review to be assigned to an alternative user.

## Editing user profiles access

Senior Delegates can amend existing user’s access to CIMS IT functions.

See [Adding a new user](#AddingNewUser)and follow from Step 8 for information about completing this screen.

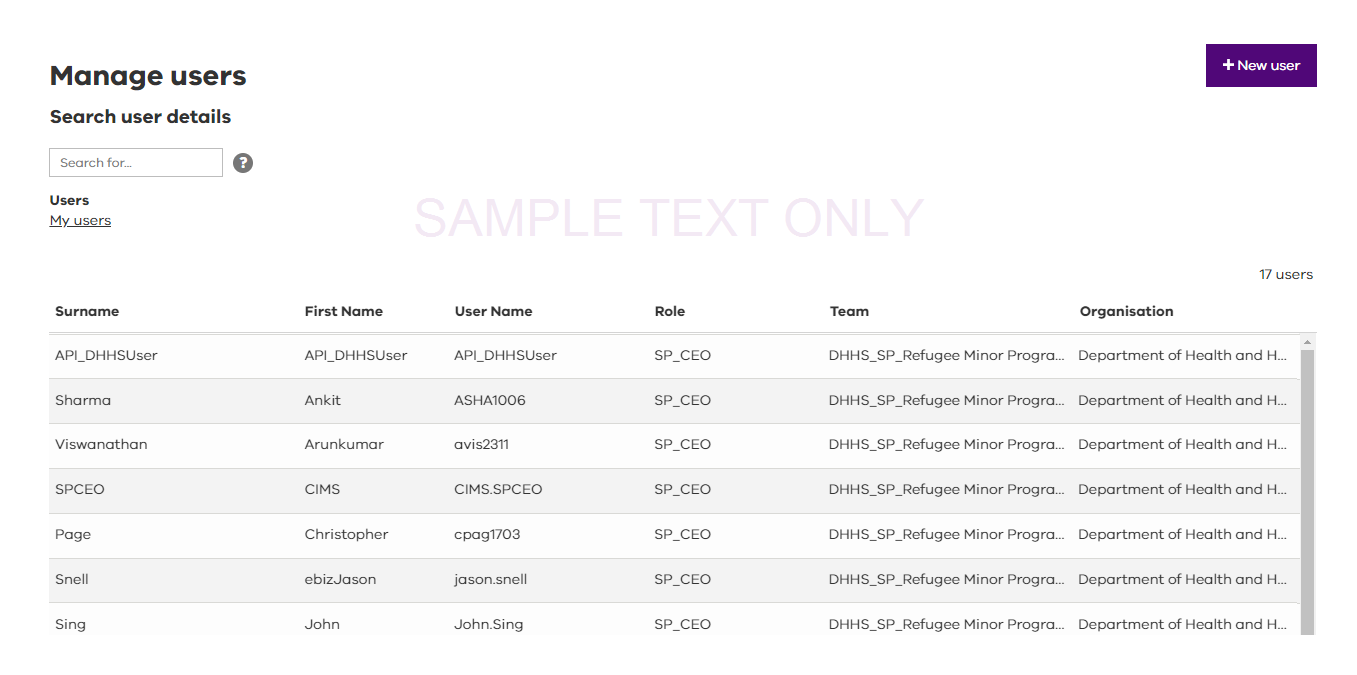


Note: changes made to the information recorded here may impact incidents and recommended investigative activities that have been assigned to the user.

## Assigning existing user profiles to a team

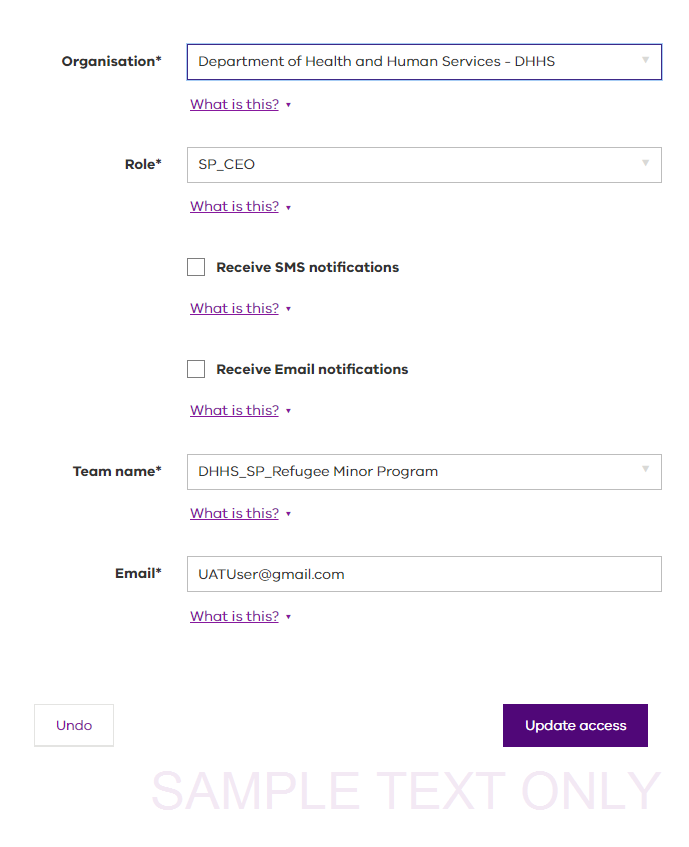
A Senior Delegate user is only able to assign existing user profiles to the teams they manage.

