1. RedR Australia Incident Response Handbook

Acronyms

CANADA	Control, Assess, Notify, Act, Document, Audit
CEO	Chief Executive Officer
DD	Duty Director
DO	Duty Officer
DFAT	Department of Foreign Affairs and Trade
HotH	House on the Hill
IR	Incident Responder
IRM	Incident Response Manager
IRT	Incident Response Team
RMT	Regional Management Team
UNDSS	United Nations Department of Safety and Security

2. Foreword

This Handbook outlines in writing **what** should be done when an incident occurs, **when** and by **who**. Formulated from a number of sources including the 2020 version of the same document, it comprises recognised actions, procedures and checklist that shall be used in the event of an incident arising.

While the instructions in this manual are detailed, they are not necessarily comprehensive for each emergency that may arise. As such, any Incident Response Team (**IRT**) that has been formed may/can adapt the guidelines to suit the situation. Furthermore, the Incident Response Handbook should be seen as a 'living' document to be re-evaluated after the resolution of a given crisis; as such it should be subject to future change.

All staff (new or existing) should read the Incident Response Handbook to gain the basic knowledge of steps to take during an incident. Annual training will be conducted on use of the Incident Response Handbook. This said, it is not deemed necessary for staff to know the contents verbatim; rather a copy should be available and consulted by any Incident Responder (**IR**), Incident Response Manager (**IRM**) or IRT as required.

This Incident Response Handbook is separate to the RedR Crisis Management Plan. It is recognised that it may not be initially obvious that an incident constitutes a crisis, and so this Incident Response Handbook may be the guideline for the response until the adoption of the measures in the Crisis Management Plan are utilised. For critical incidents, the Crisis Management Plan should be consulted.

3. Definitions

Crisis	An event, or series of events, either sudden or slow burning, that critically threatens RedR's people, assets, operations, earnings, reputation, brand and / or strategic viability.
Critical incident	Any incident that critically threatens RedR's people, assets, operations, earnings, reputation, brand and / or strategic viability.
Incident	Any unplanned event resulting in injury, ill health, damage or other loss [adapted from AZ/NZS 4801]. n.b. this could include damage to organisational reputation.
Gap Guardian	RedR's smartphone monitoring application.

4. How to use the Incident Response Handbook

4.1 The 'CANADA' protocol applies to the management of incident reporting and response for RedR Australia. It applies to all RedR Australia personnel. All incident responses are to be managed individually, following the six step CANADA incident response process:

a) **C**ontrol
b) **A**ssess
c) **N**otify
d) **A**ct
e) **D**ocument
f) **A**udit

4.2 Any situation can utilise the CANADA protocol in the early stages of a response. If the Incident is deemed to become a crisis, then the Crisis Management Plan is to be consulted. The Crisis Management Plan contains detailed considerations for a range of crises.

5. C.A.N.A.D.A.

5.1 **Control.** All personnel at RedR Australia may be called upon to field a phone call from a colleague or deployee who is facing a pressurised and/or potentially hazardous situation. It is most likely that the Duty Officer (DO) will field this phone call. In order to effectively triage an incident and initiate an appropriate response, it is first vital to record accurately what has taken place. Doing so may require proactive control of any individual not relaying information in a logical or considered fashion. The below points may be of some assistance in guiding a colleague or deployee through the information you require of them:

- **WHO** is calling? How are they contacting you? How can you contact them if the call is dropped?
- **WHERE** are they? Obtain a country and locality at least (alternatively they could check in using Field Connect if available). Are they safe in their immediate environment? If not, are they able to move to a safer environment before continuing the call?

- **WHAT** has happened? The account should be detailed enough to understand the events leading up to the incident.
- **WHEN** did the incident take place? Confirm and record the time zone.
- **ACTIONS** required. What have they done/are they planning on doing next? What assistance do they require? Do not assume that the person contacting you for help has not already formulated a plan.
- **NEXT** contact. Set a time to call them back and a means of doing so; ensure this is recorded and passed on. Are there any deadlines that you need to be aware of (e.g., a time they are moving on to a different location or a threat may return)?

You should not shy away from pausing and/or recapping elements of the call, in order to control the pace of the conversation and ensure you are recording details accurately. In particular any contact and/or location details should be checked back to ensure accuracy.

5.2 **Assess**. In order to ensure that a given incident is dealt with in the appropriate manner, it is necessary to apply a logical process to determine its severity. This is sometimes known as 'triaging' in the medical field, a term which is equally applicable in the context of incident response. RedR Australia utilises a numeric scale for the triage of incident severity (see Annex A).

