Incidents Management & Whistleblowing

Solution Description

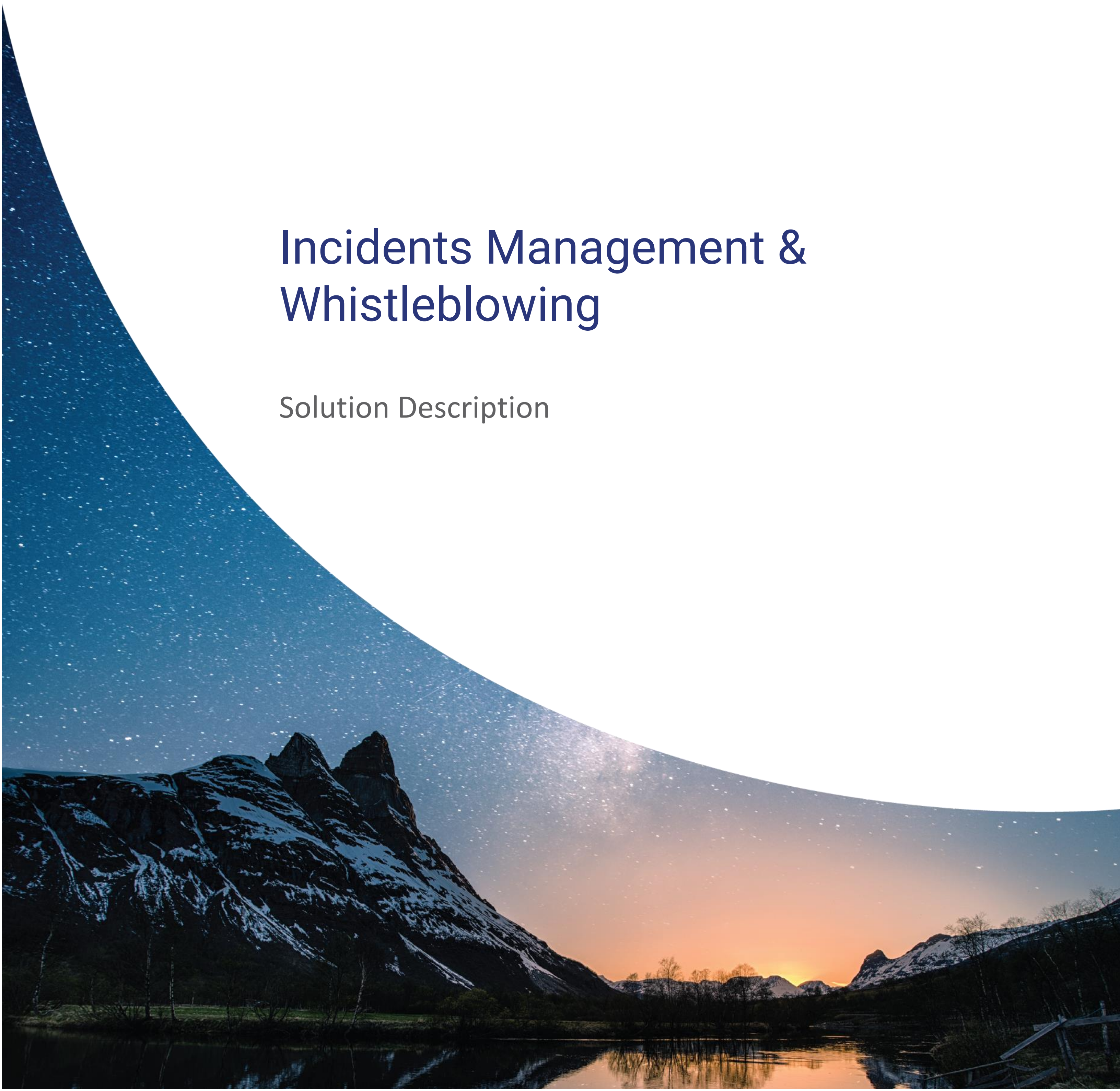


Table of Contents

Table of Contents 2
1. Confidentiality Statement 3
2. Overview 4
3. Benefits 5
4. Key Features 6
5. Fields and Functionality 7
6. Incident Treatment Process 10
7. Monitoring 12
8. Solution Scope 13
9. Configuration Options 14

1. Confidentiality Statement

2. Overview

Incidents Management

An incident is an occurrence that may have a negative impact on your organization. The Incidents module enables you to customize and organize information related to a tip or fraud incident, conduct investigations, collect evidence, and store and organize this data for potential legal action. With each incident, you can create and maintain status updates, investigations, and actions that pertain to the incident. You can also link related incidents and evidence documents as well as workflow teams and security permissions.

