*IBM Cúram Social Program Management*

# Cúram Investigations Guide

*Version 6.0.4*

**Note**

Before using this information and the product it supports, read the information in Notices at the back of this guide.

This edition applies to version 6.0.4 of IBM Cúram Social Program Management and all subsequent releases and modifications unless otherwise indicated in new editions.

# Table of Contents

# Chapter 1

# Introduction

## 1.1 Purpose

The purpose of this guide is to define the functionality provided by the application in support of investigation management. The goal of the investigation process is to collect accurate and comprehensive information to investigate and resolve allegations reported to the organization, for example, allegations of benefit fraud or child abuse.

After reading this guide, the reader should have a basic understanding of how investigations are created to manage and resolve allegations that are reported during screening or case processing.

## 1.2 Audience

This guide is intended for any reader interested in understanding the business concepts of investigation management.

## 1.3 Prerequisites

It is helpful to understand how the application supports case management before reading this guide. See the Cúram Integrated Case Management Guide for information on integrated case management.

## 1.4 Chapters in this Guide

The following list describes the chapters within this guide:

**Overview of the Investigation Process**

This chapter introduces the concept of investigation management and provides an overview of how the investigation process works.

**Tools for Conducting an Investigation**

This chapter provides information on the optional tools available for conducting an investigation.

**Investigation Administration**

This chapter provides an overview of the aspects of investigations set up as part of application administration.

# Chapter 2

# Overview of the Investigation Process

## 2.1 Introduction

An investigation is an inquiry into circumstances surrounding an allegation. Social Enterprise organizations receive thousands of reported allegations each year which must be investigated. Examples include allegations of benefit fraud and child abuse. Allegations of benefit fraud or child abuse may come from a number of sources such as members of the public or family members. For example, John is in receipt of Disability Benefit due to being unable to work because of a back injury. John's neighbour informs the organization that John has been working for 'cash in hand' and is committing benefit fraud.

When allegations are made, the organization must examine the details of each allegation reported to establish if the allegation is true and effectively resolve the matter. Cúram Investigation Management provides a mechanism for the organization to manage and resolve reported allegations. It enables the organization to initiate an investigation into a reported allegation, record details of the allegation, enter findings, and record an overall resolution for the investigation. A resolved investigation may result in other processes being put in place. For example, for substantiated allegations of benefit fraud, the organization may decide to withhold the perpetrator's benefit payments and put in place a process to recoup the money owed. Alternatively, if it is decided that an allegation is unfounded, the investigation may be closed.

This chapter provides an overview of the investigation process. The investigation process begins when an investigation is created. Once the investigation is created, a number of investigation management activities must be completed in order to resolve and close the investigation. These management activities include recording an allegation, completing findings on an allegation, entering an investigation resolution, approving the investigation, and closing the investigation. Additionally, any individuals involved in the investigation can be added during the course of the investigation and a closed investigation can be reopened if required. If reopened, the findings

recorded on the investigation can be overridden.

## 2.2 Creating an Investigation

An investigation can be created at the integrated case level or at the product delivery case level. Alternatively, a standalone investigation can be created. For example, an investigation might be created within a product delivery case if a client is alleged to have committed fraud as part of a particular benefit payment.

Similarly, if a client has several ongoing benefit payment cases and is alleged to have committed fraud on all benefit payments, the organization can create the investigation within an integrated case as the allegation relates to more than one product delivery.

Alternatively, the organization may wish to handle investigations separately from other types of case processing. In this situation, a standalone investigation can be created. The process of creating an investigation is designed to be completely flexible. The decision to create a standalone investigation or an investigation at the product delivery case or integrated case level is made at the discretion of the organization.

Standalone investigations can be created for a registered person, a registered prospect person, or an unregistered individual who is registered on the system as a person participant during the investigation creation process.

When an investigation is created at the integrated case level, the primary client for the investigation can be selected from any of the case members of the case from within which the investigation is created.

If an investigation is created at the product delivery case level, the primary client of the investigation is set to the primary client of the case within which the investigation is created. Once the investigation is created, it is progressed through a series of activities by the appropriate user, such as a case worker.

## 2.3 Assigning Investigation Ownership

The application provides a sample investigation ownership strategy which can be overridden by agencies as required. When a standalone investigation is created, the system automatically sets the administrator of the primary client as the initial case owner of the investigation. When an investigation is created from an integrated case, the case owner of the integrated case is automatically set as the owner. Investigation ownership can be transferred. The owner of an investigation can be a user or an organization group such as an organization unit, position, or work queue. If the investigation owner is set to an organization unit, work queue or position, any users who are members of the organization group can work on the investigation. The agency's own investigation ownership strategy can be configured depending on its requirements. For more information on configuring investigation

ownership consult Section 4.3, *Configuring Investigation Ownership*.