Critical incidents

Depending on the circumstances, an incident may be deemed as 'critical' when it critically threatens RedR's people, assets, operations, earnings, reputation, brand and / or strategic viability. This will formally be a crisis and escalation to the Crisis Management Plan if appropriate. If in doubt, the Head of Risk, Safety and Security should be contacted during working hours, or the Duty Director should be contacted outside of normal working hours, to assess whether the incident is critical.

Critical incidents will generally be a Level 4 or Level 5 on the afore-mentioned scale. Examples of critical incidents (all of which are reportable) include, but are not limited to:

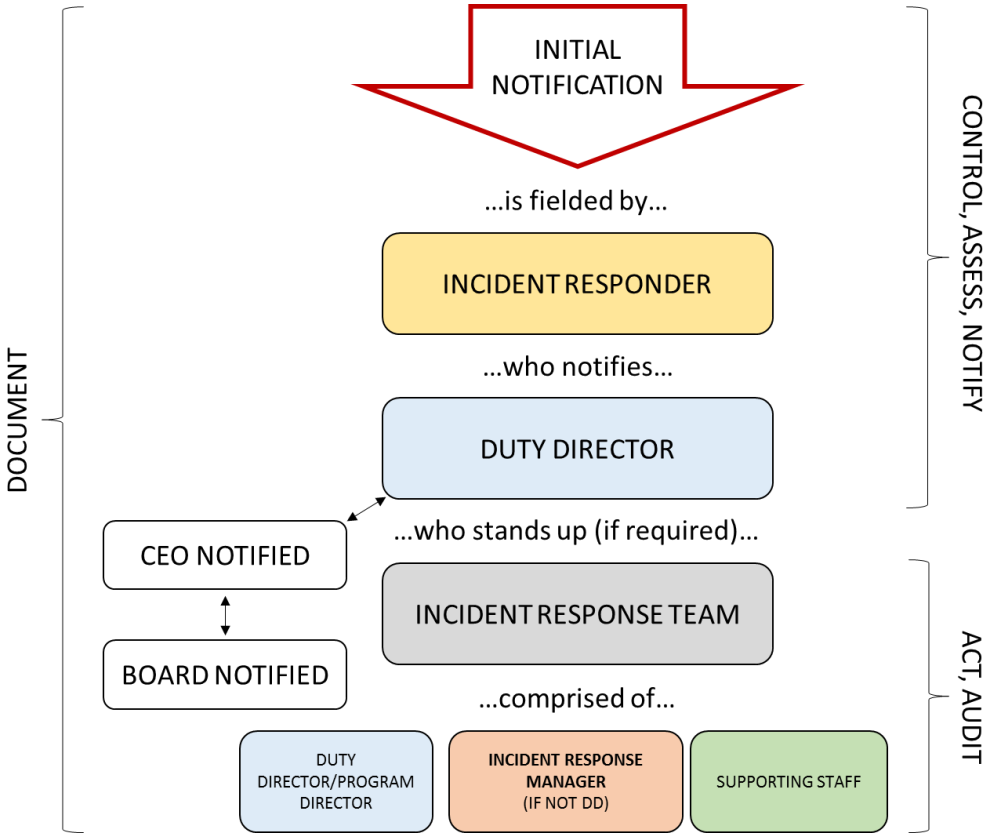
- Health or medical emergency, whether requiring admission to hospital or not (e.g. serious illness or injury (physical or psychological), electrical shock/injury, infectious disease, substance overdose);
- An assault or safety incident (e.g. threats of violence, sexual assault, physical attack);
- Personnel or deployees who are uncontactable, whose whereabouts or location is unknown and for whom there is concern for their safety;
- Natural or environmental disaster which impacts or has the real potential to impact RedR Australia personnel or operations;
- Evacuation or relocation of personnel due to a safety and/or security incident (e.g. 'stalking');
- RedR Australia or host organisation (where RedR personnel or deployees may be affected) building or facility fire, explosion, chemical, radiation or biological hazard;
- Theft, loss or other compromise of sensitive documents or other assets;
- Breach of Child Protection Policy;
- Suspicion of, or actual fraud and/or corruption;
- Hostage or kidnapping situation;
- Civil unrest or riots which impact or have the real potential to impact RedR Australia personnel, deployees or operations;
- Death (including death of a dependant), whether by natural causes, accident, suicide, result of an injury/illness or murder;
- Threatened or actual legal proceedings.

5.3 **Notify**. The person who first identifies and records an incident or situation (critical or non-critical) is the IR. This individual has an obligation to ensure that it is immediately brought to the attention of their line manager, and/or an identified IRM. A full explanation of the key roles within the IRT can be found at Annex B.

