217, Sheikh Rashid Building
P.O Box 56272, Dubai
United Arab Emirates

Tel: +971 4 2973236
Email: uae@verbat.com

BUSINESS REQUIREMENTS DOCUMENT

Incident Communication Mobile App

Prepared for:
Miral

Submission Date:
14 June 2018

Proposal ID:
AD/BRD/17052018/1921/2

Confidentiality Notice: This Proposal is confidential and contains proprietary information and intellectual property of Verbanet Technologies LLC. Neither this proposal nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of Verbanet.

Review & Approval

Document Name	Business Requirements Document	Date	14 June 2018
Prepared by	Asha George	Version	2.0
Reviewed by	Luay Houri	Version	2.0

ROLE	NAME	SIGNATURE	DATE

Glossary of Terms

Abbreviation / Acronym	Description
Acknowledger	A person who is a member of the Functional role that has the privileges to acknowledge (take ownership) of an incident under a specific Incident category. These privileges are set by the system administrator.
Alert / App Alerts	Alerts are notifications sent out by ICM App to alert the recipients of an occurring incident or an activity within the App system that needs the recipients action e.g. if an incident is not acknowledged within a pre-determined time. Alerts are push notifications, that may or may not override phone settings, in the form of a symbol or icon with tunes based on the severity of incident. The alerts will continue unless user dismisses it or takes action that cancels the cause of alert trigger.
Authorized person / Authorized user	A user of the ICM App who has been given the pre-requisite privileges by the system administrator to perform a certain system activity like take ownership of an incident, confirm that an incident is of severity level 3, etc.
Cache	A hardware or software component that stores data so future requests for that data can be served faster.
Button	Button is a graphical user interface in a small outlined area on the screen that will perform a function when the user clicks it. Some of the buttons in the ICM app are Contact Button (linked to a mobile no or incident owners or recipients), Emergency Button (Police, Ambulance or

	Civil Defense hotlines), Feedback Button (user to provide text feedback).
ERP	ERP (Enterprise Resource Planning) refers to the systems used by Miral to manage day-to-day business activities, such as HR, Finance, procurement, project management, etc.
Geolocation	Identification or estimation of real-time geographic location of the person (mobile device) using the ICM mobile App by generating a set of geographic coordinates. The location can be identified by GPS, Wi-Fi position or others
GPS	Global Positioning System is a navigation device or receiver that is capable of receiving information from GPS satellites and then to calculate the device's geographical position. Using suitable software, the device may display the position on a map
Graphical Slider	The Graphical slider is a graphical control element with which a user may set a value by moving an indicator, usually in a horizontal fashion. Colored shaded area can be superimposed on top of the slider to indicate levels like red, amber & green for severe, significant, and minor severity levels respectively
Icon Button	Buttons respond to mouse clicks to trigger a system action or event. The information on an Icon button is represented by an icon (image) instead of text. E.g. A "Call Mobile" button can be represented by the image of a mobile instead of text on the button.
ICM App	ICM (Incident Communication Mobile) App is a mobile application that that is used to report an incident and to notify relevant people on the status of the incident in real-time.

	The application can work on mobile devices (iOS & Android) as well as Web Application.
IMT	Incident Management Team
IRT	Incident Response Team: The team on the ground that first responds to an incident e.g. first aider, security guard, etc.
Incident	Incident is an uncontrolled or unexpected event occuring in a workplace or location that may cause or has caused injury, illness, or property damage or some combination of all three in varying degrees from minor to severe levels of negative impact. Incidents are categorized into "Incident Category" and subcategories of "Incident Type"
Incident Category	All incidents are assigned to categories for easy classification of incidents. Some of the categories are HSE, Media, Security, etc. Categories are set by the system administrator.
Incident Status	These are statuses used by the ICM App to track the progress of the Incident. The incident status is used to trigger actions and for reporting purposes (dashboards & reports). The current status used is "NEW", "WORK IN PROGRESS", "RESOLVED", "ON-HOLD", and "CLOSED". System administrator will maintain the Status table with the definition of each status.
Incident Type	Incident type are sub-categories under the Incident Category i.e. crowd surge, fights, bomb threats are examples of incident types under the Incident Category "Security". Incident Type table is maintained by the system administrator
Initiator	The person who logs or records the incident into the Incident Communication Mobile App.

IVR	IVR (Interactive Voice Response) is a pre-recorded voice message that is sent to the Recipients either for incident notification or alerts.
Location Category	YAS has an area of over 17 sq. kms covering Yas Mall, Hotels & apartments, YAS Marina, and others. These locations are categorized for better reporting purposes e.g. Theme Parks, Real Estate Projects, etc.
Location site	Location sites are specific areas defined within a Location category for a more precise reporting of an incident. E.g. Yas Waterworld and Ferrari World is categorised under "Theme Park". All the location sites for the ICM App is maintained by the System Administrator.
Miral	Miral is an Asset Management Organisation responsible for creating and managing destinations in Abu Dhabi. Miral leads the development of Yas Island, a world-class leisure and entertainment destination that is home to Ferrari World, Yas Waterworld, Yas Marina and others
Notification	Notification is a message or email or icon symbol (alert) that appears when the ICM App wants to inform the App user or a Recipient on an Incident creation, an Incident status change, or any action required from the Recipient. ICM App solution can push notifications even when user is not using it, so that important information or activity taking place in the App is not missed.
OTP	One Time Password (OTP) is type of password that is valid for only one use. The password becomes invalid after it has been used and cannot be used again. This is required for two-factor authentication where the user would require a PIN no as well as a mobile number.
Owner / Incident Owner	People who has the privileges to acknowledge the incident. By acknowledging, he/she has taken

	ownership of the end to end monitoring of the Incident
Parameter	Parameter is an element of a system that is useful, or critical, when identifying the system. Defining key elements as a parameter gives the system administrator the flexibility to change it at any time without modifying every page or program, thus reducing the dependency on IT programmers and developers. Elements such as emails, logos, names, contact nos, etc. can be managed as parameters.
Recipients	People who is identified by the system to get the Initial notification when an Incident is created. Every incident will have unique set of Recipients based on the location site of the incident, the Incident severity and Incident type
Root Cause	Root cause is the initiating cause of a condition(s) or event(s) that has led to the incident.
Severity Factor Range	This defines the level of severity of the incident. It is depicted as a number or score. For the ICM App, the severity factor is defined between ranges from 1 to 10. A factor range or score from 1-4 means incident of Minor severity or severity level 1. A factor range between 5-7 is severity level 2 A factor range between 8-10 is severity level 3 The maximum range and Levels are to be parameterized.
Severity Level	Severity Level or Incident Severity Level are categorization of the impact of an incident that has occurred. In ICM App Solution, it is parameterised at 3 levels 1) Severity L1 /Severity Level 1 - Minor 2) Severity L2 /Severity Level 2 - Significant 3) Severity L3 /Severity Level 3 - Severe

SIMT	SIMT (Strategic Incident Management Team) is the Miral leadership who needs to be kept informed of any occurrence of Severity Level 3 (Severe) incidents. They will have access to the ICM solution Dashboards and reports.
Severity L1 /Severity Level 1	Incidents that are classified as having minor negative impact. (Factor range 1-4)
Severity L2 /Severity Level 2	Incidents that are classified as having major or significant negative impact. (Factor range 5-7)
Severity L3 /Severity Level 3	Incidents that are classified as having severe negative impact. (Factor range 8-10)
SMS	SMS (Short Message Service) is a text messaging service component of most mobile device systems.
System Administrator	System Administrator is the person who is responsible for the configuration, support and maintenance of the ICM App solution.
Time stamp	Timestamp is the current stored date/time of creation or modification or deletion of a data file or transaction file in the ICM App Solution.
Timer	A timer in the ICM App Solution is a software program that counts down a specified duration of time that is pre-set and triggers an action or notification.
Users	Refers to the people who are authenticated to use the ICM App Solution either through mobile devices or desktop. They have a user account and is required to authenticate oneself with password and other credentials. Their details are maintained by the System Administrator. Users of the system are Initiators, Incident Owners, some section of the Recipients and the System Administrator.

Table of Content

1 Introduction

1.1 Scope

This document provides the high-level user requirements for an Incident Communication mobile (ICM) app that can work on both Android and iOS. The mobile app will be used by Miral Staff, Miral subsidiaries staff, Miral contractors and selected partner's staff at YAS Destination to manage any incidents arising at Yas Island i.e. Projects at Miral, Theme Parks, Operational Assets and YAS Destination in general.

The mobile app is to function as a tool for incident capture, communication & collaboration and management reporting. It is not meant to operate as a full-fledged Incident Management Tool.

1.2 Objective

The main objective of the Incident Communication Mobile App is not just to capture incidents but to notify the right people at the right time with the right information to ensure quicker response to incidents. With the App in place, Miral aims to have a cohesive real-time view of the incidents, improved performance timelines as well as strategic information for any decision making.

The key benefits expected from the solution is

a) Immediate notifications ensuring quicker response time to address incidents
b) Centrally located real-time information for viewing and decision making
c) Performance measurement & KPIs
d) Reputation Management
e) Collaboration between teams
f) Knowledge capture

Note: The "Incident Communication Mobile App" will be referred to as the "ICM App" for the rest of the document.

2 Business Requirements

There are over 1000+ stakeholders in Yas Island namely Miral staff, Miral subsidiaries, Miral contractors & sub-contractors and YAS Destination's partners.
The Incident Communication Mobile ICM App should have facility to record an incident with option of taking videos, photos, etc. The Apps critical feature would be to notify all the relevant stakeholders of an incident, based on the type of incident, its severity and location site.

The App is not intended for public use. It can be downloaded by anyone. However only users authorized by Miral can activate it. There is expected to be 200+ active App users. Activation will be via a 2 factor authentication with OTP i.e. once user signs in with activated User id and password, there will a verification code that will be sent to the mobile number provided by the user. User needs to enter the verification code to complete the activation.

The system should be parameterized to the maximum so that the dependency on developers or IT staff should be minimal to nil. Only the system administrator should have access to the parameter and system set-up modules that drives the functionality of the ICM App.

2.1 Business Concept

The basic business requirement is for a Reporting tool that is very user friendly and intuitive ensuring seamless adoption of the ICM App. The App will be used by the stakeholders of Miral for reporting an incident or setting up a planned event.

The core of the ICM system is the notification work flow that gets triggered when an incident or event is reported. The ICM App should send out the notifications immediately to all the relevant stakeholders as soon as an event or incident is reported. The system identifies the stakeholders by their functional roles. The notification workflows will be pre-set by the system administrator to automatically notify the predetermined set of functional roles e.g. The Project manager or HSE

Supervisor; based on a combination of the 3 key parameters namely (refer section 2.3):
a) the **location** of the occurrence of the incident e.g. Clymb or Miral HQ,
b) the **type of incident** i.e. whether fire, structural damage, near miss, etc. and
c) the **severity** of the incident.