The Senior Delegate will need to need to change the CIMS IT view to **Show all** as shown.



To assign an existing user profile to a team:

1. Locate the user you want to add to your team.
2. Hover the mouse over the user’s name. The action buttons will be displayed.
3. Select **Edit** to display the **Maintain users** screen.
4. Select **Add access to user** to display the provisioning screen as shown.



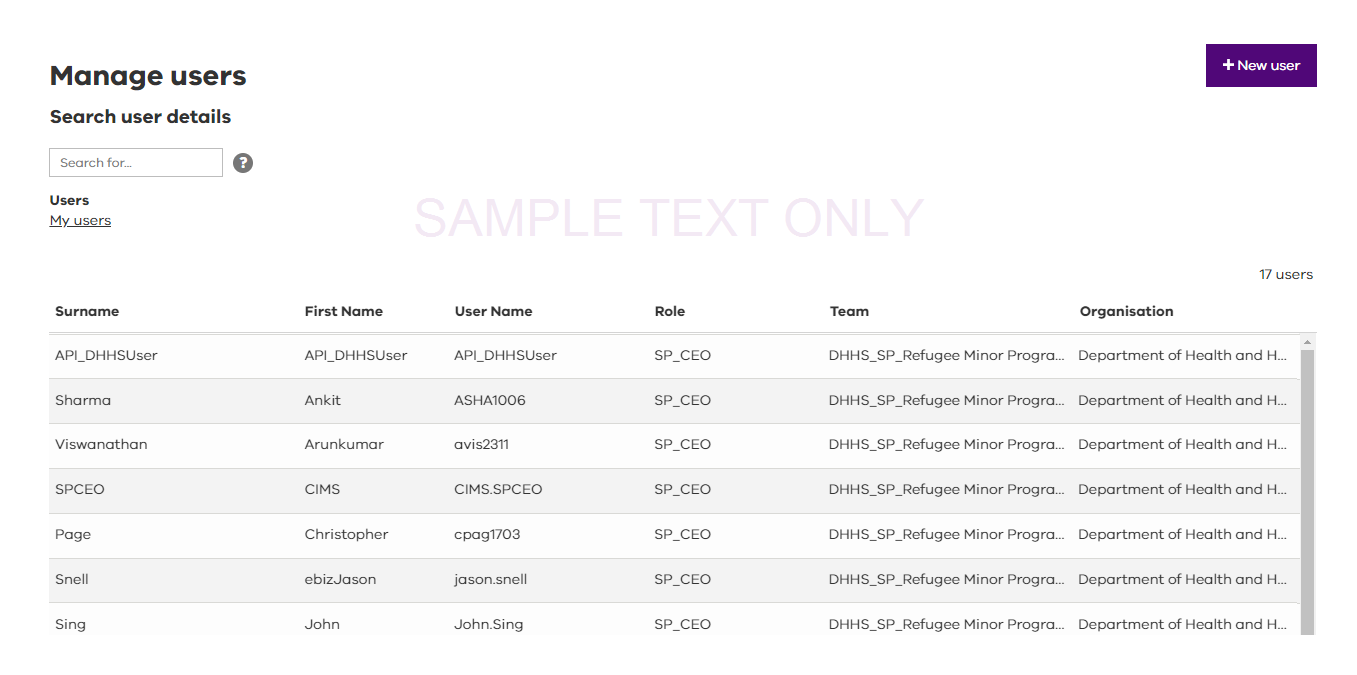
1. Select in the **Organisation** field to choose the required organisation from the activated drop-down list
2. Select in the **Role** field to choose the required role from the activated drop-down list.
3. Select in the **Team name** field to choose the **Team name**.
4. Type the user’s **Email** address.
5. Select **Update access**.

The **Maintain users** screen will display. This screen shows that the user’s record has been updated with the new access along with the pre-existing access.