Clear and streamlined communications are essential in responding to any incident; the first step in this process is ensuring that the key personnel are informed as quickly as possible so that the IR is supported, and subsequent actions can occur. These actions include ensuring that:

- Appropriate immediate action can be taken to address the situation;
- Senior management are made aware of the event (if appropriate); and
- Organisation and partner reporting obligations are met.

The below diagram demonstrates a simple communications flow following an incident.



Sample communications flow.

The first RedR Australia staff member involved in an incident automatically assumes the role of IR until otherwise instructed or relieved by a more senior member of their team or the IRM.

Members of the IRT should ensure they have ready access to the contact details of all other potential IRT members at all times. Staff contact details for RedR Australia can be found on the S: drive at S:\RedR Common\Contacts\.

The CEO will manage any communication with the Board as required.

5.4 **Act**. While the specific response and management will vary on a case-by-case basis, the following procedure provides the general structure that will apply to the majority of incidents.

5.4.1 **Appointment of the IRM, activation of the IRT**. Initially, the IRM is the first appropriate manager or team leader who is advised of an incident – they fill this role until they are replaced at the direction of a RedR Australia director. They will be responsible for the activation, assembly and management of the IRT and oversight of the response to the incident or situation. The IRM, in consultation with the DD, will decide the timing and frequency of IRT meetings.

5.4.2. **Composition of the IRT**. The role and responsibilities of each member of the core members of the IRT are defined in Annex B. The extent of involvement of each member of the IRT will depend on the nature of a particular incident.

The IRM, in consultation with the DD, will decide the composition of the IRT, recognising that the composition may change over the course of responding to an incident. The IRM, in consultation with the DD, will also determine which personnel are to be active IRT participants and who is to be simply 'kept informed'.

The IRT will include the following personnel:

Designated members:

- Incident Responder (whilst there are designated IRs in the organisation, in effect any individual who picks up an incident will initially become IR).
- Incident Response Manager.
- Duty Director (and other Directors as required to commit funds).
- Program Director (if not DD) and/or Head of Risk, Safety and Security.

Optional members:

- Communications officer.
- Welfare officer (external and internal – these may be separate roles).
- Child Protection Officer (mandatory for incidents involving a child under 18 years of age).
- Line managers of any personnel involved.

Depending on the circumstances and nature of the incident, other RedR Australia personnel may be appointed to the IRT to bring their expertise and skills to bear in assisting with dealing with the specific incident. Representatives of clients or external stakeholders may also be appointed for incidents which affect them.

The CEO is to be kept closely informed throughout. They, in turn, are responsible for updating the Board as appropriate.

5.4.3 **Considerations for incident management**. There are a range of factors to consider in preparation for/management of an incident:

Situation monitoring. Maintaining an awareness of developing situations that may change assessed threat and risk levels is very important. No one area within RedR

Australia can undertake this task alone. Certain designated positions have a vital role to play in monitoring information sources and conveying any relevant advice, and for the monitoring of the movements and welfare of personnel who might be affected by such changes. In most cases risk advice can be communicated in writing (e-mail, SMS), however, if an acknowledgement is not received in a suitable timeframe, other forms of communication must be used.

1. **Regional Management Teams (RMTs)**. RMTs have the obligation and responsibility to monitor local media, sources of local civil defence and emergency management advice and any other available risk management advisory resources concerning their sphere of operations. Where information is received, or a situation occurs which might impact on the safety and security of deployees or operations, the RMTs shall convey that advice in a timely manner to deployees (keeping the IMT informed in so doing) and the Head of Risk, Safety and Security.
2. **RedR Australia personnel**. All RedR Australia personnel have a responsibility to be attuned to local media and any other available risk management resources concerning the organisation's sphere of operations. Wherever there is awareness of a situation that may impact on the safety and security of RedR Australia personnel or operations, they shall convey that advice in a timely manner to their line manager and/or the Head of Risk, Safety and Security. If the former, the line manager will inform the Head of Risk, Safety and Security and/or the Program Director at the soonest opportunity. Line managers shall ensure that the welfare of RedR Australia personnel in their area of responsibility is constantly monitored and are advised of any developments that may impact on their safety, security or wellbeing.

Media and external communications. The authorised spokesperson for the organisation is the CEO or, if not available, a nominated proxy (to be approved at Director level).

Any external messaging and/or media engagement will require the approval of the CEO or their delegate. All requests for information are to be referred to the Communications Manager in the first instance.

If requested by the IRT, the Communications Manager will develop a Media Brief outlining the incident. The CEO or their delegate will sign off on the company position on the situation and confirm the spokesperson for the incident.

Privacy and confidentiality.