There should be minimal number of clicks for user to capture an incident especially for emergency situations when users may not be in a position to think fast on their feet. Most of the process should take place in the back end by the system.

Say for example a fire or smoke is observed in Ferrari World. For reporting the incident, the user will:

- Enter the Incident type, say "Fire"
  Note: The system will pick the Incident category i.e. "HSE" based on the Incident type. The system will also display the default severity level on a graphical slider scale (say for "Fire" it is Severity L3 – factor 8, refer section 2.2.1).
- System will pin point the exact location of the user via geolocation within an accuracy radius of 50 m and prompt the user to confirm location. If the user is not in the location of the incident, then the user can select the actual location from location drop-down. In this example, incident has occurred in Ferrari World.
- If it is not a severe fire, the user can reduce the severity by sliding the graphical scale to bring severity level to a L2. For current example, assume it is a Severity Level 2 incident and the user has brought down the severity to factor 4 – Severity level 2.
- The User will click <REPORT> button to trigger the notification workflow.

Incident type "Fire" falls under Incident Category **HSE** i.e. **Health, Safety & Environment**. The system will identify all the **functional roles** that should be notified of a fire of **Severity L2** intensity occurring at **Ferrari World** that falls under **HSE** Incident Category. The system will check the pre-defined channel of notification i.e. whether email, SMS, etc. and send out the notification to all the identified functional roles (referred to as Recipients) at the same time.

The workflow notification should go out based on the severity levels L1/L2/L3. There are 3 categories of stakeholders that the incident notification from system goes out to:

i. IRT (Incident Response Team): They are the initial on the ground responders. They will be notified on incidents of all severity levels i.e. L1, L2 & L3
ii. IMT (Incident Management Team): They are the management team and higher level of responders. They will be notified of only the severity L2 and L3 incidents
iii. SIMT (Strategic Incident Management Team): They are the leadership team and will be notified on only the severity L3 incidents.

For the current example of fire occurring at Ferrari world, the Recipients under IRT and IMT will be notified of the fire.

Any of the Recipients can increase the severity level. If the fire situation has escalated, the severity level can be increased to a Severity L3. This will automatically trigger the notification workflow of the next level i.e. L3 thereby notifying the recipients under functional roles IRT. IMT and SIMT.
Note: SIMT will be notified only after confirmation by IMT. Refer section 2.3.1.3.2 Incident Notification.

Recipients can be notified through various channels i.e. via eMail, App notification, mobile call, etc. The channel set-up and notification workflow is detailed in section 2.3.2

2.1.1 Key Modules

The ICM App will have 4 key functional modules as below. Users can access the modules or screens based on the system privileges provided by the system administrator:

i. SYSTEM SET-UP & MAINTENANCE: Accessed only by the system administrator, this module has all the parameter and master set-up tables for Incident and

Event, Location, Functional groups, User maintenance, notification workflow and other system feature required.

The data for master tables is available in Appendices 4.1: Miral Information sheet.

ii. INCIDENT: The Incident module is the core of the ICM App. Users can report an incident or address/action an incident through this module. System will automatically send out the appropriate notifications and/or alerts as required.

iii. PLANNED EVENTS: Users can schedule events like concerts, rallies, conferences, etc. This module enables stakeholders to be notified of all events and avoid conflicts in planning or scheduling events.

iv. DASHBOARD & REPORTS: Contains Dashboards that visually display a consolidated view of incidents and other information for management review and strategic decisioning. Users should be able to filter the data on-demand and further click the graphs to drill-down and view the underlying data.

There can be both on-demand and scheduled reports. Reports can be extracted to excel, pdf or word.

Further details on the above modules are provided in sections 2.2 to 2.5.

2.1.2 Mobile App features

i. App System should be highly responsive, intuitive and easy to use.
ii. The app should be branded by Miral branding guidelines with an option to have different branding per entity in the future.
iii. Native Android & IOS.
iv. Log In with user authentication and stay logged in till user logs out.
v. All functionality elements should be parameterised as much as possible and should be easily controllable by the system administrator
vi. The ICM App should capture all essential information such as user’s credentials, activities and time stamps.
vii. System should display appropriate & user friendly error messages.

viii. SMS and messages generated from the app should be transmitted via a toll free number so that the users are not charged for the same.

ix. Offline Capability: The ICM App should operate as an offline app when there is no internet connection available i.e. user should be able to raise an incident in real time, even if the internet is not accessible or very weak.

x. All buttons, options, drop down menus, etc. should be icon based or graphically represented for better user experience. System should have strong visual impact, for example; big graphical buttons, pop-up calendar when user clicks date field, etc.

xi. The incident severity should be represented by a graphical slider (1-10)

xii. Alert or push notification facility that can be sent out to all ICM users by the system administrator

xiii. Search field should have both auto fill as well as Smart Search feature where suggested search strings are displayed beneath the search field; all dropdowns to have the auto fill, smart search, auto predict as applicable.

xiv. App should include accessibility features like changing the font size or inverting the app screen colours.

xv. Document repository for Help Module: Provision to store Standards, Procedures and Policy documents, Help documents in the back end. The App should have a help button that links to the relevant document or file for easy retrieval.

xvi. User can customize the media download preference i.e. whether over WI-FI only, over mobile data only, anytime or manually only.

xvii. Feedback button or option for users to provide feedback.

2.1.3 File format

The ICM App should have feature to upload any existing file/photo/video/audio content from the mobile device gallery when using mobile application.
In addition, provision should also be provided to upload any file, photo or video content from local device if using web application.
System administrator should be able to specify the file formats and the respective maximum size that can be uploaded / downloaded for viewing. Some file types provided below

- Standard graphic file formats include bitmap, JPEG, PNG, TIFF & GIF
- Audio file like MP3, WAV, MPEG4
- Other file formats like DOC, DOCX, XLS, PPT, PDF, MSG

File types not conforming to the parameterized types cannot be uploaded or viewed.

2.2 System Set-up & Maintenance

Only the System Administrator has access to the System Set-up and Maintenance Module. This module contains all the parameter and system master tables that are relevant for the functioning of the ICM App.

The System Administrator should have the facility to Add or Modify or Delete the information in the master or parameter tables.

2.2.1 Incident

An incident can be an accident, fire, fatality, medical emergency, near miss, safety observation, security related, etc. Every Incident type is characterized under an incident category and an Incident Severity level.

2.2.1.1 Incident Severity Level

The Incident Severity level indicates the severity of the incident i.e. whether Minor, Significant or Severe. Only the system administrator should have rights to define the parameters for the Incident Severity Level i.e. the Factor range and colour code

The ICM App should display the Incident Severity level as a sliding scale of 1-10, where 1 is the lowest severity factor and 10 is the highest. Following table shows the 3 levels of severity L1 – Minor, L2-Significant and L3-Severe and their respective factor ranges and colour coding.

Severity level	Severity name	Factor	Colour
L1	Minor	1-4	Green
L2	Significant	5-7	Amber
L3	Severe	8-10	Red

The System should validate that there are no overlapping factors and duplicates. The system should also ensure that the full range from 1 to 10 is covered during the incident severity level parameter set-up.

2.2.1.2 Incident Category

All incidents are currently grouped under 5 categories as shown in table below.

S.No	Incident Category ID*	Incident Category Description
1	GST	Guest Related
2	HSE	Health, Safety & Environment
3	MED	Media
4	SEC	Security
5	UTY	Utility

2.2.1.3 Incident Type

The system administrator should be able to capture all possible types of incidents. These incidents should fall within one of the Incident categories as shown in table below.

Each incident type will be tagged to a default severity factor. When logging an incident using the ICM App, the user should input the Incident Type. The graphical slider provided will default to the Severity Factor set up (refer below table). The user can increase or decrease the severity by moving the slider.

S.No.	Incident Type	Incident Category ID	Severity Factor*	Hard Factor*	Minimum Cap*
1	Fatality	HSE	10	Yes	-
2	Injury	HSE	6	No	1
3	Medical Emergency	HSE	6	No	-
4	Fire	HSE	8	No	4
5	Structural damage	HSE	4	No	-
6	worker welfare violation	HSE	4	No	-
7	HSE violation	HSE	4	No	-
8	inclement weather	HSE	4	No	-

9	Near Miss	HSE	4	No	-
10	Security violation	SEC	7	No	4
11	Crowd Surge	SEC	4	No	-
12	Crowd Fights	SEC	4	No	-
13	Bomb Threat	SEC	10	Yes	-
14	Suspicious Package	SEC	4	No	-
15	Guest Safety	GST	4	No	-
16	Guest Experience	GST	4	No	-
17	Near Miss	GST	4	No	-
18	Power Failure	UTY	4	No	-
19	Water shutdown	UTY	4	No	-
20	Telecom/IT Failure	UTY	4	No	-
21	Flooding/Water leakage	UTY	8	No	4
22	Negative coverage/Trend	MED	4	No	-

A Hard Factor of "Yes" means the severity factor (graphical slider) cannot be changed or updated while logging the incident.

There will be a minimum cap set for some Incident Types. If set, then the initiator cannot reduce the severity below the minimum factor set.

E.g. based on the table set above, when logging an incident of incident type "Fire", the system will default the severity factor to "8" (Severity L3). As this is not a "Hard Factor", the initiator can reduce or increase the severity. However the severity cannot be reduced below severity factor 4 as there is a minimum cap set.

*The value in ID and Factor fields used is only indicative to better explain the parameter set-up

2.2.2 Location

The ICM App will be used to manage any incidents arising at Miral Projects, Theme Parks, Operational Assets and YAS Destination in general.

2.2.2.1 Location Mapping

The ICM app should have a Geolocation tracking to capture the location of the user. Geo-fencing should be accurate up to 50 m. If Geolocation cannot identify exact location i.e. if on the borderline or overlap of location, then suggested locations should be shown so that the user can select the right location.

Manual location search should be available if the App user is in an area without GPS or Internet connectivity.

The various location categories and the location sites are displayed in the sections below.

2.2.2.2 Location Category

S.No	Location Category ID**	Location Category Description
1	MOF	Miral offices
2	TPP	Theme Park Project
3	REP	Real estate Projects
4	THP	Theme Parks
5	ROH	Residential/office/Hotel
6	ROL	Retail outlet
7	YAS	Yas Marina
8	OOA	Other operational asset
9	EVT	Events
10	DYS	Destination Yas

2.2.2.3 Location Site

The location sites are categorized under location category.