By using the Incidents module, you can:

- Record data related to a tip or fraud incident, collect evidence, and store and organize this data for potential legal action.

- Conduct investigations on one or more issues identified in an incident and include interview notes, findings by investigators, and recommendations on how to proceed.

- Link incidents to other items, such as divisions, policies or risks , to further organize the evidence of compliance.

- Create an incident template to establish the components of a specific type of incident, then use it each time you create a similar incident.

- Relate an incident with other incidents, create workflow templates, establish teams, record actions and maintain status updates of your investigation, and organize evidence.

Incidents, investigations, status updates, and evidence documents move through predefined workflows, guided by workflow templates defined by your organization. Depending on the setup of your workflow templates, steps for investigation, evidence collection, remediation planning, closeout, and retraining processes may be included.

Whistleblowing

The SAI360 Whistleblowing software uses webline integration to report incidents. The website on which the incidents are reported (input software – Webline) is logically separated from the processing software (SAI360 Whistleblowing). The incidents are entered via a web form (in the case of reporting via hotline, the entry is made by the hotline staff).

3. Benefits

Our incidents management software automates the reporting and investigations of potential non-compliance issues, helping organizations quickly detect and respond to problems.

- Reduce time to identify root causes and resolve issues.
- Achieve end-to-end case management.
- Efficient, timely management of incident investigations.
- Maintain a continuous audit-ready state
- Achieve rapid results via a secure internet service.