1. **Privacy considerations**. During high stress situations it is particularly difficult, but crucial, that the privacy of the individuals concerned is respected. This is governed by the 'need to know' principle – only share information that is required for the recipient to respond appropriately. This relates not only to anyone directly or indirectly involved in the IRT, but also any other personnel and/or external stakeholders who may become subject to privileged information in the course of a given incident.

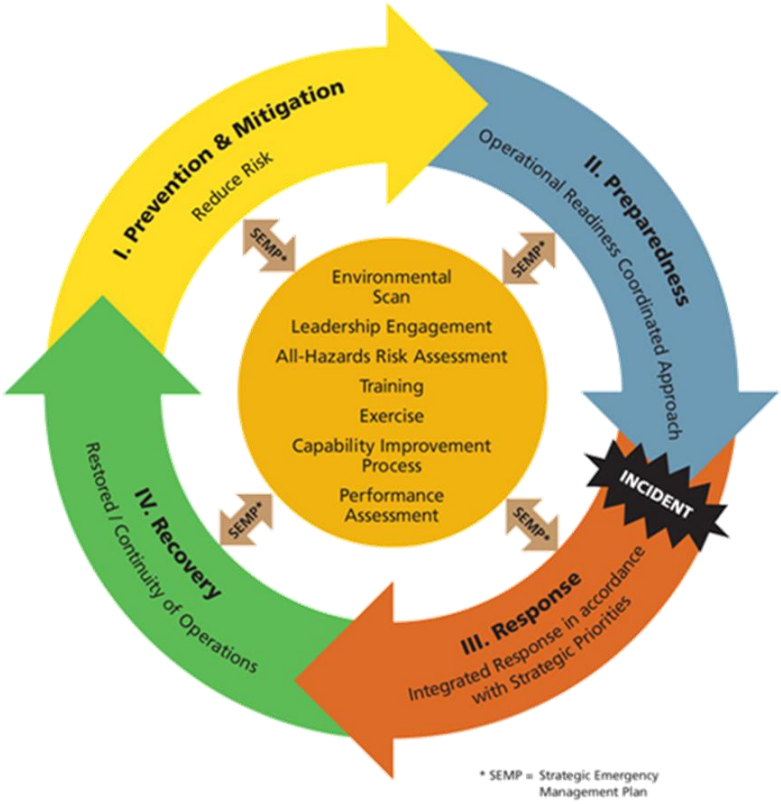
   Information sharing is to be in line with RedR Australia's Privacy Policy and more broadly with Australian Privacy Principles.

Sharing information with family members requires particular sensitivity. Regardless of the age of the personnel involved, they will generally be adults and must be treated with this in mind. If the person involved is able to communicate, it should be assumed that they will inform their family and friends. RedR Australia will not do this unless specifically requested to do so by the individual. If the person involved is unable to communicate and has indicated an emergency contact on their file, this is the person that should be communicated with.

2. **Confidentiality**. Confidentiality of the personal information of all parties involved in an incident is to be maintained at all times throughout the management and follow up of that incident. This includes ensuring that only required RedR Australia personnel are included in the incident response.

5.5 **Document**. All personnel involved in a given response share responsibility for ensuring that all actions are documented effectively. This may include incident reports using organisational templates, chronological summaries of actions, minutes and agreed actions of IRT meetings, Media Briefs and talking points, and any written communications to key external stakeholders. Conversations that precede key decision-making should also be recorded. The IRM bears overall responsibility for ensuring that all actions are documented effectively.

The IRM, in conjunction with the Head of Risk, Safety and Security, will ensure that an incident log on House on the Hill (HotH) is created at the earliest reasonable opportunity (generally when the incident transitions from the *Response* to the *Recovery* phase – see below). Creation of the log on HotH should only happen when rhythm of the incident response allows for its creation, as to not detract staffing power away from the actual response. The Head of Risk, Safety and Security has overall responsibility for ensuring that the log on HotH is an accurate version of events, with all recorded documentation attached to the incident log.



Incident Management Phases

5.6 **Audit**. Following the conclusion of the 'response' phase of an incident, a hot debrief will be held by the IRM immediately at the end of the situation involving all available participating members of the IRT.

The IRM is responsible for ensuring that all communications are recorded and a written record produced. This will include any lessons learned and an action plan for follow up. This will be included in the incident log as above.

At a later time and when all relevant information is available, a cold debrief will be conducted by the IRM in conjunction with the Head of Risk, Safety and Security, to evaluate the response to and management of the incident.

6. Roles and Responsibilities

All personnel.
All personnel, regardless of seniority or experience, should read the Incident Response Handbook to gain the basic knowledge of steps to take during an incident.