S.No	Location	Location category ID
1	Miral HQ	MOF
2	Miral Site Dar Site Office	MOF
3	Miral Site WB Site Office	MOF
4	WB TP Project	TPP

5	WB Car Park Project	TPP
6	Clymb	TPP
7	Sea world	TPP
8	5D Cinesplash	TPP
9	Yas Village project	REP
10	Yas South (IDR)	REP
11	Project Acqua	REP
12	Project Windsor	REP
13	Ferrari World	THP
14	Yas Water World	THP
15	W.B Abu Dhabi	THP
16	Farah Offices	THP
17	Zeina Complex	ROH
18	Muneera Complex	ROH
19	Gate towers	ROH
20	Cipriani	ROL
21	Cascade dinning	ROL
22	West Yas Plaza	ROL
23	Yas Marina	YSM
24	West Yas School	OOA
25	Event	EVT

**The value in ID field used is only indicative to better explain the parameter set-up

The location site information is used for functional role contact set-up. It is also used during planning an event and while logging an incident when internet connectivity is either not available or there is an overlap (intersections) in location.

2.2.3 Functional Groups

The Functional Group parameter set-up is key to ensure that the right incident notification goes to the right people at the right time.

2.2.3.1 <u>Functional Category</u>

The current functional category will have 3 teams.

S.No	Functional Category ID	Functional Category Description
1	IRT	Incident Response Team
2	IMT	Incident Management Team
3	SIMT	Strategic Incident Management Team

2.2.3.2 *Functional Role*

Functional roles are defined against each category.

*** Functional roles that are distinct to every location site i.e. every location site may have a different HSE Supervisor.

S.No	Functional Role	Functional Category ID
1	HSE Supervisor ***	IRT
2	Security Supervisor ***	IRT
3	First Aider (group) ***	IRT
4	Fire warden (group) ***	IRT
5	Duty Manager ***	IRT
6	Operations Manager ***	IRT
7	Guest Experience Supervisor ***	IRT
8	Incident Response Manager ***	IMT
9	Facility Manager ***	IMT
10	Project Manager ***	IMT
11	Guest Experience Manager ***	IMT
12	Operations Manager ***	IMT
13	Miral BC Manager	IMT
14	Miral Facility Manager	IMT
15	Miral Project Manager	IMT
16	Miral Incident Response Manger-HSE	IMT
17	Miral Incident Response Manger-Technology	IMT
18	Miral Incident Response Manger-Admin	IMT
19	Miral Incident Communication Lead	IMT
20	General Manager ***	SIMT

21	Farah CEO	SIMT
22	Miral CFO	SIMT
23	Miral General Counsel	SIMT
24	Miral Chief Portfolio officer	SIMT
25	Miral Head of HR	SIMT
26	Miral Head of Commercial	SIMT
27	Miral Head of Strategy & Innov	SIMT
28	Miral Head of Destination Management	SIMT
29	MiraL CEO	SIMT

2.2.4 Event Type

The Event Type data is maintained for use in the Planned Events module. All the possible event types will be stored in the table. Below table represents few event types.

S.No	Event ID	Event Type
1	E01	Marathon
2	E02	Road Closure
3	E03	Drill
4	E04	Others

2.2.5 Stakeholder Contact Maintenance

The ICM App communicates with 3 kinds of stakeholders as follows. System should store all the relevant information, especially the contact details for notification.

2.2.5.1 App Users

The App Users are the authorized people who actively use the ICM app. They are granted privileges by the system administrator to access the modules of the ICM App to report an incident or planned event, acknowledge and take ownership of an incident, view dashboards, etc.

Initiators, Incident Owners, some section of the Recipients and the System Administrator are all App users. Their profile data like user id, name, registered eMail and mobile no is captured at the time of initial user activation. Further data relevant to the user profile should be captured.

UserID (or Login Id)	Name	Password hash	eMail	Mobile No

2.2.5.2 Functional Role Contact maintenance

Table should be maintained by the system administrator to store the relevant contact information of every functional role under a location site. The eMail and mobile no are critical to the notification workflow to ensure the notifications are received by the functional roles i.e. Recipients identified by the system.

The Functional role contact Id should be a combination of the Functional Role, Category & Location site so that role can be easily identifiable from the Contact ID.

Functional Role Contact ID	Functional Role	Location site	Mobile No	Alternate Mobile No	eMail
		Miral HQ			

2.2.5.3 Planned event stakeholders

Table should be maintained by the system administrator to store the relevant contact information of all the stakeholder who will receive a notification when a planned event is set and approved. It also contains information on whether a user is a moderator or not. Notification of a planned event will be triggered only when it is approved by the moderator(s).

The Event user ID should be distinct from the App User ID and the Functional Role Contact ID. Further user profile information relevant to the "Planned Events" module should be captured.

Event User ID	Name	Moderator (Yes/No)	Mobile No	Alternate Mobile No	eMail
PE01					
PE02					

2.2.6 Functional Role Assignment

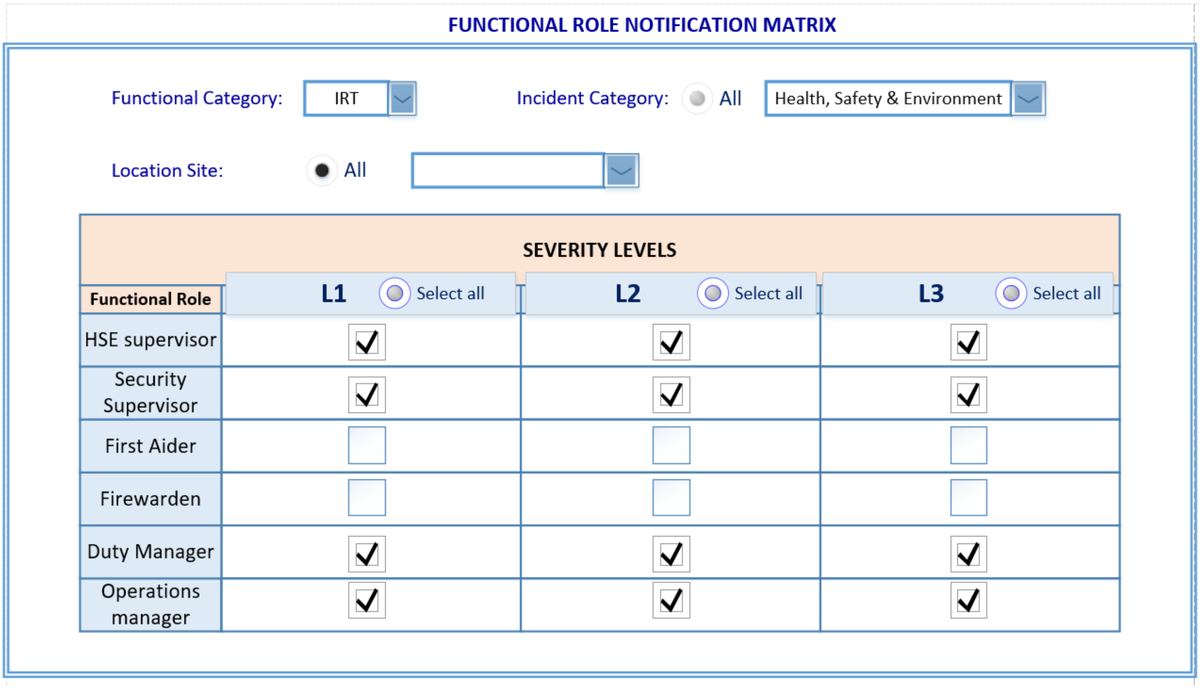
The core work engine of the ICM App is driven by 4 parameters namely
a) Location Site – refer table in section 2.2.2
b) Incident Category – refer table in section 2.2.1.2
c) Severity Level – refer table in section 2.2.1.1 and 2.2.1.3
d) Functional Role – refer table in section 2.2.3.2

Following sections lists the set-ups that are integral in directing the notification and the work-flow of the incidents.
The module should be available to easily map functional roles (users) to key functions on:

a) Identification of the Recipients who will be notified when a Severity L1, Level 2 or Level 3 incident is raised.
b) Whether the Recipient can acknowledge or take ownership of an Incident.
c) Whether the Recipient can increase or decrease the severity level of the Incident set by the Initiator.
d) Whether the Recipient can authorise or confirm the Severity L3 Incident for notification to the SIMT.

2.2.6.1 Functional Role Notification Matrix

The Functional Role Notification Matrix must be set up by the System Administrator. This set-up is critical as it identifies the Recipients that get the initial notification when the Incident is first created.



FUNCTIONAL ROLE NOTIFICATION MATRIX

Functional Category: IRT ▾ Incident Category: ○ All Health, Safety & Environment ▾

Location Site: ● All ▾

	SEVERITY LEVELS		
Functional Role	L1 ○ Select all	L2 ○ Select all	L3 ○ Select all
HSE supervisor	☑	☑	☑
Security Supervisor	☑	☑	☑
First Aider	□	□	□
Firewarden	□	□	□
Duty Manager	☑	☑	☑
Operations manager	☑	☑	☑

The Functional Category, Incident Category and location site should be easily selected by the System administrator e.g. drop-down having smart filters. Once the Functional Category is selected, the system should display the pre-defined Functional roles that are set-up against the Functional Category. The system administrator can select the Functional Roles to whom the notifications should go to based on the severity levels. Option to "Select All" should be available and made default. For exceptions, system administrator can select the specific Incident category or location site to set-up the functional role notification.

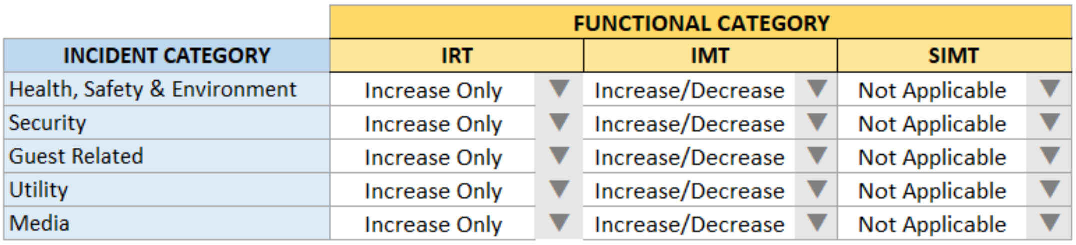
This module is used to identify the Recipients, especially for the initial Incident Notification as detailed in section 2.3.1.3.2 - Incident Notification.

2.2.6.2 Severity Level Change Matrix

The Severity Level Change Matrix is to be set up by the System Administrator. This module gives the user privileges to either increase or decrease the severity level factor set by the Initiator.

The functional roles are categorized under the functional category (refer section 2.2.3). As per current business requirement, Recipients from:

a) IRT (Incident Response Team) can only increase Severity level i.e. using the severity factor slider, they can increase severity factor from 1 -> 2 -> 3 -> 4 -> 5 -> 6 -> 7 -> 8 -> 9 -> 10. IRT cannot decrease the default severity factor set by the Initiator.