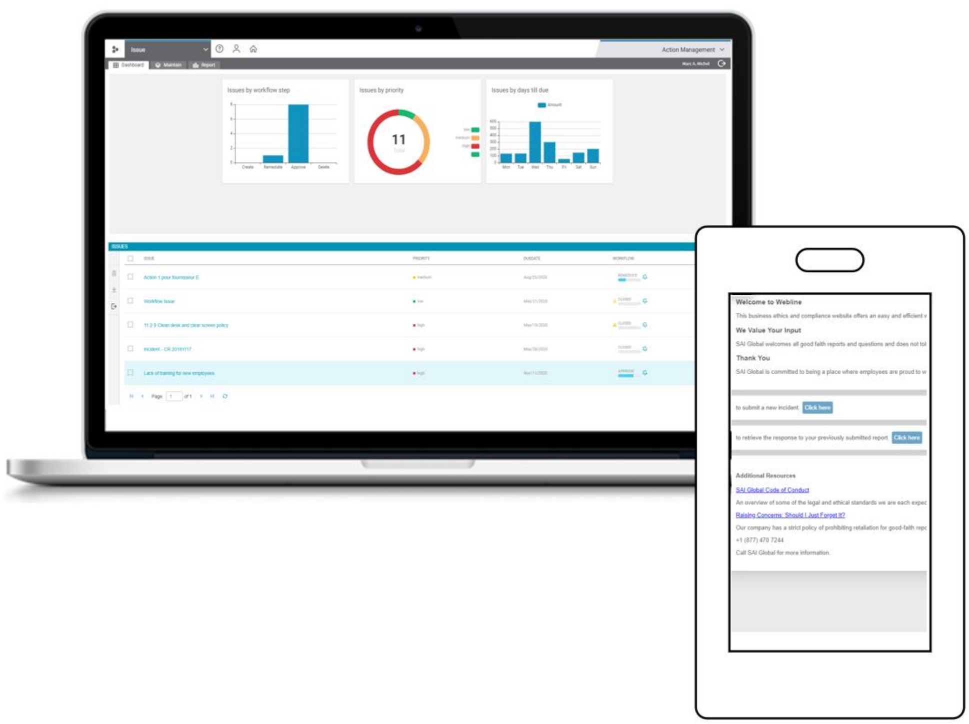


Figure 1 - Overview

4. Key Features

Figure 2 – Incidents Management and Whistleblowing Key Features

INCIDENTS MANAGEMENT & WHISTLEBLOWING MODULES FUNCTIONALITY

- Custom multi-lingual web portal intake through your corporate intranet, internet or browser-enabled mobile devices
- For phone-based reporting, secure and anonymous hotline service delivered by trusted hotline partner
- Intuitive online forms with your unique input fields for each incident type
- Flexible workflows for content, assessments, and tasks automates the process of complying with new and changing regulations.
- Supports any corporate structure (centralized, distributed autonomous or hybrid approach).
- Real-time dashboard metrics plus advanced reporting functionality enable quick and easy data views and analysis.

5. Fields and Functionality

SAI360 is a configurable platform. While this document outlines the “out of the box” configuration, fields and forms can be edited using the administrative capabilities of the tool which training can be scoped in additional to the best practice solution. To aid review of this document, below is a list of the default fields:

INCIDENTS MANAGEMENT

The Message form shows the details that are documented (Section General)

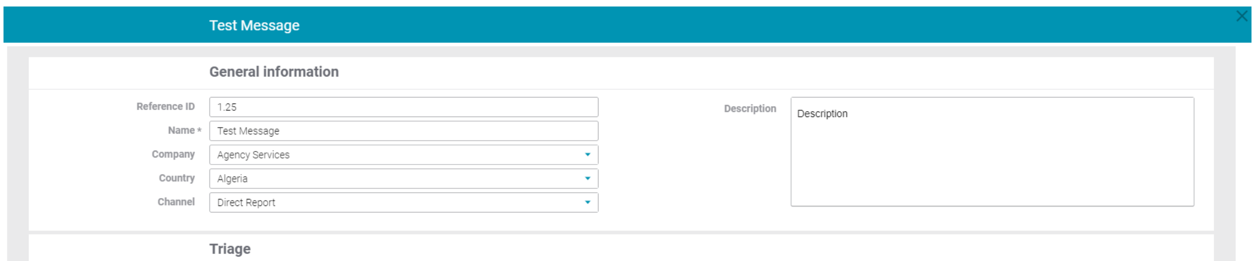


Figure 3 – Message Form

The Triage shows the result of the assessment of the case by categories like Financial, Legal and Reputational in order to decide if further Investigation of the case is required.