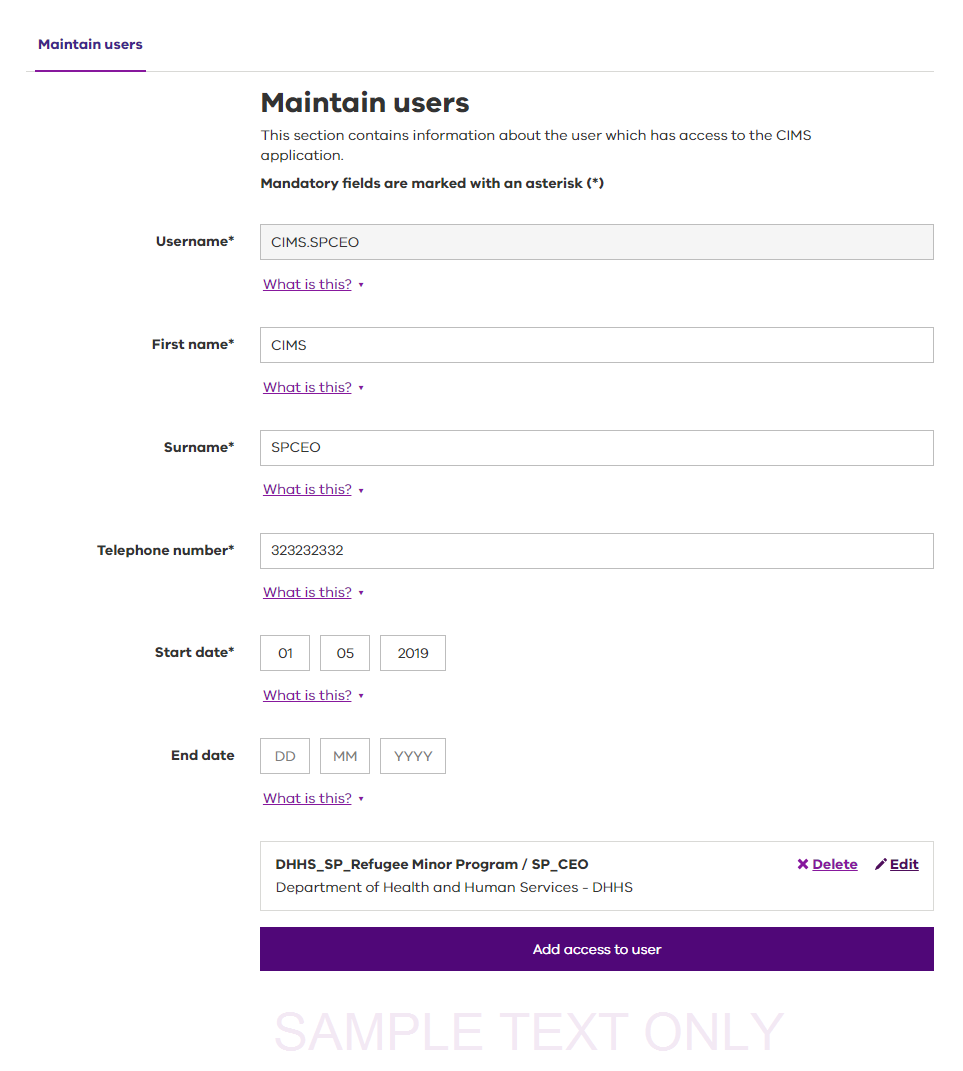
|  |
| --- |
| To remove the previously existing user from your team, follow the steps in [Deleting user access](#_13.5_Deleting_user). You can only delete the provisioning that has been previously allocated by you. This means that if a user originally belonged to another team, only that team’s manager can delete the allocated provisioning. |

## Deleting user access

If a user no longer requires access to CIMS IT, for privacy and security reasons, their user provisioning needs to be deactivated. The Senior Delegate level users can delete the provisioning allocated to the user from the **Manage users** screen by:



1. Firstly, locate the user whose access needs to be deleted.
2. Hover the mouse over the user’s details to display the action buttons.
3. Select **Edit**. The **Maintain users** screen is displayed.



Some users will have more than one form of user provisioning. The Senior Delegate level user can only delete the provisioning that relates to their team. To delete the user’s access to CIMS IT (for example, if the user is leaving the organisation), the Senior Delegate must remove all allocated provisioning.

Continue with the steps below to learn more about deleting user access:

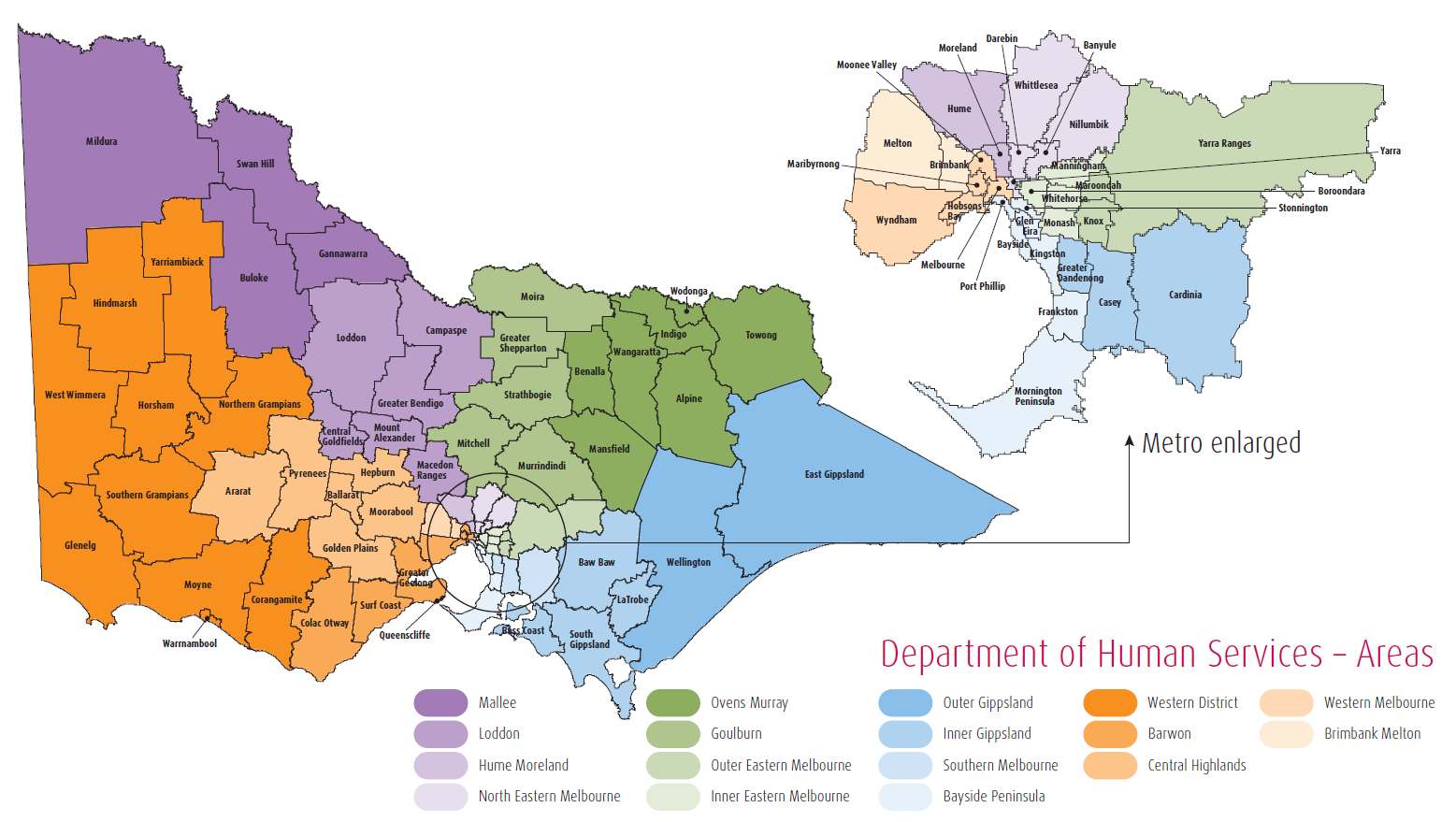
1. Select **Delete** beside the user provisioning to be removed. A **Remove this access** confirmation is displayed.
2. Select **Remove**.

|  |
| --- |
| Be mindful of investigations or reviews assigned to the user whose access is being deleted. It may be necessary to provide alternative access to ensure the timely completion of the reviews. |

Where the user has provisioning to more than one area, only the provisioning deleted will be affected. The user will not be deactivated until all provisioning has been deleted.

# Appendix A: Department service area maps

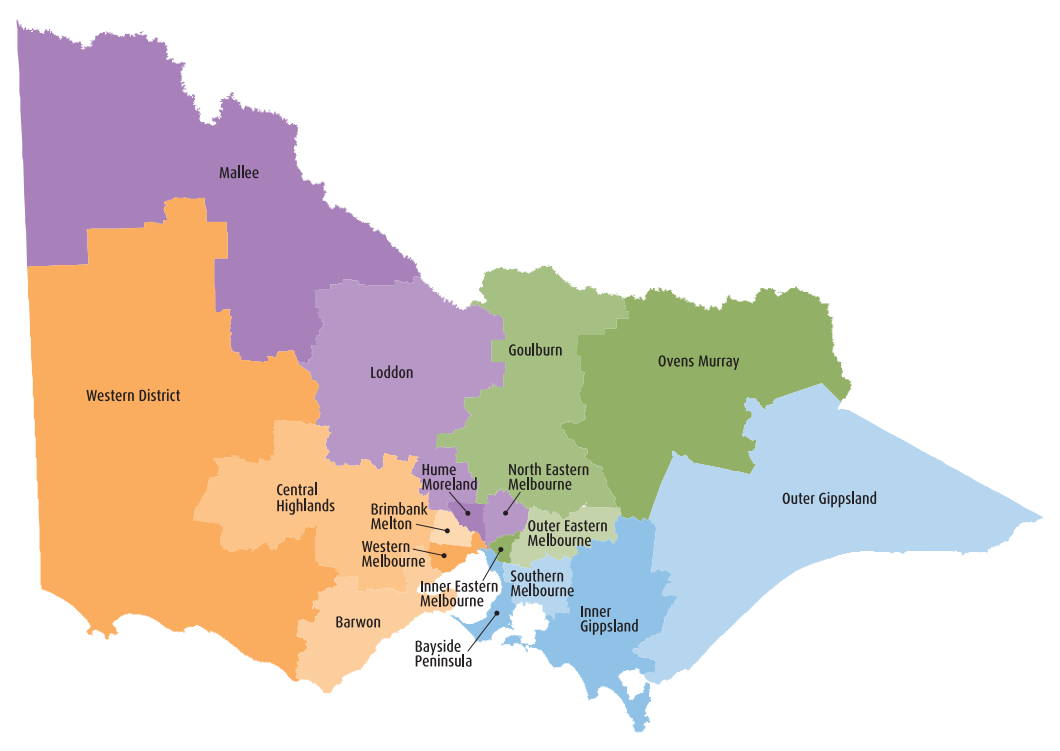
### Figure A.1 Department service area maps - metropolitan