	FUNCTIONAL CATEGORY		
INCIDENT CATEGORY	IRT	IMT	SIMT
Health, Safety & Environment	Increase Only ▼	Increase/Decrease ▼	Not Applicable ▼
Security	Increase Only ▼	Increase/Decrease ▼	Not Applicable ▼
Guest Related	Increase Only ▼	Increase/Decrease ▼	Not Applicable ▼
Utility	Increase Only ▼	Increase/Decrease ▼	Not Applicable ▼
Media	Increase Only ▼	Increase/Decrease ▼	Not Applicable ▼

b) IMT (Incident Management team) can increase or decrease the default factor set in the system against the Incident Type, but within the minimum cap if defined.

c) SIMT (Strategic Incident management Team) have only View privileges and hence the Severity Level Change set-up is not applicable to them.

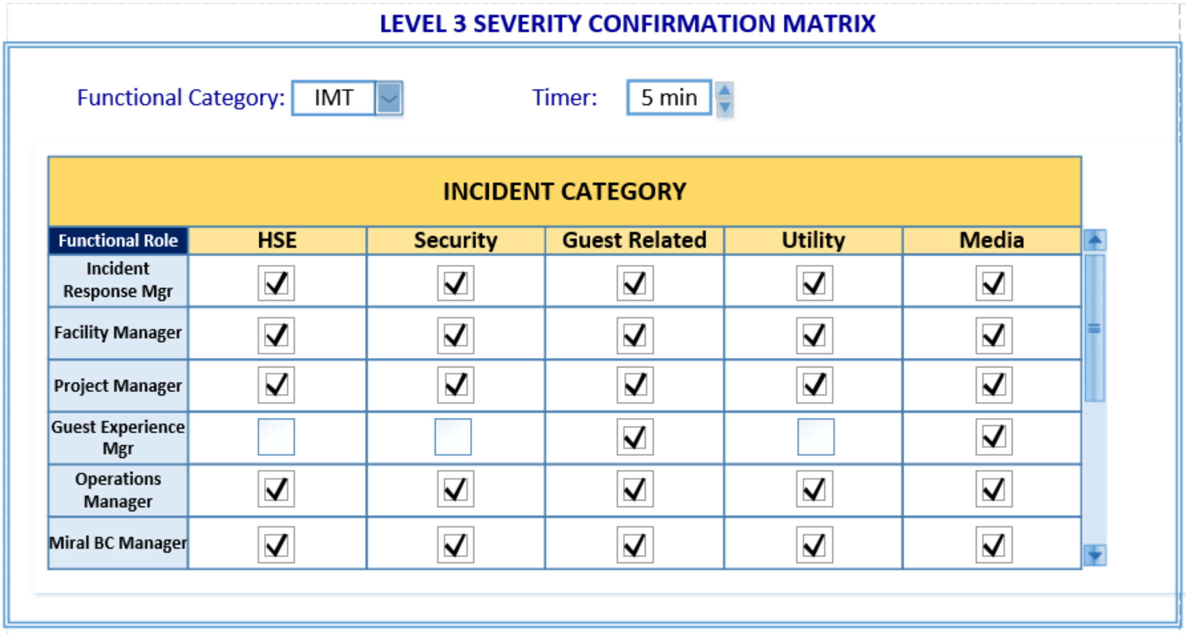
Screenshot above shows the possible set-up. A dropdown should be provided with:

- Increase Only
- Decrease Only
- Increase/Decrease
- Not Applicable

2.2.6.3 Level 3 Severity Confirmation Matrix

The L3 Severity Confirmation Matrix is to be set up by the System Administrator. This set-up gives the user privileges to confirm the validity of an L3 Incident. As per the current business requirement, notification of all Severity L3 Incidents goes out only to the IRT and IMT personnel at first. The L3 notification goes to the SIMT only after confirmation by the authorized person from IMT team i.e. as per the set-up done in the module.

Though currently only IMT team member can confirm the Severity Level 3, the system however should have the flexibility of providing Confirmation privileges to anyone irrespective of the functional category they belong to.



LEVEL 3 SEVERITY CONFIRMATION MATRIX

Functional Category: IMT

Timer: 5 min

Functional Role	INCIDENT CATEGORY				
	HSE	Security	Guest Related	Utility	Media
Incident Response Mgr	☑	☑	☑	☑	☑
Facility Manager	☑	☑	☑	☑	☑
Project Manager	☑	☑	☑	☑	☑
Guest Experience Mgr	□	□	☑	□	☑
Operations Manager	☑	☑	☑	☑	☑
Miral BC Manager	☑	☑	☑	☑	☑

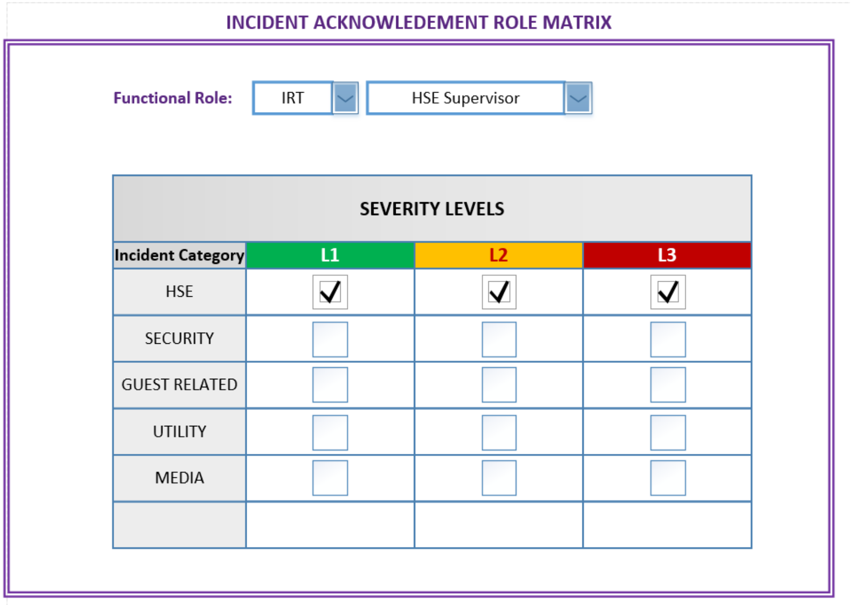
When system administrator selects the Functional Category, all Functional roles falling under the category should be displayed along with the Incident category. The administrator can check all roles that are authorized to confirm Severity Level 3.

A timer field should be provided. If the Severity level L3 is not confirmed within the set time, then system will automatically assume confirmation and proceed to notify the SIMT members on the L3 Incident.

2.2.6.4 Incident Acknowledgement Role Matrix

All Incidents logged should have an incident Owner who will acknowledge and take ownership of the incident and monitor it till it is closed. This is detailed in section 2.3.1.3 - Incident Workflow.

The Incident Acknowledgement Role Matrix ensures that the right person takes ownership of the incident. When a user <Acknowledges> an incident, the system validates via the role matrix if he/she is eligible to take ownership. If eligible, the system marks the user as the Incident Owner.



INCIDENT ACKNOWLEDEMENT ROLE MATRIX

Functional Role: IRT | HSE Supervisor

	SEVERITY LEVELS		
Incident Category	L1	L2	L3
HSE	☑	☑	☑
SECURITY	□	□	□
GUEST RELATED	□	□	□
UTILITY	□	□	□
MEDIA	□	□	□

The module should have the facility for system administrator to select the Functional role and check the types of incidents the Functional role can take the ownership of based on the severity level and Incident category.

2.2.6.5 *Functional Role Incident Resolution Matrix*

Once an incident is under resolution (Refer section 2.3.1.3 - Incident workflow) i.e. status = "WORK IN PROGRESS", only Recipients with the pre-requisite privileges can mark an incident as "RESOLVED".
This module should allow the System Administrator to set the privileges for Functional roles who can move an incident to 'RESOLVED" status.

2.2.6.6 *Status Change Notification set-up*

All recipients need not be notified of every incident status change notification other than the Initiator and the Owner of the Incident. This table defines which functional roles should be informed of the status change.

FUNCTIONAL ROLES	INCIDENT STATUS				
	NEW	WORK IN PROGRESS	ON-HOLD	RESOLVED	CLOSED
HSE Supervisor	✓	✓	✓	✓	✓
Security Supervisor	✓	✓			✓

2.3 Incident

The incident module is used to either report an incident or action a reported incident like take ownership of incident, provide resolution comments, etc. Anyone who is logged into the ICM App can report an incident.

Below sections provides details of the Incident & notification workflows.

2.3.1 Incident Life-Cycle

2.3.1.1 User Roles

Following are the Users of the ICM App

a) **Initiator**: Initiator is the person who can log an incident. All authorized users, who have downloaded the ICM App and are active i.e. 2 factor authentication by Miral, can record or log an Incident.

b) **Recipient**: The Recipient is the person who receives notifications or status related information of the Incident. The Recipient notification is set-up (section 2.2.6.1) by the System administrator based on pre-defined criteria of the Location of Incident, the Incident Severity level and the Incident category. They are the group of people that receives the initial notification when the Incident is created. More on the recipient identification and notification is explained in section 2.3.1.3.2
Note: The Recipient need not be an active/authorized user of the ICM App e.g. a Security Guard. However the person should have a mobile no or email to receive the notifications.

c) **Incident Owner**: The person who acknowledges or takes ownership of the incident is the Incident Owner. Only ICM App users who are given the Acknowledge privileges, by the system administrator, can take ownership of the incident. The privileges are segregated by Location, Functional Role, Incident Category and Severity Level E.g. An HSE Supervisor can acknowledge or take ownership of only HSE Incident

d) Viewers: Users given the View privilege. They can view the Dashboards and their related reports.

e) System Administrator: The person who is responsible for the maintenance and support of the system. Only the system administrator has full privileges to the system i.e. full system parameter set-up, notification set-ups & workflow assignments, Functional role assignments, User assignments, view Dashboards, reports extraction among others. The administrator has access to all the modules of the system and can also change the status of any incident with appropriate comments/remarks