## 2.4 Recording Allegations for an Investigation

When an investigation is created, details of the reported allegation that gave rise to the investigation must be recorded. The investigation then conducted by the organization is intended to substantiate or unsubstantiate these allegations. An investigation may include one or more allegations that are reported by a source, who may be anonymous, who believes that individuals have been involved in a situation that requires investigation such as the fraudulent receipt of benefits and/or services, or the abuse or neglect of a child.

Allegations capture details about what is being investigated, for example, Mary Smith alleges that John Smith sexually abused his daughter Linda Smith and that the alleged abuse took place in the home on 16 June 2006.

Mandatory details, such as the type of allegation and date are recorded. Additionally, the allegation location, a description of the allegation, the allegation participants and their roles, date the allegation was reported, and any additional information is recorded if known.

Allegations cannot be added, deleted, or modified from within an investigation that has been submitted for approval, approved, or closed. When an investigation is submitted for approval, it is under review by a supervisor therefore the allegations should remain static until the supervisor decides whether or not to approve the Investigation. No additional allegations can be added to or modified within approved or closed investigations because these investigations are effectively completed.

## 2.5 Entering Allegation Findings

A finding is a determination by a user as to whether or not an allegation is founded or unfounded. A finding must be recorded on each allegation in the investigation in order for the investigation to be resolved. A user resolves the investigation based on the findings of the allegations.

Examples of allegation findings include 'Substantiated' (founded/true), 'Unsubstantiated' (unfounded/false), and 'Indicated'. A finding of 'Indicated' is used when the organization has sufficient evidence to suggest an allegation is true however the evidence is not strong enough to warrant a substantiated finding. In this situation, the user may prefer to enter a finding of 'Indicated' instead of 'Unsubstantiated'.

A finding cannot be modified on an investigation which is submitted for approval, approved, or closed. When an investigation has been submitted for approval, it is under review by a supervisor and therefore the allegation findings should remain static until the supervisor decides whether or not to approved the investigation. Allegation findings cannot be modified on an approved or closed investigation because these investigations are effectively completed. .

The findings that can be entered on an allegation are set up as code table items as part of system administration. For information on adding code table items to code tables, see the Cúram System Configuration Guide.

## 2.6 Entering the Investigation Resolution

Once the allegation findings have been entered, an overall resolution is recorded. The overall resolution is determined by the user using best judgment based on the allegations and findings that exist on the investigation. For example, a 'Founded' resolution may be indicated for an investigation if at least one of the allegations has received a finding of 'Substantiated' and further action needs to be taken by the organization. This might involve a suspend payment workflow event that will be triggered in the event that an investigation into suspected benefit fraud is founded.

The resolutions that can be entered are inherited from those configured for the investigation type during system administration. Any workflow event associated with the resolution configuration will also be raised when that resolution is entered on an investigation.

## 2.7 Approving the Investigation

Once a user records a resolution for the investigation, the investigation must be approved. The purpose of this stage is to verify that the allegations, findings, and overall resolution entered are correct. The investigation approval stage gives an appropriate user, such as the investigation supervisor, the opportunity to approve or reject the findings documented by the user. This is important because these findings often dictate whether ongoing services should be provided to the client. For example, the investigation supervisor may not agree with a particular finding that the user has given to an allegation or to the overall resolution provided.

When a resolution has been recorded on an investigation, the investigation is submitted for approval and either approved or rejected. If the details recorded for the investigation and the recommended resolution are found to be appropriate, it is manually approved. If additional work is required or the resolution is incorrect, the investigation is rejected and returned to the user for modification. If the user has investigation approval rights as part of his or her security profile, or if the investigation supervisor submits the investigation for approval, the investigation is automatically approved.

Investigations submitted for approval have a status of submitted; approved investigations have a status of approved. If the investigation is rejected, it must be resubmitted in order to progress.

Note that some organizations may not require an investigation to be submitted to an investigation supervisor for approval. Investigations functionality can be configured to support approval check functionality which allows the organization to determine the percentage of investigations to be manually

approved by a supervisor. See section 4.6 for information on setting approval checks.

## 2.8 Closing or Reopening an Investigation

If further involvement by the organization is not needed, an investigation can be closed at any stage. For example, an investigation may be closed if an allegation recorded on it is withdrawn.

An investigation is typically closed when all the investigation allegations are resolved, the investigation findings do not require further action by the organization, and the investigation is approved.

When an investigation is closed, the reason for closing the investigation is specified. After an investigation is closed, the closure details can be changed by a user.