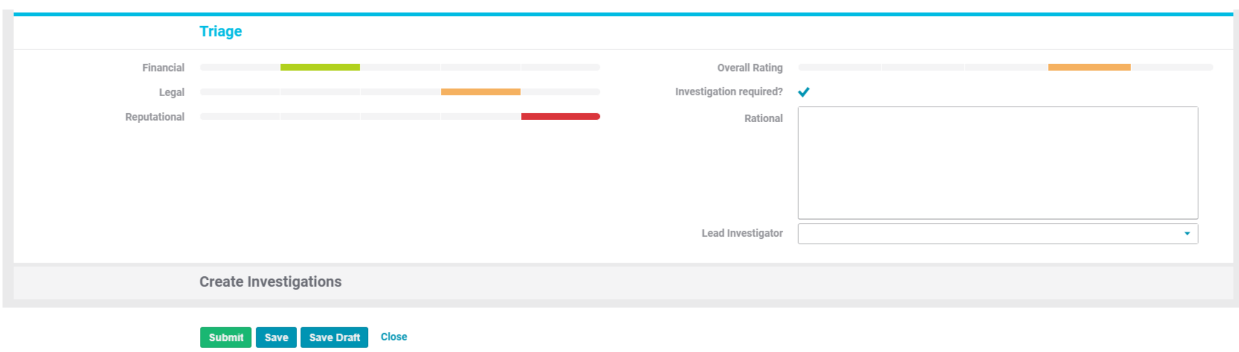
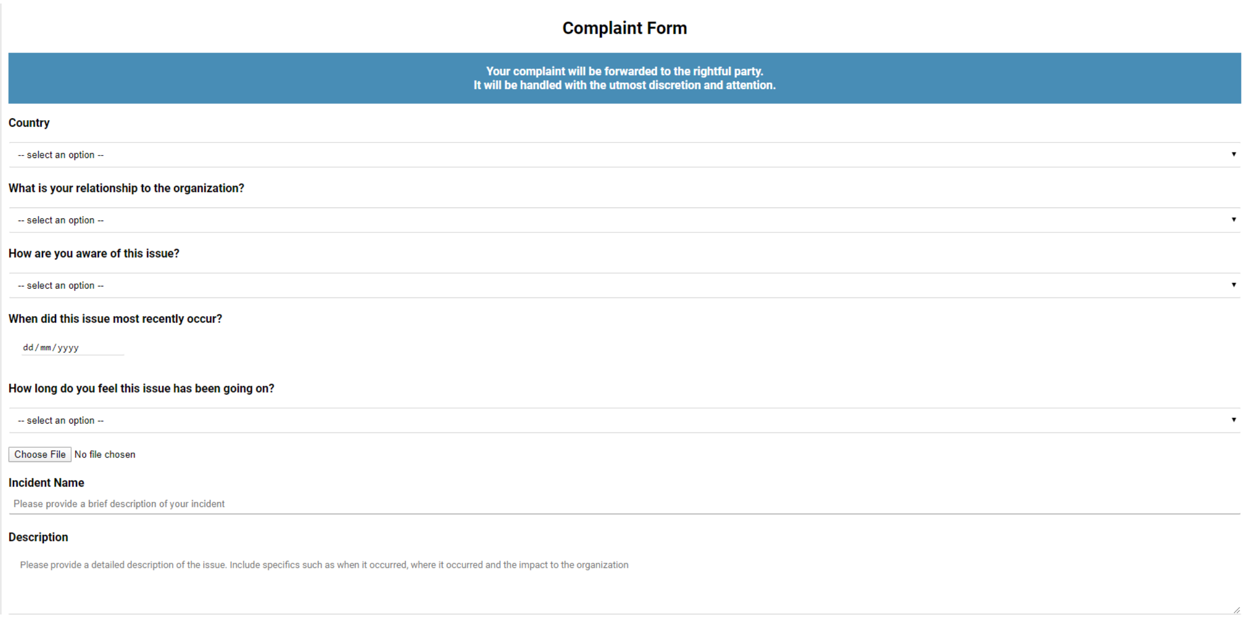


Figure 4 – Example Triage

WHISTLEBLOWING

Whistleblowing messages can be used as a starting point for an investigation. After receiving an allegation and performing a triage, an investigation can be created and linked to the whistleblowing case.


Complaint Form

Your complaint will be forwarded to the rightful party.
It will be handled with the utmost discretion and attention.

Country

-- select an option --

What is your relationship to the organization?

-- select an option --

How are you aware of this issue?

-- select an option --

When did this issue most recently occur?

dd/mm/yyyy

How long do you feel this issue has been going on?

-- select an option --

Choose File No file chosen

Incident Name

Please provide a brief description of your incident

Description

Please provide a detailed description of the issue. Include specifics such as when it occurred, where it occurred and the impact to the organization

Figure 5 – Whistleblowing Portal

<u>Anonymization</u>

Data of the whistleblower will not be requested or stored in no input field.
The whistleblower has the possibility to follow up the further processing of his incident. For this purpose, the system assigns an anonymous access ID. Please note that due to the preservation of anonymity, this data cannot be assigned to a person. This also means that if an access ID is forgotten, it cannot be restored.

<u>Processing</u>

After the disclosure has been made, the webline software transfers the data (and only the data) from the input form to SAI360 for further processing. This means that the anonymized access ID is transferred.

IP Addresses

IP addresses of the whistleblower are neither stored nor are IP addresses transmitted from the input software (Webline) to the processing software (SAI360). Therefore tracking via IP address is not possible.