2.3.1.2 Incident Status

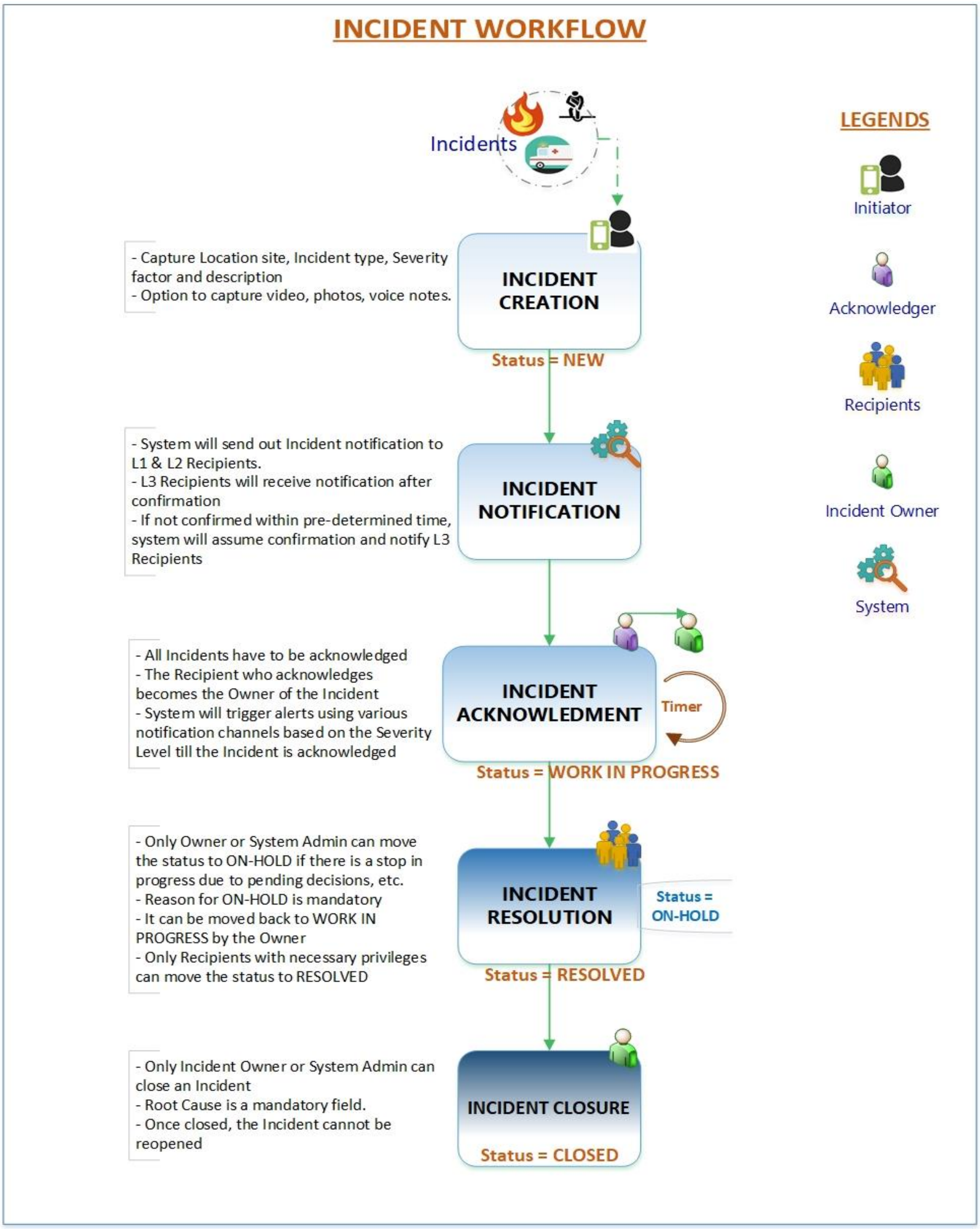
The various status that an incident can hold during its life-cycle are:

a) NEW: This is the initial status when an incident is logged into the ICM App by the Initiator.
b) WORK IN PROGRESS: When the Recipient acknowledges the incident the system will change the incident status to "WORK IN PROGRESS". Only a user with the relevant privileges/authorization can acknowledge an Incident.
c) ON-HOLD: Once incident is in "WORK IN PROGRESS", the Owner can move the incident to "ON-HOLD", if there is any approvals or dependencies keeping the incident resolution from progressing.
The Owner has to provide a reason/remark for moving the incident status to "ON-HOLD".
Incident can be moved back to "WORK IN PROGRESS" from "ON-HOLD" at any time.
d) RESOLVED: Once all the actions or activities are completed by the team, the Recipient with the required privileges or authorization can mark the status as "RESOLVED" with a mandatory remarks/comment.
e) CLOSED: The Incident Owner will mark the incident as "CLOSED" once the resolution has been verified. The Owner has to update the 'Root Cause" field.

Only the owner or the system administrator can close an incident. They can directly move an Incident to "CLOSED" from any of the status of NEW/WORK IN PROGRESS/ON-HOLD, if it is a duplicate incident. In such instances, the incident should be flagged as duplicate and field to be made available to update or link the pre-existing Incident.

2.3.1.3 Incident Workflow

Below identifies the high level process flow of the ICM App from initiation to closure.



- Capture Location site, Incident type, Severity factor and description
- Option to capture video, photos, voice notes.

- System will send out Incident notification to L1 & L2 Recipients.
- L3 Recipients will receive notification after confirmation
- If not confirmed within pre-determined time, system will assume confirmation and notify L3 Recipients

- All Incidents have to be acknowledged
- The Recipient who acknowledges becomes the Owner of the Incident
- System will trigger alerts using various notification channels based on the Severity Level till the Incident is acknowledged

- Only Owner or System Admin can move the status to ON-HOLD if there is a stop in progress due to pending decisions, etc.
- Reason for ON-HOLD is mandatory
- It can be moved back to WORK IN PROGRESS by the Owner
- Only Recipients with necessary privileges can move the status to RESOLVED

- Only Incident Owner or System Admin can close an Incident
- Root Cause is a mandatory field.
- Once closed, the Incident cannot be reopened

2.3.1.3.1 Incident Creation

- Any user who has downloaded the ICM App and given the essential credentials should be able to log an incident e.g. an accident, near miss, safety observation, etc.
- The bare minimum information that needs to be captured by the Initiator is
  - Location site - via Geolocation
  - Incident Type
    - (Combobox or similar options like icon buttons must be provided to enable the Initiator to easily select the Incident category and then proceed to select the related Incident Type
    - As an alternative, the Initiator can also type in the incident type and the system automatically fetches the category that the incident type falls under. The dropdown must have the auto fill/smart search facility.
  - Severity Factor – The default severity factor of the incident type should be displayed via the graphical slider. The Initiator can change the severity level if it is not a hard factor, but within the factor cap limits
  - Description of the Incident – Text field
  - User Id – System will automatically identify the Initiator from his/her login credentials
- The Initiator should have facility to capture additional incident related information like photo(s) of the incident, video(s) of the incident or voice note.

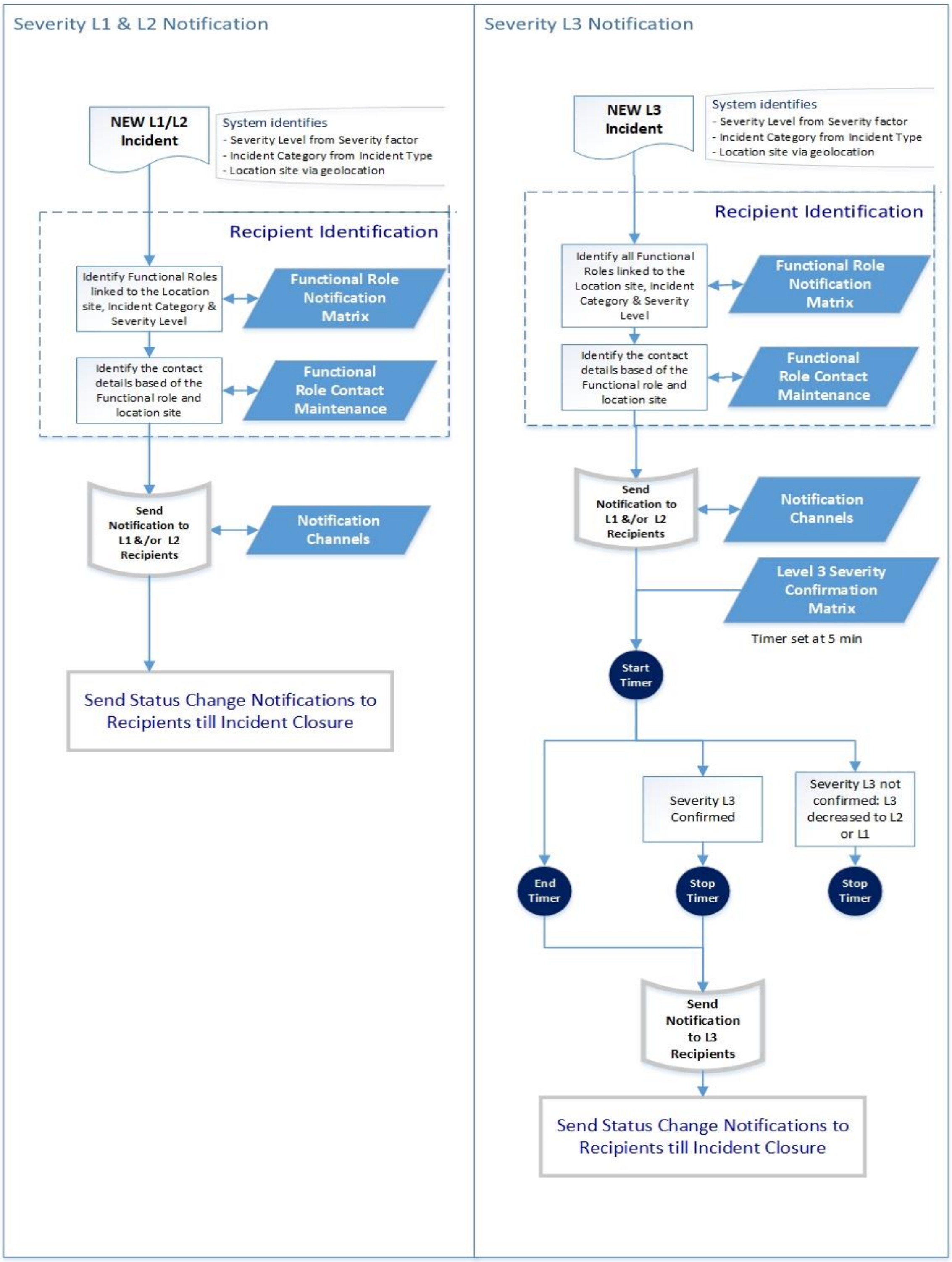
  Note: Attachment formats to be predetermined by system administrator. Refer section 2.1.3

Once the minimum information is captured the Incident will be saved with status as “NEW” status.
All incidents logged will be queued in respective Recipient pools for acknowledgement.

2.3.1.3.2 Incident Notification

- Once an Incident is logged, the system will identify all the recipients who should be notified of the incident.

- System will pull information of the Location site, Severity Level and incident category.
- From The Functional Role notification table, for the specific location site and Incident category, the system will identify all the checked functional roles under the functional categories (IRT, IMT & SIMT) that are to receive the notification based on the incident severity level.