Occasionally, an investigation that is completed and closed may need to be re-opened. For example, a closed investigation may need to be re-opened for a number of reasons, such as:

- The original investigation decision was incorrect.
- New information justifies a different finding on the allegation; and/or
- The investigation was closed in error.

When an investigation is re-opened, a reason for re-opening the investigation is specified.

## 2.9 Overriding a Finding on a Reopened Investigation

If an investigation is re-opened, a finding previously recorded on an allegation can be overridden. For example, if the original finding recorded on the allegation is found to be incorrect, the finding can be overridden and a new finding entered.

In order to complete the override of a finding, the user must specify the reason for changing the finding and the effective date of the new finding.

A finding history is automatically maintained for all allegation findings. The finding history records details of each finding, the effective date and the override reason if applicable.

## 2.10 Summary of Participant Roles Played in an Investigation

Investigation participants are participants who play a role either directly or indirectly in an investigation. Additional participants who were not recorded on the investigation when it was created may be added during the course of

the investigation. These participants can be added manually by a user or automatically by the system when a participant is selected by a user to be a participant in an allegation or to be the source of the allegation.

An allegation participant is a participant who plays a role in an allegation. Examples of roles an allegation participant can play include alleged victim, alleged perpetrator, or impacted party. An allegation participant can be an existing case participant, a registered participant that is identified through a participant search, or an unregistered participant. When a registered or unregistered participant plays a role on an allegation, and is added to the allegation, the system automatically adds the participant to the investigation as a case participant and assigns a role of 'case member' to the participant.

The source of the allegation is also considered an allegation participant. The source can be an existing case participant, a registered participant, or an unregistered participant. When an allegation source who is not a case participant is added to an allegation, the system automatically adds the source to the investigation as a case participant and assigns a role of 'allegation reporter' to the participant.

Multiple allegation participants can be added to an allegation. Each allegation participant added is assigned a role. A participant can play multiple roles in an allegation. For example, a participant who plays the role of alleged victim may also be the source of the allegation.

# Chapter 3

# Tools for Conducting an Investigation

## 3.1 Introduction

The application provides a number of optional tools for conducting an investigation. This chapter provides information on these tools. The organization can use these tools over the course of the investigation to:

- Monitor action plans for the course of action to be taken in the event that an allegation is warranted.
- Use milestones to track significant events that occur during the course of an investigation.
- Maintain a detailed contact log of interviews and meetings with various investigation sources.
- Track the progress of the investigation through its life cycle using the investigation status history.
- Determine the need for a translator to mediate between the primary client of an investigation and a case worker
- Manage legal actions and legal status for investigation participants
- Use standard tools within investigations.

## 3.2 Monitoring the Investigation Action Plan

Action plans are created to identify the actions required to address the needs of the concerned participants during the investigation process. The action plan documents the situations requiring action that concern each participant, any related allegations and the expected and actual dates for addressing the situation. Examples of situations include a concern over the safety of a child due to alleged physical abuse by a family member. The actions required to

address each situation are also documented, including the case participants or user responsible for completing each action. Situations within an action plan may be associated with an action when they are recorded or they may exist independently within an action plan to be associated with actions at a later date. Additionally, actions within an action plan may be associated with one or more situations when they are recorded or they may exist independently to be associated with situations at a later date. Multiple action plans can be created for a given investigation.

Typically an action plan is a voluntary agreement between a participant and the organization. For example, John's mother alleges he was physically abused by his father. A case worker conducts an investigation into the allegation and decides that the allegation is founded. Based on his interaction with John's mother, the case worker determines that it is in John's best interests to remain in his family's home if some of his concerns about John's father are addressed in an appropriate manner. Freddie creates a four-week action plan for John detailing the situation requiring action, the expected date by when the situation should be addressed, and the action required to address the situation. For example, to address the situation of John's safety, John's father will check-in to an in-patient drug addiction program at the county hospital immediately, completing the program successfully before returning home. After talking with Freddie, John's father agrees to check himself into an in-patient drug abuse program at the county hospital as soon as possible. The family also agrees to weekly visits by Freddie to see how John and his family are progressing.

In addition to being available for use in investigations, an SEM agency may also choose to implement action plans for use within any other type of case that would also benefit from having an associated action plan.

## 3.3 Tracking Milestones

In the application, milestone functionality is used to track the completion of significant events or tasks during the life cycle of an investigation. For example, a milestone can be created to track the progress of initial contact with the participant being investigated. Milestones can be assigned a user other than the investigation owner to take ownership of a milestone.

Support is provided to add custom functionality to track whether or not milestones are meeting their scheduled time frames. When created, each milestone has an expected start and an expected end date. Each milestone also has a placeholder for recording the actual start and end dates. The application can be set up to look out for a lapse between the expected start date and actual start date, as well as between the expected end date and actual end date. Additional processing can be triggered to handle these lapses. For example, initial client contact may be scheduled to start on a particular date. Should the initiation of this contact go past its scheduled start date, a workflow can be enacted to handle the delay.