### List of department service areas

* Barwon
* Bayside Peninsula
* Brimbank Melton
* Central Highlands
* Goulburn
* Hume Moreland
* Inner Eastern Melbourne
* Inner Gippsland
* Loddon
* Mallee
* North East Melbourne
* Outer Eastern Melbourne
* Outer Gippsland
* Ovens Murray
* Southern Melbourne
* Wimmera South West
* Western Melbourne

Figure A.2 Department service area maps - regional



# Appendix B: Service provider user roles

## Service provider user roles

The client incident register (CIR) has four different user roles available. Each role has a different level of access and abilities to ensure that each task is completed at an appropriate level of authority. Each of the four user roles is shown below, along with the key tasks for which they are responsible.

|  |  |
| --- | --- |
| Service provider role | Description |
| Manager | The manager role is the first level user within the CIR and has the primary role of quality assurance, overseeing the service provider’s immediate response and escalation of incident reports to the Senior Delegate for final endorsement and subsequent submission to the department. This quality assurance and immediate response responsibility applies to major and non-major impact incidents.  This user can view, edit, withdraw and escalate incident reports to the Senior Delegate. Users with this role will also be able to generate reports on incidents, follow-ups and outcomes that are assigned within their organisation and team.  The Manager role is not able to access the follow-ups or outcomes within the client incident register unless they have been assigned an investigation or review. |
| Senior Delegate | The Senior Delegate role is the highest authority level role within the CIR. The Senior Delegate role has the ability to access all aspects of the system (within their organisation and the team they are assigned) and complete all actions available to the ‘manager’ or ‘investigation manager / review manager’ level users.  Additional functionality only available to the Senior Delegate level user includes:   * authorisation and submission of major and non-major impact incidents to the department on behalf of the service provider * creation and submission of follow-up recommendations to the department in response to a major impact incident (includes assigning an investigation manager / review manager) * endorsement and submission of investigation and root cause analysis review outcomes to the department * the ability to add, edit or remove user provisioning on behalf of the service provider. |

|  |  |
| --- | --- |
| Service provider role | Description |
| Investigation manager / review manager | The investigation manager or review manager role is assigned by the Senior Delegate during the follow-up recommendation process. The role is assigned to the user responsible for completing the investigation, root cause analysis or case review outcome section prior to it being escalated to the Senior Delegate for final endorsement and submission to the department.  The user will only have access to the incident report, follow-up recommendation and outcome section of the incident to which they have been assigned as the investigation manager or review manager.  *Note: When an existing manager-level user is assigned the additional role of investigation manager or review manager, they will maintain all existing access and functionality from the manager role, while gaining access to the investigation/review details for the incident that they have been assigned.* |
| Read-only | The read-only role enables a user to have full visibility of incidents, follow-ups, outcomes and reports within the organisation and team that they are assigned.  A read-only user is able to view, print and access reports on incidents but has no workflow functionality, such as the ability to endorse or submit. |

# Appendix C: Service provider system status

## Status descriptions

Table 1: Service provider incident report status

Status descriptions of incident reports within the **Manage incidents** screen. These status descriptions reflect that of the service providers actions in their management of the incident report.

|  |  |  |
| --- | --- | --- |
| Status name | Incident impact | Description |
| New | Major / non-major | Incident reports have a status of ‘New’ when first submitted via the webform by unregistered or registered users into the service provider’s CIR.  All incident reports at this status require review and approval by a manager user prior to being escalated to the Senior Delegate user for final endorsement and submission to the department.  *Note: A Senior Delegate user has the ability to review and approve the incident report.* |
| Pending Authorisation | Major | Major incident reports have a status of ‘Pending Authorisation’ when a manager user has completed a quality assessment of the service provider’s response section of a major impact incident. This status indicates that the incident report requires a Senior Delegate to authorise and submit the major impact incident to the department (required to occur within 24 hours of the service provider becoming aware of the incident). |
| Approved | Non-major | Incident reports have a status of ‘Approved’ when a manager user has completed a quality assessment and approved a non-major impact incident for submission to the department. A Senior Delegate is responsible for submitting all approved non-major impact incidents to the department within three business days of the incident being disclosed. |
| Submitted | Major / non-major | Incident reports have a status of ‘Submitted’ once they have been submitted to the department. A major impact incident will remain at a status of ‘Submitted’ until a Senior Delegate submits the service provider’s follow-up recommendation to the department (required to be submitted within three business days of the service provider becoming aware of the incident) when it will change to ‘Follow-up’.  Non-major impact incidents remain at a status of ‘Submitted’ as no follow-up recommendation is required. |
| Follow-up | Major | Major impact incident reports have a status of ‘Follow-up’ where a proposed follow-up recommendation for either investigations, root cause analysis reviews or case reviews, have been submitted to the department.  A major impact incident report will remain at the ‘Follow-up’ status until all required outcomes have been submitted and endorsed by the department.  Following endorsement by the department, the major impact incident report can be closed. |
| Withdrawn | Major / non-major | Incident reports have a status of ‘Withdrawn’ when a received incident is removed from the CIR by a manager or Senior Delegate due to it not being in scope for reporting under the CIMS policy. This status can be applied to incidents withdrawn by a service provider prior to submission to the department, or to incidents that are submitted and subsequently withdrawn by the department. |
| Draft | Major / non-major | Incident reports have a status of ‘Draft’ when a new incident is created and saved by a manager or Senior Delegate prior to being completed within the CIR (and not via the webform). Incident reports with a status of ‘Draft’ will only be visible to the user who created the incident report. |
| Closed | Major | Incident reports have a status of ‘Closed’ when all completed follow-up actions have been submitted to the department and endorsed. It applies to major impact incident reports only and is the final status that indicates that the report has been finalised with no further actions to be completed within the CIR relating to the incident. |