Severity L1 & L2 Notification
NEW L1/L2 Incident
System identifies
- Severity Level from Severity factor
- Incident Category from Incident Type
- Location site via geolocation
Recipient Identification
Identify Functional Roles linked to the Location site, Incident Category & Severity Level
Functional Role Notification Matrix
Identify the contact details based of the Functional role and location site
Functional Role Contact Maintenance
Send Notification to L1 &/or L2 Recipients
Notification Channels
Send Status Change Notifications to Recipients till Incident Closure
Severity L3 Notification
NEW L3 Incident
System identifies
- Severity Level from Severity factor
- Incident Category from Incident Type
- Location site via geolocation
Recipient Identification
Identify all Functional Roles linked to the Location site, Incident Category & Severity Level
Functional Role Notification Matrix
Identify the contact details based of the Functional role and location site
Functional Role Contact Maintenance
Send Notification to L1 &/or L2 Recipients
Notification Channels
Level 3 Severity Confirmation Matrix
Timer set at 5 min
Start Timer
Severity L3 Confirmed
Severity L3 not confirmed: L3 decreased to L2 or L1
End Timer
Stop Timer
Stop Timer
Send Notification to L3 Recipients
Send Status Change Notifications to Recipients till Incident Closure

- From the User maintenance table, system will identify the Users having the specific functional role under the location site. Note: These users are the Recipients.

- Using the contact details (i.e. eMail & mobile no) of the Recipients, system will send out the initial notifications.
- As per current business scenario, notifications to the identified Recipients will be as follows:
  - IRT (Incident Response Team) will be notified of all incidents i.e. Severity Level 1, Level 2 & Level 3 incidents
  - IMT (Incident Management Team) will be notified of only Severity L2 & L3 incidents
  - SIMT (Strategic Incident Management Team) will be notified of only Severity L3 Incident after it is confirmed but authorised person from IRT/IMT

    (Note: If the Severity L3 is not confirmed before a predetermined time set-up in the "Level 3 Severity Confirmation Matrix module", then system automatically confirms it and send out notification to the SIMT.
- The notification channels should be predefined by System administrator. The Recipients will be notified of the "NEW" Incident by SMS, email and App Notification
- Any of the Recipients can increase or decrease the Severity factor if they have the relevant privileges. If this results in a Severity Level change, the notification workflow should reset.

2.3.1.3.3 Incident Acknowledgement

- The incident can be acknowledged only by the Recipient from the IRT or the IMT team based on the set-up done in the Incident acknowledgement Role matrix.
- Once acknowledged the incident status will be moved to "WORK IN PROGRESS".
- The Recipient who acknowledges the incident will be the Incident Owner till the lifecycle of the incident ends. The contact button (mobile no) will be made available for Recipients or Initiator to contact the Incident Owner.
- Alerts will be triggered if the Incident is not acknowledged. The alerts will repeat at set intervals and channels till the incident is acknowledged.
- The no of alert cycle repetitions to trigger escalation has to be parameterised. Once the maximum no of alert cycles is reached, escalation notification should go to the SIMT team

- Once the Owner is assigned, the ownership can be changed only by the system administrator.

2.3.1.3.4 Incident Resolution

- During the resolution process the Owner &/or Recipients should have the facility to collaborate using call buttons and In-App chat feature. Refer section 2.3.3 - Collaboration
- The Owner can move the status from "WORK-IN-PROGRESS" to "ON-HOLD" and back to "WORK-IN-PROGRESS" at any time, if there is any pending decisions, approvals, etc.
- Any of the Recipients who are given the required privileges (section 2.2.6.5) by the system administrator can move the incident to "RESOLVED" with a mandatory update in the Resolution Remarks field.

2.3.1.3.5 Incident Closure

- After the incident is resolved, the Owner (or System Administrator) can close the Incident. The Root Cause is a mandatory field for closure.
- Once the status of the incident is "CLOSED", it cannot be reopened.
- Notification should go out informing all Recipients on the incident closure. (**Note**: This will be set-up in the Status Change notification table; refer section 2.2.6.6)

Whenever there is a change in Incident Status, Notifications in predetermined format should go out to the Incident Recipients, stating the Incident Type, Severity Type, Severity Factor, Location Site, From status, To Status and the relevant remarks if applicable.

2.3.2 Incident Notification & Alerts

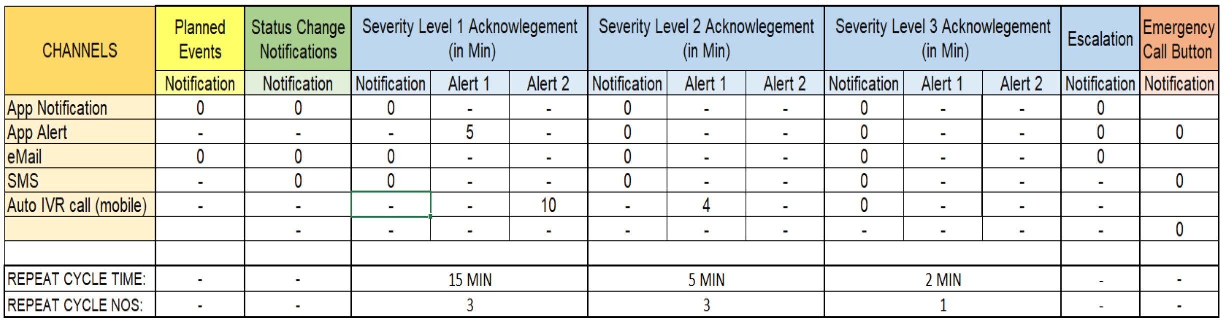
2.3.2.1 <u>Notification Channels</u>

The following notification channels shall be used by the application for all notifications pertaining to incidents, planned events or others

a. App Notifications: Push notifications
b. App Alerts: Tune shall be configured according to the severity of the alert and it shall override the phone settings if it has been changed to silent mode or even if the app notifications or alerts have been turned off

c. Email
d. SMS (Mobile)
e. Auto IVR call (mobile): System will take the necessary information from the Location (geolocation), severity level and incident category and send out the automated voice message to the pre-defined recipients
f. Voice call via App (optional)

App Notification, email, SMS is default notification for all severity levels.
The ICM App should have the provision for the System Administrator to set up notification and alert channels when any transaction triggered, including cascading alert channels according to the Incident severity level.



CHANNELS	Planned Events	Status Change Notifications	Severity Level 1 Acknowlegement (in Min)			Severity Level 2 Acknowlegement (in Min)			Severity Level 3 Acknowlegement (in Min)			Escalation	Emergency Call Button
	Notification	Notification	Notification	Alert 1	Alert 2	Notification	Alert 1	Alert 2	Notification	Alert 1	Alert 2	Notification	Notification
App Notification	0	0	0	-	-	0	-	-	0	-	-	0	
App Alert	-	-	-	5	-	0	-	-	0	-	-	0	0
eMail	0	0	0	-	-	0	-	-	0	-	-	0	
SMS	-	0	0	-	-	0	-	-	0	-	-	-	0
Auto IVR call (mobile)	-	-	-	-	10	-	4	-	0	-	-	-	
		-	-	-	-	-	-	-	-	-	-	-	0
REPEAT CYCLE TIME:	-	-	15 MIN			5 MIN			2 MIN			-	-
REPEAT CYCLE NOS:	-	-	3			3			1			-	-

Channel Notification Table

There should templates to set-up the default messages e.g. for Status change eMail, Incident Acknowledgement Request, etc.

The above table depicts notification channel set-up for
a) Default notification channel for planned events
b) Default notification channels for any status change, etc.
c) Notification for incident acknowledgement and Alerts if not acknowledged; for severity L1, L2 & L3
d) Escalation notification to SIMT if acknowledgement exceeds repeat cycle nos
e) Notification alert when ICM App user calls the emergency line

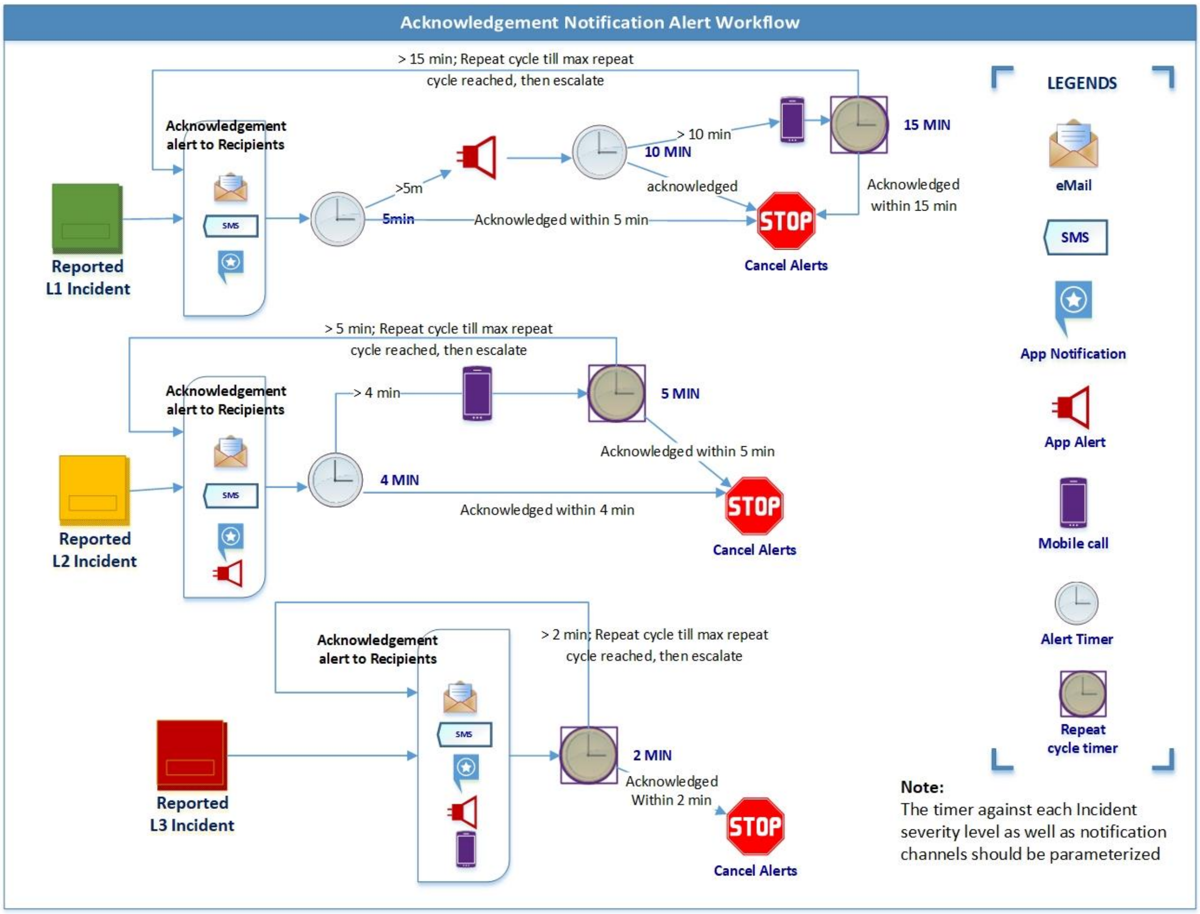
Note: "0" min means immediately triggered.