The application supports the ability to manually create milestones. It also

supports the automatic creation of milestones in-line with events that occur within an investigation. For example, milestones can be automatically created by the system on the date an investigation is created in order to track the progress made on the investigation. Both manually and automatically created milestones are based on milestone configurations set up as part of investigation administration (see Section 4.4, *Configuring Investigation Milestones*).

Note

OOTB application provides functionality to set up the automatic creation of milestones. Note, however, some development is required to enact the automatic creation of milestones. For more information, see the Cúram Milestone Developers Guide.

### 3.3.1 Milestone Waiver Request Approval

Given that milestones are used to track important investigation events over time, a milestone waiver request may be required in order for the milestone expected start and end dates to be changed for an automatically created milestone. Expected start and end dates for manually created milestones can be changed without a wavier request. The milestone waiver request approval process is used to confirm that the changes in dates to the milestone are valid. Once a submitted request has been approved, the new expected start and/or end dates will take effect.

Milestone waiver requests can only be submitted, i.e., the expected dates for a milestone can only be changed, if the Expected Date Extension Allowed setting has been configured. The approval process (i.e. the need to submit a waiver request for approval) for these requests will only be necessary if the Waiver Required setting has also been configured. If the Waiver Required setting has not been configured, a user will be able to change the expected start and/or end dates directly. See Section 4.4, *Configuring Investigation Milestones* for a description of these settings.

Milestone waiver request approval check settings for a milestone determine the percentage of submitted waiver requests for a milestone of a particular type that need to be reviewed by an investigation supervisor. For example, an approval check can be set up on a milestone that requires 60% of all submitted requests to be approved; 40% will not require approval. Setting approval checks at the milestone level governs all milestones of a particular type. Milestone waiver request approval checks can also be set up at the organization and user level, with user configuration settings taking precedence over organization unit and milestone settings, and organization unit settings taking precedence over milestone settings. Consequently, the approval check settings for a particular type of milestone are the last step in the system's evaluation of whether or not a waiver request requires approval. In other words, when a waiver request is submitted for approval by a user, the system first checks the user's milestone waiver request approval check settings, then checks the milestone waiver request approval check settings for the organization unit that the user belongs to. After checking these settings,

the system checks the approval settings at the milestone level. The system may determine at any point in this process that the milestone waiver request requires approval.

The approval process is initiated when a user submits a milestone waiver request. If the waiver does not require approval, the waiver is automatically approved and the milestone date changes take effect. If the waiver requires approval, the status is submitted. Note that only one waiver for a milestone can be in a submitted state.

A notification is sent to the appropriate user or group of users to approve or reject the waiver request. Once the user approves the waiver request, the waiver request status changes to approved and the date changes take effect. Alternatively, the user can reject the waiver request and the status is set to rejected.

## 3.4 Using the Contact Log

A contact log maintains details of any follow-up action that is carried out for the investigation. A contact log includes one or more associated contacts, which can be carried out face to face, by E-Mail, phone or hard copy. Maintaining contacts in the contact log involves documenting accurate details of interactions such as those of the following nature:

- Individual contacts with the alleged abuser, alleged victim, or other investigation participant
- Contacts with non-case participants, such as doctors or police personnel etc.

The contact log provides the user with a way to record important dates and details about each contact, such as the participant that the contact concerns, additional attendees, location, purpose, start date and time, type, method and supporting narrative. One or many concerning participants may be specified for a contact and are selected from the existing case participants of the investigation. As part of application administration, an administrator may configure whether or not all case participants are available for selection, or case members only. Multiple attendees may also be associated to the contact and can be selected from existing case participants, registered persons and registered users.

The contact log also provides a mechanism to upload and store multiple attachments, such as scanned documents (letters, photographs, and evidence forms) that were received as part of the investigative process.

The preview function allows the user to view a snapshot of the key data of any contacts relating to that contact log. One or more contacts can also be previewed as part of a specific contact log. In addition, users can also search for a specific contact.

Information recorded in a contact log helps the organization to assess the investigation, and provides the basis for determining appropriate plans or ac-

tions required to successfully conduct the investigation.

## 3.5 Viewing the Investigation Status History

A status history is automatically maintained for all investigations. The status history records details of each status change that the investigation has undergone during its lifetime. The status history is automatically updated when a user submits an investigation for approval, or approves or rejects an investigation.

Every time the system detects an instance of processing for an investigation, it is added to the history. The history displays a record of the investigation, the status, and the effective date of the status change. The effective date allows the user to determine the duration of each status. The status history allows a user to track the progress of an investigation from the time it is created to the time it is closed.