Table 2: Service Provider assessment status for follow-up recommendations and outcomes

Status descriptions of incident investigations, root cause analysis reviews and case reviews within the **Manage follow-ups** screen. These status descriptions reflect the service providers actions in their management of the follow-up recommendations and outcomes.

|  |  |  |
| --- | --- | --- |
| Assessment status name | Incident impact | Description |
| Draft | Major | A follow-up recommendation will be at a status of ‘Draft’ when a Senior Delegate creates a follow-up recommendation but does not submit it to the divisional office. This can apply to a follow-up recommendation of investigation, root cause analysis or case review. |
| Open | Major | A follow-up recommendation will be at a status of ‘Open’ when a Senior Delegate has submitted a follow-up recommendation to the divisional office. |
| Pending Authorisation | Major | A follow-up recommendation will be at a status of ‘Pending Authorisation’ when an investigation has escalated an investigation, root cause analysis or case review to the Senior Delegate for endorsement prior to being submitted to the divisional office. |
| Completed | Major | A follow-up recommendation will be at a status of ‘Completed’ when the final investigation or root cause analysis has been submitted to the divisional office.  Note: A case review will change to a status of ‘Completed’ once endorsed by the Senior Delegate as the outcome and outcome report are not submitted to the divisional office. |
| Pending | Major | A follow-up recommendation will be at a status of ‘Pending’ when the Senior Delegate submits an investigation or root cause analysis outcome of ‘On-hold’. This is only to be used when external factors outside the control of the service do not allow for the investigation/root cause analysis to be conducted. |
| Withdrawn | Major | A follow-up recommendation will be at a status of ‘Withdrawn’ when a follow-up recommendation has been withdrawn by the divisional office due to requiring a different form of follow-up and the service provider Senior Delegate has subsequently withdrawn the recommendation. |

# Appendix D: Department divisional office status

## Status descriptions

Table 3: Department divisional office assessment status for incident reports

Status descriptions of incident reports within the **Manage incidents** screen. These status descriptions reflect that of the department divisional office actions in their management of the incident report.

|  |  |  |
| --- | --- | --- |
| Status name | Incident impact | Description |
| Received | Major / non-major | The assessment status of an incident will be ‘Received’ once an incident report has been successfully submitted to the divisional office for endorsement by the Senior Delegate. |
| Assessment in Progress | Major | The assessment status of an incident will be ‘Assessment in Progress’ when the incident has been quality-checked by the divisional office and has been escalated to a department manager for endorsement. |
| Escalated | Major | The assessment status of an incident will be ‘Escalated’ when the incident has been quality-checked by the divisional office and has been escalated to a department director for endorsement. |
| Assessment Complete | Major / non-major | The assessment status of an incident will be ‘Assessment Complete’ when the incident has been quality-checked and endorsed by the divisional office. |
| Follow-up | Major | The assessment status of an incident will be ‘Follow-up’ once the submitted follow-up recommendation has been endorsed by the divisional office. |
| Closed | Major | The assessment status of an incident will be ‘Closed’ when all the follow-up recommendations and outcomes for an incident have been endorsed by the divisional office. |
| Withdrawn | Major / non-major | The assessment status of an incident will be ‘Withdrawn’ when the incident has been returned to the service provider by the divisional office due to requiring amendments (will need to be resubmitted) or if not in scope of the CIMS (will not need to be resubmitted). |

Table 4: Department divisional office assessment status for follow-up recommendations and outcomes

Status descriptions of incident investigations, root cause analysis reviews and case reviews within the **Manage follow-ups** screen. These status descriptions reflect the department divisional office actions in their management of the follow-up recommendations and outcomes.