INVESTIGATION

This overview shows all sections which are used on investigation form for performing an investigation

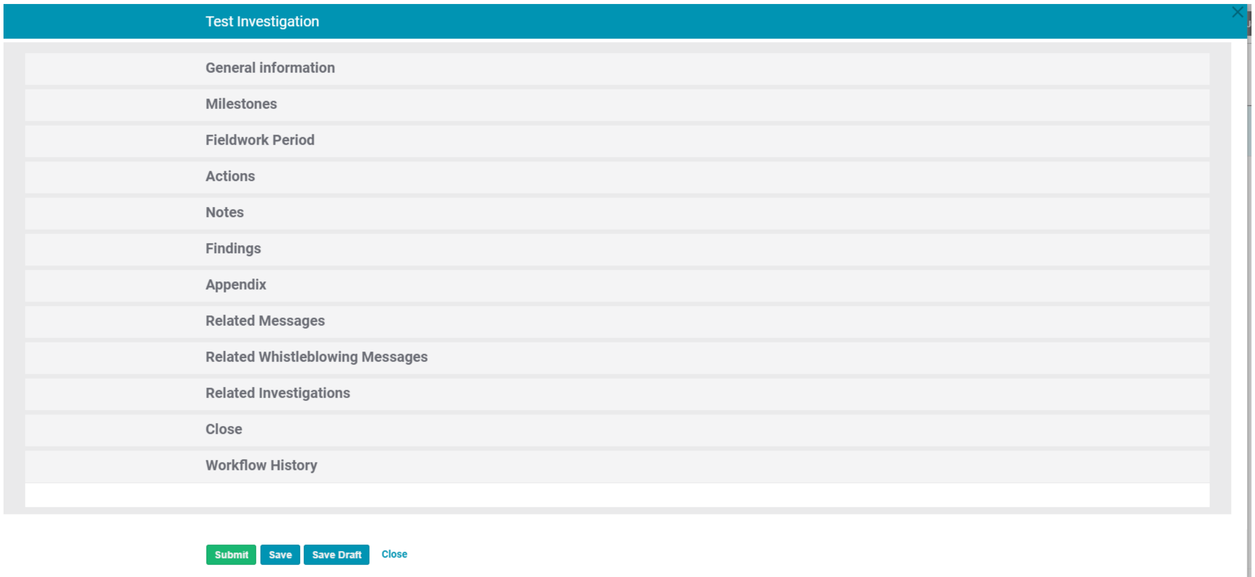


Figure 6 – Incident Form

The section general information shows all relevant related to the investigation.