Each investigation has a status which describes its progress during the investigation process. There are five investigation statuses: open, submitted, approved, rejected, and closed. Each status changes during investigation processing.

The following table describes each investigation status:

| Status | Description |
|---|---|
| Open | An investigation status is 'open' when the investigation is first created on the system. An investigation can also have an open status if it has been closed and re-opened. |
| Submitted | An investigation status is 'submitted' when the investigation is submitted for approval. |
| Approved | An investigation status is 'approved' when the investigation has been approved by an authorized user, e.g., an investigation supervisor or has been automatically approved by the system. |
| Rejected | An investigation status is 'rejected' if it does not pass the approval process and has been 'rejected' by an authorized user, e.g. an investigation supervisor. A rejected investigation can be modified and resubmitted for approval. |
| Closed | An investigation status is 'closed' if the investigation is completed and no further action is required. If no further action is required, investigations are manually closed by a user. |

Table 3.1 Investigation Processing Statuses

## 3.6 Determining the Need for a Translator

The organization may occasionally require a translator to mediate between the primary client of the investigation and a case worker. Translation services may be required if users working on an investigation are unable to interact with a client in his or her preferred language. A client's preferred language is recorded when the client is registered with the organization. For example, when James Smith is registered with the organization, his preferred language is recorded as "Spanish" and he cannot speak any other language. In order to interact with the client, the case worker responsible for the investigation must be able to interact with James in Spanish or have a translator who can mediate between them.

Determining the need for a translator is evaluated depending on the translation requirements present on an individual investigation. For example, a client may require translation services on one investigation but not on another. The need for a translator for a client can be recorded manually by a case worker or it can be determined automatically by the system. Whether the translation needs for a client are set manually by a caseworker or automatically by the system is dictated by a configuration setting that is set on the investigation type on which the investigation is based as part of application administration.

The system determines the need for a translator by checking if the case worker's language skills match client's preferred language. If they do not match, the system determined that a translator is required. A user may also manually update the translation requirements for a case even if they are initially determined by the system. If a translator is required for a client, users are kept informed of it when they view the client's case participant details. Additionally, the system displays the preferred language of the client who requires the translation services.

## 3.7 Managing Legal Actions and Legal Status

Case workers may capture the Legal Actions that are taken during the course of an investigation. Legal actions are used to manage directives, actions or other activities concerning investigation participants that are conducted by a legal authority. Examples of directives and actions include hearings, petitions, and orders. For example, a court may order a participant with a history of violence to stay away from the family home. Alternatively, the agency may prepare a petition for a court to detain a participant who has committed an offense. Legal actions can result from another legal action, decision or any other reason that is deemed appropriate by the agency. For example, a legal action such as a temporary custody petition may result in a temporary custody hearing that is scheduled as a result of the petition.

Three main categories of legal actions are supported: Legal Petition, Legal Hearing and Legal Order

A case worker may also document the legal status of an investigation participant. When a court makes a decision about what will happen to a participant, it determines a legal status. Examples of legal statuses include adjudicated, crown ward, parental rights terminated, parental custody, and temporary custody. During the course of a case or legal action, a participant's legal status may change. The changes in a participant's legal status can be accessed and tracked by a case worker. A history of a participant's legal status is maintained to allow the case worker to see how a participant's legal status has changed over time, e.g. a participant's legal status may have initially been determined to be 'temporary custody' but then changed to 'parental rights terminated' when there was no longer the possibility that the participant would return home. Legal statuses are not tied to legal actions but may vary depending on or be impacted by the legal action outcome.

The types of legal actions and legal status that can be created within an Investigation are configured as part of administration.

For more information on legal actions and legal status, see the Curam Appeals Guide.

## 3.8 Additional Tools for Managing an Investigation

The following additional tools are also available for managing investigations. These features are modeled after case management functionality that is available in integrated cases and product delivery cases.

### 3.8.1 The Investigator Homepage

The Investigator homepage provides summary information to help users manage their workload. This includes:

- A view on appointments for today or any other day within the week or the following week.
- Assigned tasks due for that day, as well as any overdue tasks.
- Any cases or investigations marked as items of interest.

In addition, summary information is also provided on the investigations assigned to the user:

- A chart displaying details of all assigned investigations that have a resolution recorded during a specific period. The user can change the view to see this information for different periods e.g. for that day or the previous week.
- Details of investigations either owned or submitted by the user which are still awaiting approval.

### 3.8.2 My Investigations

The my investigations view allows users to access a list of investigations which are currently owned by either themselves, their organization unit, their position or their workqueue. Administrators can configure which of these ownership displays are selectable by the user, when filtering which investigations they wish to see displayed. In addition, users can also filter the investigations list based upon type and status.