|  |  |  |
| --- | --- | --- |
| Assessment status name | Incident impact | Description |
| Rec Received | Major | Follow-up assessment status will be ‘Rec Received’ when a follow-up recommendation has been successfully submitted to the divisional office for review and endorsement. |
| Rec Approved | Major | Follow-up assessment status will be ‘Rec Approved’ when the submitted follow-up recommendation has been endorsed by the divisional office. |
| Rec Withdrawn | Major | Follow-up assessment status will be ‘Rec Withdrawn’ when the submitted follow-up recommendation has been returned by the divisional office as it requires amendment (will require resubmission by the Senior Delegate) or a different type of follow-up recommendation is proposed (a new follow-up recommendation will be required). |
| Rec Escalated | Major | Follow-up assessment status will be ‘Rec Escalated’ when the submitted follow-up recommendation has been quality-checked and escalated to a department manager for endorsement. |
| Rec Pending Acceptance | Major | Follow-up assessment status will be ‘Rec Pending Acceptance’ when the submitted follow-up recommendation has been quality-checked and escalated to a department director for endorsement. |
| Outcomes Received | Major | Follow-up assessment status will be ‘Outcomes Received’ when the investigation or root cause analysis outcome has been submitted to the divisional office for quality assessment and endorsement. |
| QA in Progress | Major | Follow-up assessment status will be ‘QA in Progress’ when the submitted investigation or root cause analysis outcome has been escalated to a department manager for endorsement. |
| QA Escalated | Major | Follow-up assessment status will be ‘QA Escalated’ when the submitted investigation or root cause analysis outcome has been escalated to a department director for endorsement. |
| Outcomes Approved | Major | Follow-up assessment status will be ‘Outcomes Approved’ when the submitted investigation or root cause analysis outcome has been endorsed by the divisional office. |
| Outcomes Withdrawn | Major | Follow-up assessment status will be ‘Outcomes Withdrawn’ when the submitted investigation or root cause analysis outcome has been withdrawn by the divisional office.  Outcomes that have been withdrawn will have a reason and rationale as to why they have been withdrawn to enable the service provider to make amendments and resubmit to the divisional office when complete. |
| On-hold | Major | Follow-up assessment status will be ‘On-hold’ when the submitted investigation or root cause analysis outcome is ‘On-hold’ and is endorsed by the divisional office.  Investigations or root cause analysis that are put on hold will also have a revised due date created by the divisional office to enable the service provider to submit an outcome when agreed. |

# Appendix E: Mandatory investigation criteria

Impact = Major

Primary/Secondary incident type = Poor Quality of Care

Primary/Secondary incident type - more information = Staff to Client

Primary/Secondary involvement in the incident = Victim OR

Impact = Major

Primary/Secondary incident type = Sexual Abuse

Primary/Secondary incident type - more information

= Staff to Client, or Client to Client

Primary/Secondary involvement in the incident = Victim OR

Impact = Major

Primary/Secondary incident type = Sexual Exploitation

Primary/Secondary incident type - more information

= Staff to Client, or Client to Client

Primary/Secondary involvement in the incident = Victim OR

Impact = Major

Primary/Secondary incident type = Physical Abuse

Primary/Secondary incident type - more information

= Staff to Client, or Client to Client

Primary/Secondary involvement in the incident = Victim OR

Impact = Major

Primary/Secondary incident type = Emotional/Psychological Abuse

Primary/Secondary incident type - more information

= Staff to Client, or Client to Client

Primary/Secondary involvement in the incident = Victim OR

Impact = Major

Primary/Secondary incident type = Financial Abuse

Primary/Secondary incident type - more information

= Staff to Client, or Client to Client

Primary involvement in the incident = Victim OR

Impact = Major

Primary/Secondary incident type = Injury

Primary/Secondary incident type - more information

= Unexplained injury

Primary/Secondary involvement in the incident = Participant

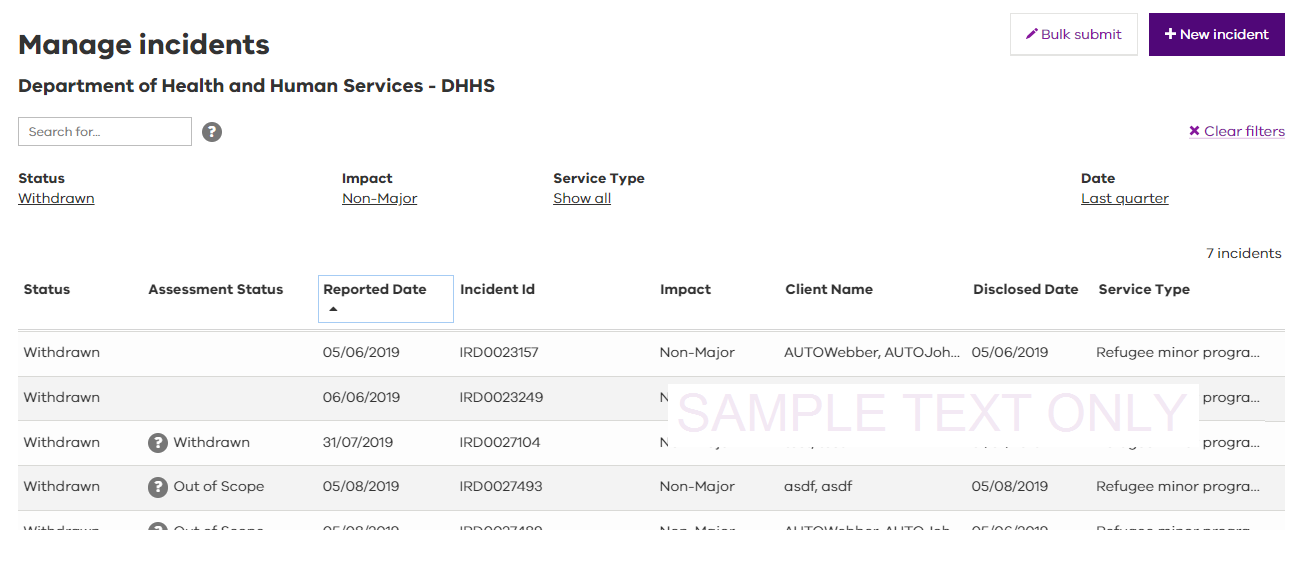
# Appendix F: Non-major - bulk submissions

A bulk submission is the process of collating non-major impact incident reports and submitting them to the department in a single batch.