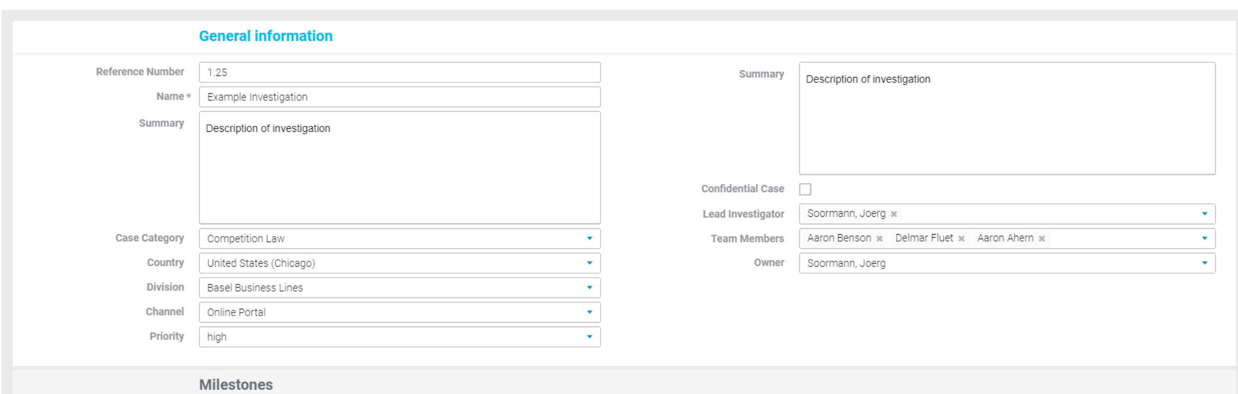


Figure 7 – Incident Form – General Section

6. Incident Treatment Process

INCIDENT LIFECYCLE

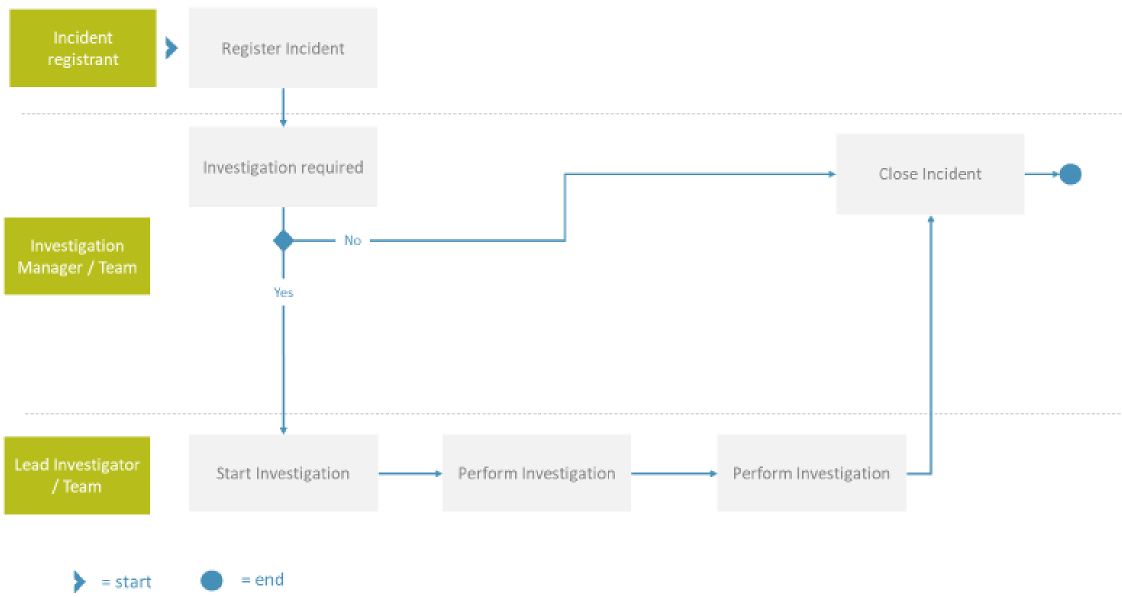


Figure 8 – Incident Flow

PERFORM ACTION PLAN LIFECYCLE

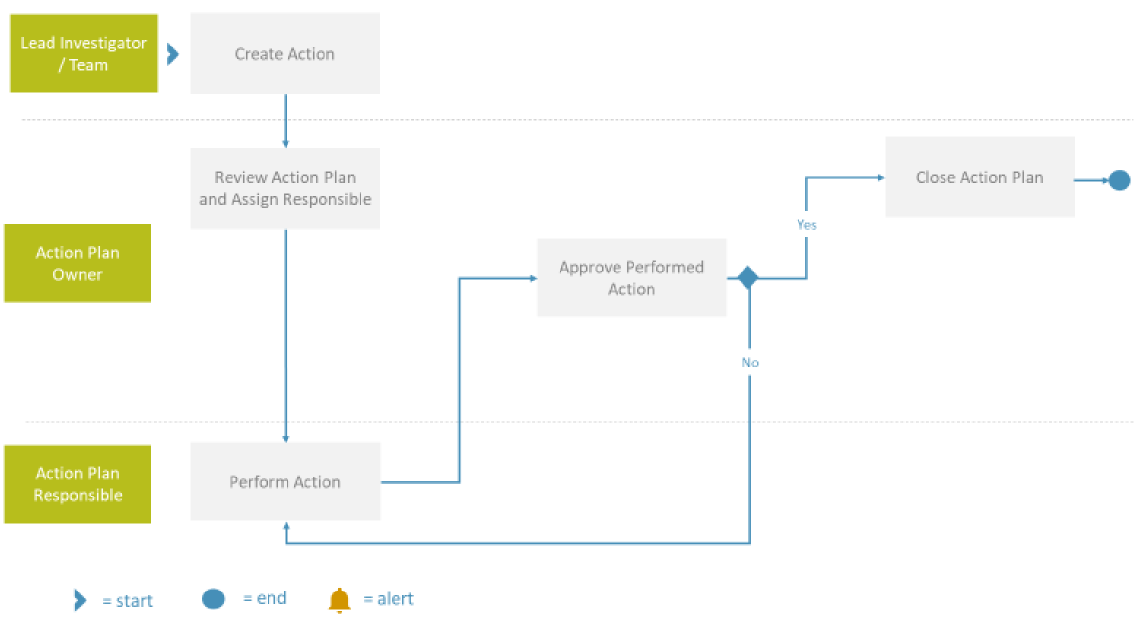


Figure 9 – Action Plan Flow

Each Action Plan will be managed through a workflow with the following steps:

1) Creation
An authorized person creates a new action plan, either within an existing incident/disclosure or ad-hoc within the solution. A specific person is assigned as action responsible to perform follow-up or remediation.

2) Perform Action
The action responsible acts upon the information provided in the action plan in an effort to move it towards resolution.

3) Approve
The treatment plan owner reviews the remediation performed and validates that it has resolved the issue. They may also choose to reopen the treatment plan if they believe the work is not complete or satisfactory.