System admin should be able to create any no of Notification Channel/Alert routes with or without repetition cycles.

2.3.2.2 Incident Acknowledgement Alert Workflow

Notifications should go out to the Recipients who have the privileges to acknowledge an Incident.
If the incident is not accepted within the pre-defined time setup in the Channel Notification table, it should trigger alerts based on the Incident Severity level.

As per business requirement, following is the set-up for Acknowledgement alerts (refer Channel Notification table)


Acknowledgement Notification Alert Workflow
> 15 min; Repeat cycle till max repeat cycle reached, then escalate
Acknowledgement alert to Recipients
SMS
Reported L1 Incident
>5m
5min
> 10 min
10 MIN
15 MIN
acknowledged
Acknowledged within 5 min
Acknowledged within 15 min
STOP
Cancel Alerts
> 5 min; Repeat cycle till max repeat cycle reached, then escalate
Acknowledgement alert to Recipients
SMS
Reported L2 Incident
> 4 min
5 MIN
4 MIN
Acknowledged within 5 min
Acknowledged within 4 min
STOP
Cancel Alerts
Acknowledgement alert to Recipients
> 2 min; Repeat cycle till max repeat cycle reached, then escalate
SMS
Reported L3 Incident
2 MIN
Acknowledged Within 2 min
STOP
Cancel Alerts
LEGENDS
eMail
SMS
App Notification
App Alert
Mobile call
Alert Timer
Repeat cycle timer

Note:
The timer against each Incident severity level as well as notification channels should be parameterized

a) Severity Level 1 (Minor):
   - At 0 MIN: Default Alert to Recipients (having privileges to acknowledge) via SMS, eMail & App notification

- At +5 MIN: If not acknowledged within 5 min, then alert Recipients via App Alert
- At +10 MIN: If not acknowledged in 10 min, then alert Recipients via mobile call (auto IVR)
- Repeat the same cycle after 15 Minutes till acknowledgement

b) Severity Level 2 (Significant):

- At 0 MIN: Default Alert to Recipients via SMS, eMail, App notification, App Alert
- At +4 MIN: If not acknowledged within 4 min, then alert Recipients via mobile call
- Repeat the same cycle after 5 minutes till acknowledgement

c) Severity Level 3 (Severe):

- At 0 MIN: Default Alert to Recipients via SMS, eMail, App notification, App Alert and mobile call
- Repeat the same cycle after 2 minutes till acknowledgement

The notification alerts will repeat till the logged incident is acknowledged i.e. till the Incident has an Incident Owner. If alert repetition cycle times is crossed, the next level i.e. SIMT team should be notified.

2.3.3 Collaboration

The ICM App should act as a strong collaboration tool. The Initiator, Owner and Recipients of the incident should be able to collaborate with one another either by chat or voice calls. By default the Comments feature should be available for all members of the incident to provide comments or chat.

2.3.3.1 Contact Buttons

The ICM App should provide facility for the

a) Initiator to call any of the Recipients by providing a call button against each Functional Role identified.
b) The Owner or Recipients to call the Initiator directly via a call button
c) Recipients to call each other by providing call button against each Recipient Functional Role.

2.3.3.2 In-App Chat

The Incident Owner OR any Recipient of the incident can open a separate secured chat group. He/she will be the Admin of the group and can add the Recipients of the incident to the chat group. Following are few exceptions

i. If chat opened by Owner and Owner is from IRT, then the Acknowledger of the incident group will be a mandatory default member of the chat group.

ii. If chat is opened by anyone of the Recipients other than the Owner or the Acknowledger , then both the Owner and the Acknowledger should be mandatory default members of the chat group

For sensitive information, the Acknowledger can open a chat group and add any of the Recipients, without including the Incident Owner.

2.3.4 Emergency button

Emergency button should be provided for emergency situations. With this facility, user can directly dial the Police, Ambulance or Civil defence via the ICM app.
Separate buttons should be provided all three.

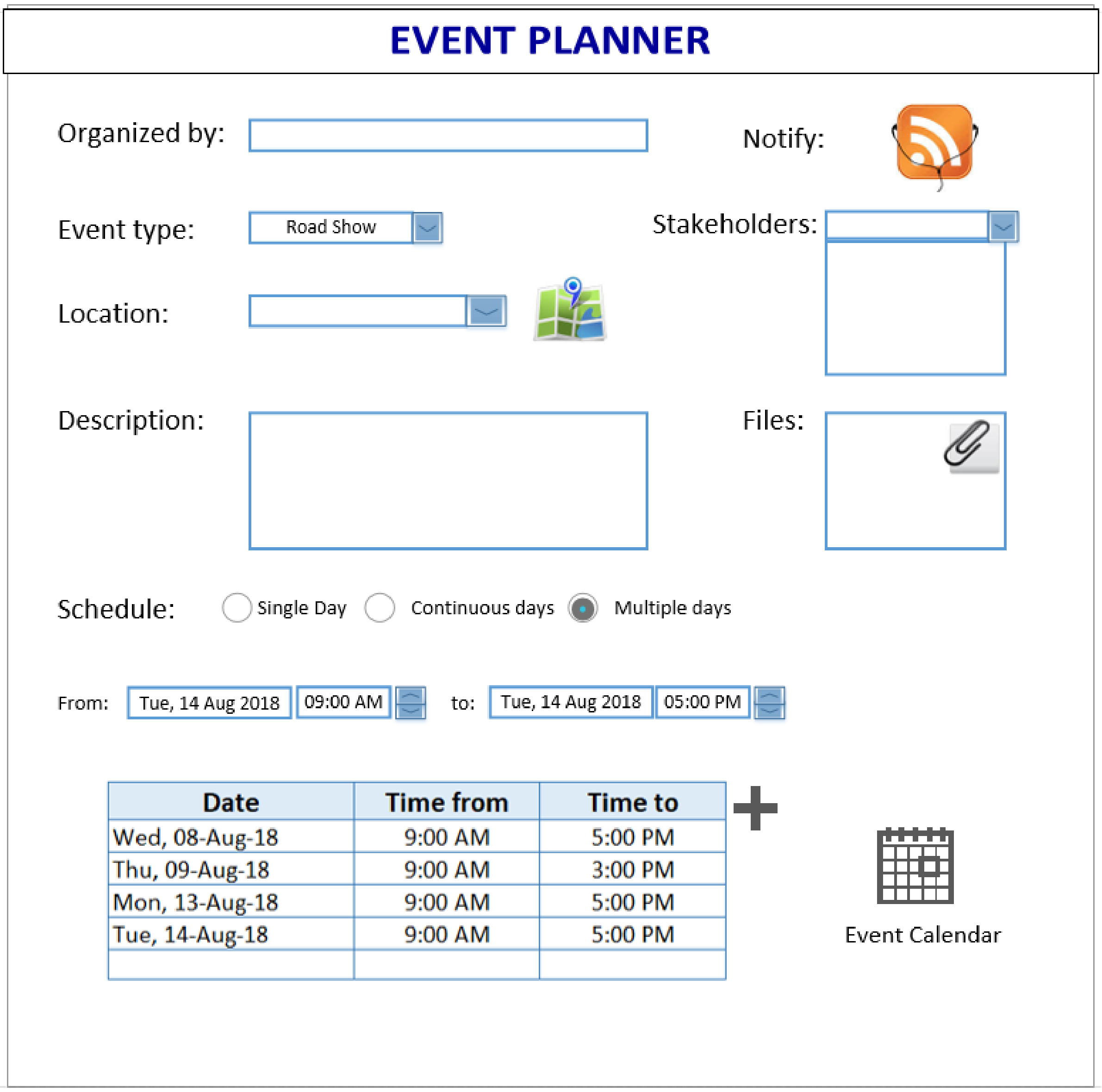
System should be able to identify that an emergency call has been made and create a "NEW" Severity Level 3 Incident with location site (using Geolocation) with Incident type as "Emergency Call". Alerts (SMS, eMail & App notifications OR as set in the Notification channel table) should go out to all the functional roles under the IRT category of that location site, irrespective of the incident category, stating that an emergency call has been made to Police/Ambulance/Civil Defence by <mobile no> (<user name>) at <location site>.

Any of the IRT recipients can take ownership of the incident after investigation and update the Incident category and incident type. The owner can CLOSE the incident if it is resolved. If it is not resolved, the IRT can assign it with the right severity level i.e. Severity L1, L2 or L3 that will follow the regular incident life cycle.

2.4 Planned Events

Many events are organized at Yas Island. This module will be used by users to capture planned events like conferences, rally, road blocks, etc. and notify stakeholders of the event to ensure all are aware of the event. Users who are provided with the required privileges will be able to access the Planned Events module.

The module should have the Calendar and Time clock facility to capture date and time. Below screen diagram gives a representation of the requirement.



EVENT PLANNER

Organized by:

Notify:

Event type: Road Show

Stakeholders:

Location:

Description:

Files:

Schedule: ○ Single Day ○ Continuous days ● Multiple days

From: Tue, 14 Aug 2018 09:00 AM to: Tue, 14 Aug 2018 05:00 PM

Date	Time from	Time to
Wed, 08-Aug-18	9:00 AM	5:00 PM
Thu, 09-Aug-18	9:00 AM	3:00 PM
Mon, 13-Aug-18	9:00 AM	5:00 PM
Tue, 14-Aug-18	9:00 AM	5:00 PM

- The “Organized by” field is a text field.
- The user or event planner will enter the event type using the dropdown provided.
- User should have the facility to select the location either using dropdown or using a location map
- User should be able to provide a brief description of the event
- There should be an option to upload files, video, pictures, etc. The formats and respective sizes should be defined by system administrator at the system parameter level.
- User should have the facility to schedule 3 kinds of events:

  a) Single day events: Events that start and end on the same day

  b) Continuous day events: Events that last for more than a day continuously. E.g. a 4 day event that starts on Monday and ends on Thursday

  c) Multiple day events: An Event that spans more than a day but not continuous e.g. a 3 day event occurring on Thursday, Sunday and Monday. For such events there should be an option to enter multiple records OR an option to select multiple dates directly from the calendar

  All the date fields should have a calendar field to input the date. There will be a warning pop-up if the event date being planned coincides with another registered event.