### 3.8.3 My Investigation Queries

Investigation queries allow users to monitor any investigations currently or previously assigned to them. The user can choose specific criteria which is important to them, and then save the criteria used in the search as a personal query. This query can be run and re-run without the user having to specify the criteria again. Users can query investigations by client, type, subtype, ownership and status. They can also filter the query results by supplying a time period to run the query against.

### 3.8.4 My Recently Approved Investigations

Users can view a list of investigations they currently own and have been recently approved. In addition, any recently approved investigations which they submitted for approval but no longer have ownershop for are also displayed.

### 3.8.5 My Recently Assigned Investigations

Any investigations which have recently been assigned to the user are available to be viewed. This is based on the ownership filter criteria defined for the users my investigations display.

### 3.8.6 My Recently Viewed Investigations

Details are provided of investigations that the user has recently viewed. This allows the user to quickly return to the investigation without having to search for it.

### 3.8.7 My Items of Interest

Users can add specific investigations as items of interest. They can then easily navigate to the investigation without having to utilize the investigation search functionality. This is especially useful for investigations which need to be monitored closely. Once the user does no longer holds an interest in that particular investigation, it can be removed from the list.

**Important**

Items of interest are not limited to investigations. They can also be added for all case types recorded in the application.

### 3.8.8 Searching for an Investigation

Investigation search functionality is provided for accessing specific investigation information across the whole organization. Users can search for an investigation by reference number, client name, client reference number, type, sub type or status. Users can also filter the search results by running the search against the investigation start or end date.

### 3.8.9 Adding Attachments

An attachment is a supplemental file, e.g., a text document, that is attached to an investigation. The organization can attach scanned documents that provide information in support of an investigation such as a transcript of an interview with an investigation source, or a bank statement. Other examples of investigation attachments include marriage certificates, invoices, and pay slips. A range of file types are supported including Microsoft® Word, Microsoft® Excel and PDF. Once the file is attached to the investigation, it may be accessed by other system users who have appropriate security privileges.

Attachments can also be integrated with a content management system through the configuration of application properties as part of administration. If an organization chooses to integrate attachments with a Content Management System, the file will be stored in and retrieved from the Content Management System.

Important

Attachments are also maintained for product delivery cases, integrated cases and participants.

### 3.8.10 Maintaining Communications

A communication is a correspondence to or from the organization. Any communication created from a communication list page within an investigation automatically relates to that investigation.

Communications can be paper, telephone, or email based. Communication functionality can be integrated with Microsoft Word templates, XSL templates, or email servers.

The correspondent of an investigation communication is automatically assigned the investigation participant role of correspondent.

### 3.8.11 Tracking Investigation Events

Events can be automatically created by the system as a result of case processing or manually created by a user. An example of an event created by the system is the investigation closure event which is created when an investigation case is closed.

The following events can be created by a user manually: investigation case referrals, investigation case reviews, and investigation case activities.

An events calendar is provided for all events. Each calendar displays the name of the event and the date on which the event occurs in the appropriate date entry.

### 3.8.12 Entering Notes

Notes are used to provide additional information about an investigation. For example, a note may be added to the investigation stating that a key participant in the investigation did not attend a scheduled meeting. A note can be entered as free text and can be prioritized and given a sensitivity rating so that the note can only be accessed by certain users. Additionally, the system can generate notes which describe case processing. For example, when an investigation is closed, the system will create a note to mark the change in the investigation status.

A note cannot be overwritten once it has been created on the system. When a note is modified, the system maintains a note history which includes each version of a note, the time and date the note was entered on the system and the user who made the note modifications. The note history also includes the reason for the note.

The system will automatically generate notes during the lifecycle of an investigation. For example, a note is automatically generated and displayed on the investigation notes list every time an investigation is closed or reopened.

### 3.8.13 Using Tasks to Manage Work on Investigations

A task is an instruction to carry out an item of work. Tasks are either manually created by a user or automatically created by the system. They are maintained in a user's workspace as part of workflow. Tasks that relate to an investigation can also be maintained from the investigation case's task list. For example, a task may be created to approve an investigation that has been submitted for approval. This task would appear on both the user's inbox and on the investigation's list of tasks.

### 3.8.14 Recording Case Relationships

A case relationship is a link between one case and another case. Case relationships are either created manually or automatically during investigation processing. A relationship can be manually created between two cases for a number of reasons. For example, if a client is being investigated for potential fraud in one product delivery case, but is also involved in another product delivery case, a relationship can be created between the investigation and the product delivery case.