4) Close / Archive
The solution administrator maintains control over the completed treatment plan until it is necessary to archive and purge it from the solution.

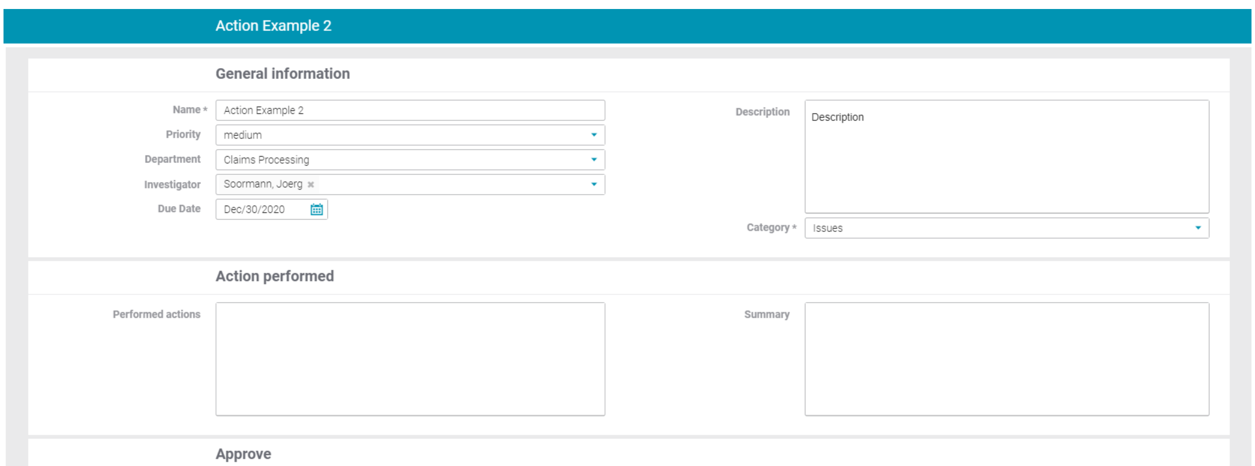


Figure 10 – Example Action

7. Monitoring

The investigation dashboard provides a visual overview of the current investigation management situation for global users.

- Investigations by workflow steps: shows an overview the number of outstanding investigations that are present in each issue workflow step
- Investigations by priority: shows an overview of the number of outstanding issues grouped by priority (high, medium, low)
- Investigations by start date: shows an overview of start date of all investigations, not closed.
- Grid table: Provides an overview of the current investigations with additional information like Country, Division, Status