This process has been replaced by singular submission of non-major impact incident reports, however older incident reports, originally submitted using the bulk process, will continue to use the bulk submission function for any resubmissions following a withdrawal. Resubmission of any older incidents can be done immediately and do not require waiting until the following month.

For new non-major impact incidents, the singular submission process should be followed. See 5 Non-major incident authorisation.

## Processing bulk submissions



1. Within the **manage incidents** screen, select the **bulk submit** button.

The **Manage incidents** screen will refresh to show all non-major impact incident reports that are to be submitted.

Only non-major impact incidents with a status of ‘Approved’ and an earlier disclosure date than the first day of the current month can be bulk submitted.

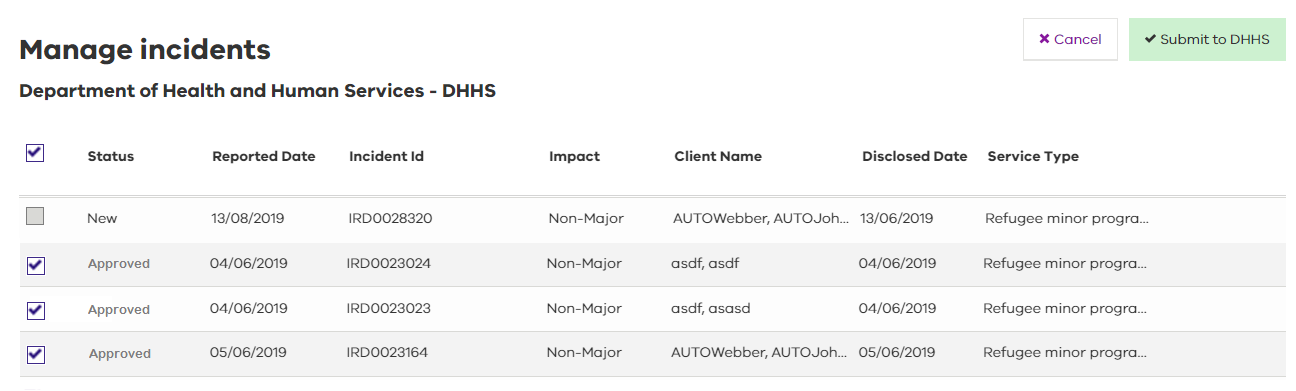
1. Non-major impact incidents with the status of ‘new’ will require quality assessment, approval and final endorsement.

Selecting the edit button on any non-major impact incident with a status of ‘new’ will display the **Service details** screen. The Service details screen enables you to review, authorise and confirm the incident so that it can be included in the bulk submission.

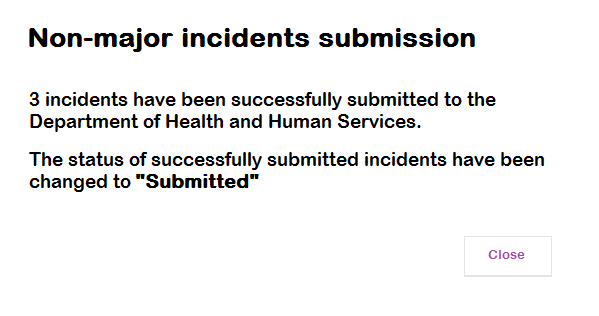
Refer to [Submitting non-major impact incidents](#_7._Non-major_impact_1) for further assistance.

1. Non-major impact incidents with the status of ‘new’ requiring rework can be returned to the reporting officer by Senior Delegate users in selecting the **Return** function.
2. Non-major impact incidents identified as out of scope can be withdrawn by Manager or Senior Delegate users in selecting the **Withdraw** function to remove from the bulk submission.

## Selecting incidents for bulk submission



1. Selecting non-major incidents ready for bulk submission can be completed by selecting the individual checkboxes or the checkbox beside the Status heading. Ticking this box automatically ticks the checkboxes beside all incidents that have been approved and are ready for submission.
2. Ensure all non-major incidents for submission are showing a status of ‘approved’ and have associated checkboxes selected.
3. Submit the bulk submission to the department by selecting Submit to DHHS. A message will display to confirm the successful submissions.



|  |
| --- |
| Non-major impact incidents that are withdrawn by the department divisional office for further information and require resubmission are submitted to the divisional office using the same bulk submit process as detailed above.  Non-major impact incidents that are being resubmitted should be actioned as soon as possible and should not be held by the service provider awaiting submission in the following month. |

1. See Appendix F: Non-major - bulk submissions [↑](#footnote-ref-1)
2. See Appendix E: Mandatory investigation criteria [↑](#footnote-ref-2)