### 3.8.15 User Roles

Standard user role functionality is used by investigations to record the investigation owner and supervisor. Ownership can be assigned to any organization object, i.e., a user, organization unit, position, or work queue. This enables any user or users within an organization unit, position or work queue to perform tasks on an investigation,

# Chapter 4

# Investigation Administration

## 4.1 Introduction

Investigations can be created on cases when investigation information has been configured as part of system administration. When an investigation is created, it inherits this pre-configured information. This chapter provides an overview of investigation information that must be configured in order to create investigations. The following information is covered in this chapter:

- Defining investigation types
- Configuring investigation milestones
- Defining investigation resolutions
- Setting up assessments for investigation types
- Setting up investigation approval checks

## 4.2 Defining Investigation Types

System administration allows the configuration of the types of investigations that can be created, for example, Benefit Fraud, Child Protection Services and Youth Justice. An Investigation type includes the following configurable information: the Home Page for the investigation, Start Date, Create Workflow Event, Close Workflow Event, and Security Rights. Additionally, investigation type configuration includes the ability to configure translation requirements and an investigation ownership strategy and whether or not only case members should be available for selection as the concerning participant of a contact created within the contact log of an Investigation.

## 4.3 Configuring Investigation Ownership

An Investigation Ownership Strategy setting is provided that allows an administrator to define an ownership strategy for investigations based on a particular type using workflow. Investigation ownership is functionally similar to case ownership. If an ownership strategy is specified for an investigation, this setting is used to define how the initial case owner for the investigation should be determined. An organization can override the default investigation ownership strategy depending upon its requirements to assign ownership to any user, organization unit, position, or work queue.

## 4.4 Configuring Investigation Milestones

All investigation milestones are based on an associated milestone configuration. The following table describes the available milestone configuration settings (both optional and mandatory):

| Configuration Settings | How Used | Optional or Mandatory |
|---|---|---|
| Name and Type | The name and type are used to distinguish the milestone configuration. When creating a manual milestone, a user must select the milestone configuration to be applied using the milestone configuration name. | Mandatory |
| Earliest Start Day (days) | This setting is used to determine the expected start date for automatically created milestones. The expected start date is set to the current date on which the milestone is created plus the number of days defined here. For example, if the milestone is created on April 1 and this setting is 3, then the expected start date of the milestone is set to April 4. This setting is used to validate the Expected Start Date entered by a user when manually creating a milestone. A milestone cannot have an Expected Start Date earlier than this number of days after the start date of the Investigation. | Mandatory |
| Duration (days) | This setting is used to determine the expected end date for all milestones. For manually created milestones, the expected end date is set to the user-entered expected start date plus this duration minus one. For example if the expected start date is April 1 and | Mandatory |

| Configuration Settings | How Used | Optional or Mandatory |
|---|---|---|
| | the duration is 7 days, the expected end date is set to April 6. For automatically created milestones, the same calculation is applied to the expected start date defined by the date on which the milestone was created and the Earliest Start Day (days). | |
| Start Date | The start date determines the active, and thus availability, period of the milestone configuration. | Mandatory |
| End Date | The end date determines when the milestone configuration is no longer active. This date is not mandatory as milestone configurations can remain active for an indefinite time period. | Optional |
| Expected Date Extension Allowed | This indicates whether or not the expected start and end dates for an automatically created milestone can be redefined. If this indicator is not set, then the expected start and expected end date calculated upon creation of a milestone are unchangeable. | Optional |
| Waiver Required | This indicates whether or not a waiver is required in order to change the expected start and expected end date for an automatically created milestone. This can only be set for milestone configurations which allow the expected dates to be extended (as described in the setting above). Milestone waivers are described in Section 3.3.1, *Milestone Waiver Request Approval*. | Optional |
| Milestone Added | Any existing workflow event can be associated with the creation of a milestone. This event can be used to extend the OOTB milestone creation processing. For example, when a milestone is added, a workflow can be enacted to notify the investigation owner. | Optional |
| Milestone Complete | Any existing workflow event can be associated with the completion of a | Optional |

| Configuration Settings | How Used | Optional or Mandatory |
|---|---|---|
| | milestone. This event can be used to extend the OOTB milestone completion processing. For example, when a milestone is completed, a workflow can be enacted to notify the investigation owner. | |
| Expected Start Date Not Achieved | Any existing workflow event can be associated with the expected start date in order to track the timeliness of the milestone. For example, if no actual start date is entered for the milestone and the expected start date passes, a workflow can be enacted to notify the investigation owner that the milestone has not yet started. | Optional |
| Expected End Date Not Achieved | Any existing workflow event can be associated with the expected end date in order to track the timeliness of the milestone. For example, if no actual end date is entered for the milestone and the expected end date passes, a workflow can be enacted to notify the investigation owner that the milestone has not been completed in a timely fashion. | Optional |

Table 4.1 Milestone Configuration Settings

## 4.5 Associating Milestones with Investigations

To support manual and automatic creation of milestones within an investigation, it is necessary to set up an association between a milestone configuration and the investigation type. There are two options for setting up these associations: either a new milestone configuration can be recorded at the same time it is associated with the investigation or an existing milestone configuration can be selected.