- An event calendar should be provided for users to view all the registered events.
- User can select the stakeholders who should receive the event notification. All the possible stakeholders are defined in the “Planned event stakeholder” table (refer section 2.2.5.3).
- Once the event is set-up, the user can notify all the relevant stakeholders using the <NOTIFY> button. This will bring up a screen containing an email subject and message using the information already captured including any files uploaded.

The email/SMS/App notification templates will be defined at system level. The notification channels will be set by the system administrator (refer section 2.3.2.1 Notification Channels).

The event notification will go out to the stakeholders once it is approved by the moderator. The moderator can reject the event with "Reason for Rejection". The user can make the necessary changes and re-submit for approval.

There should be a notification with relevant information going out to the event initiators 3 days in advance, if any of their event dates coincide.

2.5 Dashboards & Reporting

This module should cover all the necessary information related to the incidents and planned events. These reports or dashboards need to satisfy the information requirements of all the Miral stakeholders.

2.5.1 Dashboards

Dashboards should provide intelligence on how the incident management workforce contributes to the organizational strategy and success.

- The Dashboards should work on both mobile devices and desktop.
- The data in Dashboard should be graphically represented in both Pie & Bar charts
- Dashboard should have drill down feature to individual graphs, charts or tables
- User should be able to view data he/she has access to; filtering on
    - Incident status
    - Location Category
    - Location Site
    - Incident Category
    - Incident Type
    - Severity levels
    - Owners
- Data underlying information should be displayed on mouse hover on graph bar/section
- Only users with dashboard privilege will have access to the dashboard module

- Drill-down feature to data (table) representation when user clicks on the selected graph bar/chart.
- Trend analysis chart for comparison monthly, quarterly or yearly
  - Incident status
  - Severity levels
  - Total incidents by severity levels
  - Total incidents by location
- Should have capability to extract/download as pdf or image file
- Performance graph on incident closure

2.5.2 Reports

The Report access privileges will be provided by the system administrator. Report module should have search functionality as well as option to extract/download to excel or pdf or word format. System administrator should have full access to all the reports.
Following are the reports to be included, but not limited to:

- Incidents along with related information that the user (Initiator) has reported
- All master data reports for system administrator
- Functional role assignment matrix reports (refer section 2.2.6)
- Incidents along with related information for the Incident Owners; can be filtered by status, severity, location
- Incidents along with related information for the Recipients; can be filtered by status, severity, location
- SIMT group may not require report access as they will use the dashboard for real-time information. However the system administrator can provide access on a need to need basis.
- No. of duplicate Incidents created with relevant information
- Root Cause report – Closed Incident information filtered/grouped by location, severity with root cause information.
- Incident closure performance reports
- Planned events related reports

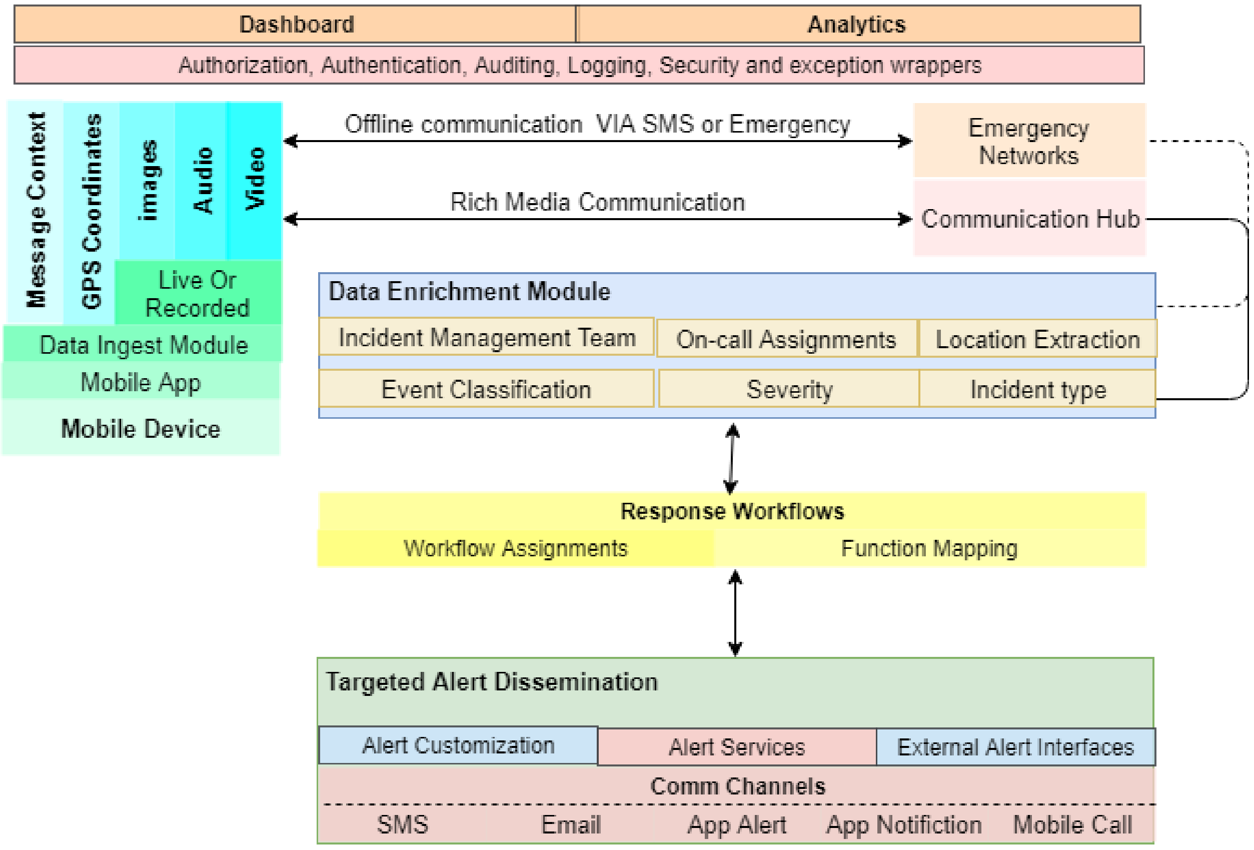
3 Interface Requirements

The ICM app should have the capability to support integrations with relevant service providers for SMS, email, chat/messaging, GPS, camera and microphone. Backend systems shall be integrated to reporting, document generation, databases, and external systems like ERP if applicable.

3.1 Functional Architecture

Below diagram depicts the functional architecture of the ICM App. The App will be hosted in the cloud and will be accessed via mobile app and web application as well.

The System usage by Web application is critical for the System administrator and also for Strategic management team to view Reports and Dashboards.



The notifications can be sent using below communication channels:

- SMS
- Email
- Mobile APP push notification
- Auto Phone call with pre-defined / pre-recorded voice message

3rd party integrations are:

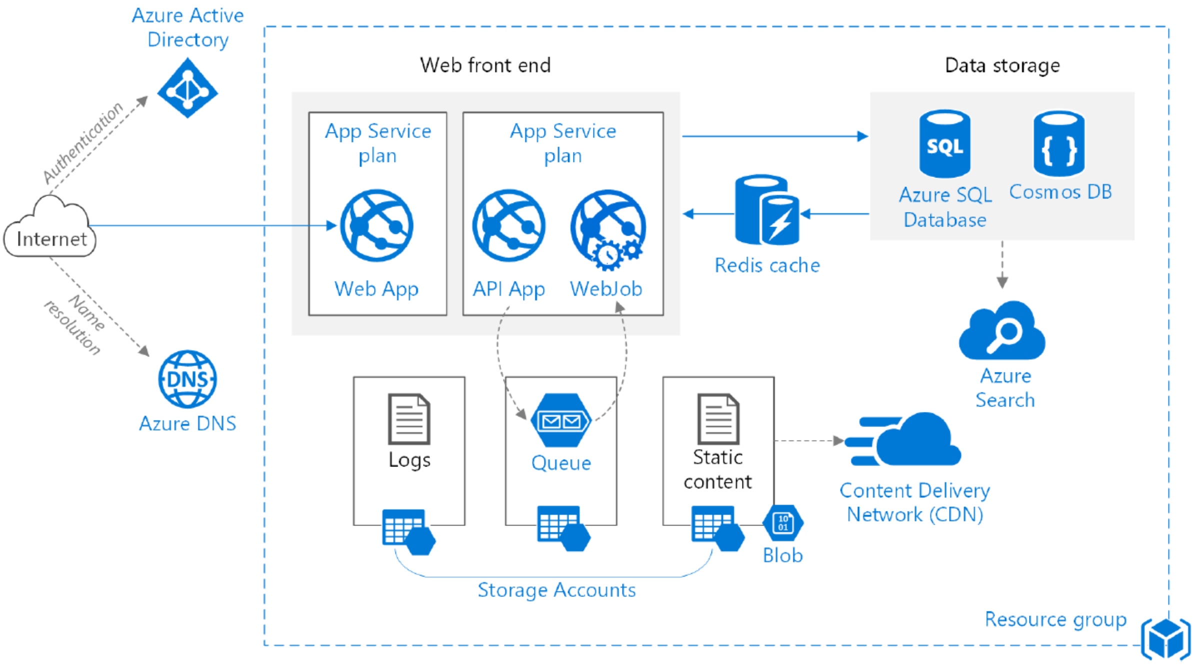
- Mobile GPS (To identify the location)
- Mobile camera (To capture video or photo that will be linked with the incident)
- Mobile Microphone (To record voice note that will be linked with the incident)
- Mobile Chat room

The ICM App will communicate with the server using API whenever internet is available.

If there is no internet access, the app will send SMS automatically using the mobile SIM card to the call center server. Once call center receives the SMS (Pre-defined code), it will call the regular Application server's API to create the incident on behalf of the Mobile APP.

3.2 Technical Architecture

Following architecture is based on the Microsoft Azure Platform for reference purposes only.



Resource group: A resource group is a logical container for Azure resources.

Web app and API app: A typical modern application might include both a website and one or more RESTful web APIs. A web API might be consumed by browser clients through AJAX, by native client applications, or by server-side applications. For considerations on designing web APIs

WebJob: Use WebJobs to run long-running tasks in the background. WebJobs can run on a schedule, continuously, or in response to a trigger, such as putting a message on a queue. A WebJob runs as a background process in the context of an App Service app.

Queue: In the architecture shown here, the application queues background tasks by putting a message onto a Queue storage queue. The message triggers a function in the WebJob. Alternatively, you can use Service Bus queues.

Cache: Store semi-static data in Redis Cache.

4 Appendices

4.1 Miral Information Sheet

Miral App Info-V5.xlsx

We look forward to hearing from you soon and hope that you will give us the privilege to work with you in meeting your business goals. Thank you.

Thank You