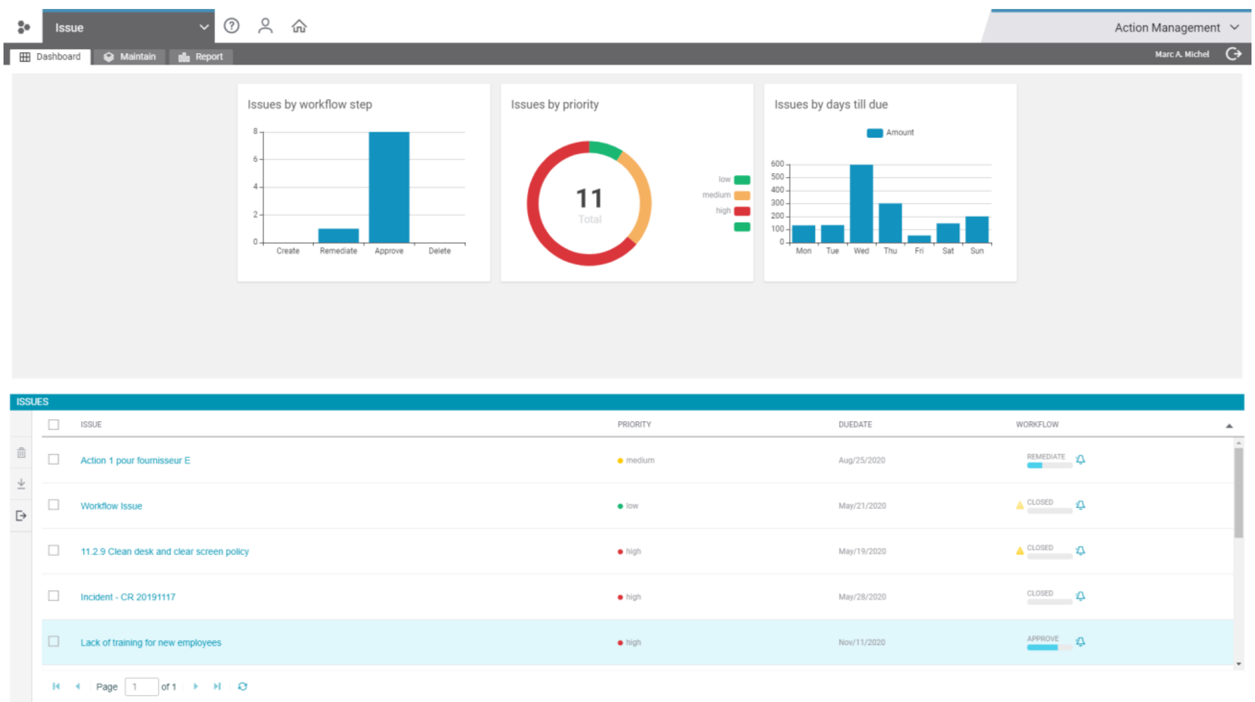


Figure 11 – Incidents Dashboard

8. Solution Scope

The SAI360 platform is fully configurable and can be tailored to the requirements of the customer. However, the scope is pre-defined and limited to core functionality. This section outlines to scope of the pre-defined solution:

FORMS AND FIELDS

The default forms will be used. However, local administrators will be trained on how to edit the component fields lookup values if required.

ORGANIZATIONAL STRUCTURE

The organization and legal entity structure are used for aggregation and consolidation of information and results, made available via dashboards and reporting.

PROFILES & AUTHORIZATIONS

The SAI360 Regulatory Change Management comes with predefined roles and authorization profiles that include

- Investigator
- Action Owner
- Solution Administrator

to facilitate your start with the SAI360 platform. However, local administrators can be trained on how to edit the roles and authorization profiles if required.

REPORTING

One elementary Report based on customer requirements.

9. Configuration Options[1]

EMAIL DISTRIBUTION

Email addresses are a property of the users account within the application. These can be managed via synchronizing with the organization's Active Directory. This requires an API integration which can be scoped as an additional configuration item.

REPORT DESIGN

A reporting universe will be set up including a default extraction report with all relevant system data. This can be used by the customer to build their own custom reports. Having additional reports designed by SAI Global can be scoped as an additional configuration item.

OTHER CONFIGURATION

Within the module there are some aspects that the Customer may determine are not relevant to their implementation. These items may then be excluded from the scope of the implementation.

[1] Add-ons must be purchased separately.