When recording a new milestone configuration as part of the association process, the milestone configuration information (as described in Section 4.4, *Configuring Investigation Milestones*) must be defined. Additional association information can also be defined if the milestone is to be created automatically. The two main configuration settings for automatically created milestones are the creation event and the completion event. These events are used by the application to automatically create and complete an instance of the milestone.

For example, a milestone can be set up to track the life cycle of an investigation from approval through closure. To set up the automatic creation of this milestone, the Approve Investigation event can be selected as the creation event and the Close Investigation event can be selected as the completion event. When an investigation is approved in the application, the Approve Investigation event will trigger an instance of the milestone. Later when the investigation is closed, the Close Investigation event will close the milestone instance.

The matching process for creating milestones within an investigation can be further specified using the component type and component category settings. A clear distinction can be made between creation and completion events at the investigation level and at the investigation component level. For example, the investigation component, Action Plan, can be set, with a creation event of Create Action Plan and a completion event of Close Action Plan.

When an action plan is created within an investigation, the Create Action Plan event will trigger an instance of the milestone and the application will associate both the Action Plan ID and the Investigation ID with it. Later when the action plan is closed, the Close Action Plan event will use both of these IDs to find and close the correct milestone instance.

## 4.6 Defining Investigation Resolutions

Resolutions for investigation types are configured during system administration. Resolutions are used to record the outcome of an investigation. Examples of resolutions include "founded", "unfounded". Any number of resolutions can be configured for an investigation type. Once configured, these resolutions can be recorded on investigations by a user in order to complete the investigation.

Each resolution is configured as a selectable code table value and may also have an associated workflow event which is raised when the resolution is entered on an investigation. Resolution events are used to trigger a specific case processing function. For example, a particular event may be triggered when a resolution of "founded" is entered on an investigation.

## 4.7 Setting up Assessments for Investigation Types

The application provides support for the ability to run assessments within an investigation. Predefined assessments can be assigned to investigation types during system administration. Although currently there are no OOTB assessments that can be run within an investigation, an organization can use the infrastructure provided to allow an assessment to be selected and executed by the organization during the investigative process to help determine the appropriate resolution for a particular type of investigation.

## 4.8 Setting up Investigation Approval Checks

Investigation approval checks can be defined for each investigation type suring system administration. As part of the investigation process, an investigation is typically submitted to a supervisor for approval of the overall resolution recorded on the investigation by the user. The percentage of investigations that require supervisor approval can be set by the administrator. For example, an approval check percentage set to 50 signifies that 5 out of 10 investigations will be sent to the investigation supervisor for manual approval.

Setting up investigation approval checks gives the supervisor an opportunity to check that the allegations, findings, and overall resolution recorded on an investigation is correct. This safeguards against incorrect information being added to the investigation or an erroneous resolution being documented. For example, the organization may require a supervisor to manually approve a set percentage of investigations submitted by a less senior user. If the supervisor does not agree with a particular finding that the user has given to an allegation or with the overall resolution provided, the supervisor can reject the investigation.

An approval check set for an investigation type will govern all investigations based on that particular investigation type. Note that there can be only one active approval check for investigations based on a specific investigation type at a given point in time.

# Chapter 5

# Conclusion

## 5.1 Summary of Features

The following is a summary of the main concepts covered in this guide:

- Investigations are created to record, manage, and resolve reported allegations of benefit fraud or child abuse.
- Investigations can be created from product delivery cases and integrated cases. Alternatively, separate standalone investigations can be created.
- The investigation process includes creating an investigation, adding an allegation to the investigation, recording a finding on an allegation, and entering an overall resolution on the investigation.
- A number of tools are provided for conducting an investigation. These tools can be optionally used during the course of an investigation and include milestone and action plan functionality and a contact log for recording interactions between the organization and key participants.
- Investigation types, resolutions, and milestones are set up as part of system administration.

## 5.2 Additional Information

Additional information on the topics covered in this guide are covered in several related documents:

**Cúram Participant Guide**

This guide covers the basic concepts of participant functionality.

**Cúram Integrated Case Management Guide**

This guide covers the basic concepts of case processing.

**Cúram Workflow Overview**

This guide provides an overview of Cúram workflow.

**Cúram Communications Guide**

This guide provides an overview of communications functionality.

# Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law.

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typograph-

ical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources.

IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products

should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

## Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trade-