Head of Risk, Safety and Security
The HRS&S has the delegated responsibility for this Incident Response Handbook, its regular review (as a minimum annually) and ensuring its implementation at all levels. He/she also responsible for ensuring that all personnel are trained, at a minimum yearly, on the contents of this document.

7. Related Policies and Documents

Crisis Management Plan
Deployments Duty Phone Policy
Incident Reporting Policy
Privacy Policy
RedR Australia Risk Management Policy

8. Document Control

Document control	
Reviewed by:	Manager RSS (AA)
Approved by:	Director P&C
Review date:	June 2023
Next review:	June 2024
Distribution:	Internal only
Version number	3.0

Annex A – Risk Scoring

	Severity	Operational	Medical/Wellbeing	Financial	Reputational	Other
1	Insignificant	No or very limited disruption to field/work day.	Very minor medical/wellbeing incident self-managed or attended to by medical specialist and/or First Aider.	Net impact of less than 1% of turnover (organisational) or self-funded (individual).	No significant direct reputational impact.	*Risk Descriptors are not presented in an attempt to capture an exhaustive list of events with the potential to impact the organisation.* *Rather they offer examples of what incidents of the respective severity may look like in four key areas of organisational risk (**Operational**, **Medical/Wellbeing**, **Financial**, and **Reputational**) in order to promote a shared/ consistent understanding of the magnitude of each level.* *Risk Owners are then able to apply this more specifically to their area of responsibility/ expertise.*
2	Minor	Field day(s) disrupted as a result of administrative and/or bureaucratic issues.	Medical/wellbeing incident requiring brief attention by medical/wellbeing specialist.	Net impact of 1-2% of turnover.	Potential for adverse reputational impact internally or within sector.	
3	Moderate	Mutliple field days disrupted as a result of minor to moderate administrative issues.	Medical/wellbeing incident requiring out-patient admission (e.g. insect-borne disease, compassionate repat).	Net impact of 3-5% of turnover.	Adverse reputational impact at state/national level.	
4	Major	Multiple field days disrupted as a result of a serious (e.g. missing staff, illegal detention, relocation/ evacuation from conflict/disaster) event.	Life-altering (non-life threatening medical/wellbeing incident or event.	Net impact of 6-20% of turnover.	Major adverse reputational impact at international level.	
5	Catastrophic	Proximate threat to organsational integrity. Forced suspension or cessation of operations, and/or loss of a substantial part of the organisation.	One or more fatalities. Kidnapping or abduction. Proximate threat to life/long-term wellbeing.	Net impact of greater than 20% of annual turnover, or any time RedR's financial obligations threaten to exceed its capacity to fulfil them.	Potential for irreparable/ unrecoverable reputational damage.	
-NM	Near Miss	Lessons can be learnt from causal factors when something almost goes wrong, not only when it does. The suffix 'NM' (e.g. 3NM) denotes a near miss; this signifies an incident where only a fortunate break in the chain of events leading up to the occurrence prevents harm from eventuating.				

Annex B – Incident Response Team (IRT) Key Roles

All personnel will ensure that any incident response is managed with the following order of priorities:

1. Protect human life
2. Minimise trauma
3. Protect reputation (organisation, host agency and individual)
4. Protect information
5. Protect equipment and other physical assets

Any personnel involved in the response to an incident will ensure that privacy and confidentiality considerations are considered at all stages of the incident response.

Incident Responder (IR). This is the first person to whom an incident is reported and who takes initial action to **C**ontrol and **A**ssess the situation, before notifying the relevant staff. This will usually be the Duty Officer (DO), or a member of the Training Team, however, anybody who finds they have answered the phone to an emergency call will assumed this position and must remain 'in role' until they are replaced by either their line manager, an IRM or a fellow team member. Their primary responsibilities are to undertake any reasonable action to ensure the immediate safety and well-being of any personnel or deployees involved, and to inform senior management of the situation.

Incident Response Manager (IRM). Initially, the IRM is the first appropriate manager or team leader who is advised of an incident – they fill this role until they are replaced at the direction of a RedR Australia director. The IRM will usually be either the Head of Risk, Safety and Security, or Program Director, however any suitable senior staff member may fill this role if available.

The IRM is a pivotal role in the response to any incident. In a time-critical situation they have the delegated authority to make any reasonable decisions to ensure the safety and security of RedR Australia personnel, deployees and/or assets.

The IRM activates, assembles and manages the Incident Response Team (IRT) to respond to the incident. In consultation with the Duty Director (DD), the IRM will determine the membership and meeting frequency of the IRT, including which personnel should be added to broader communications to be kept informed.

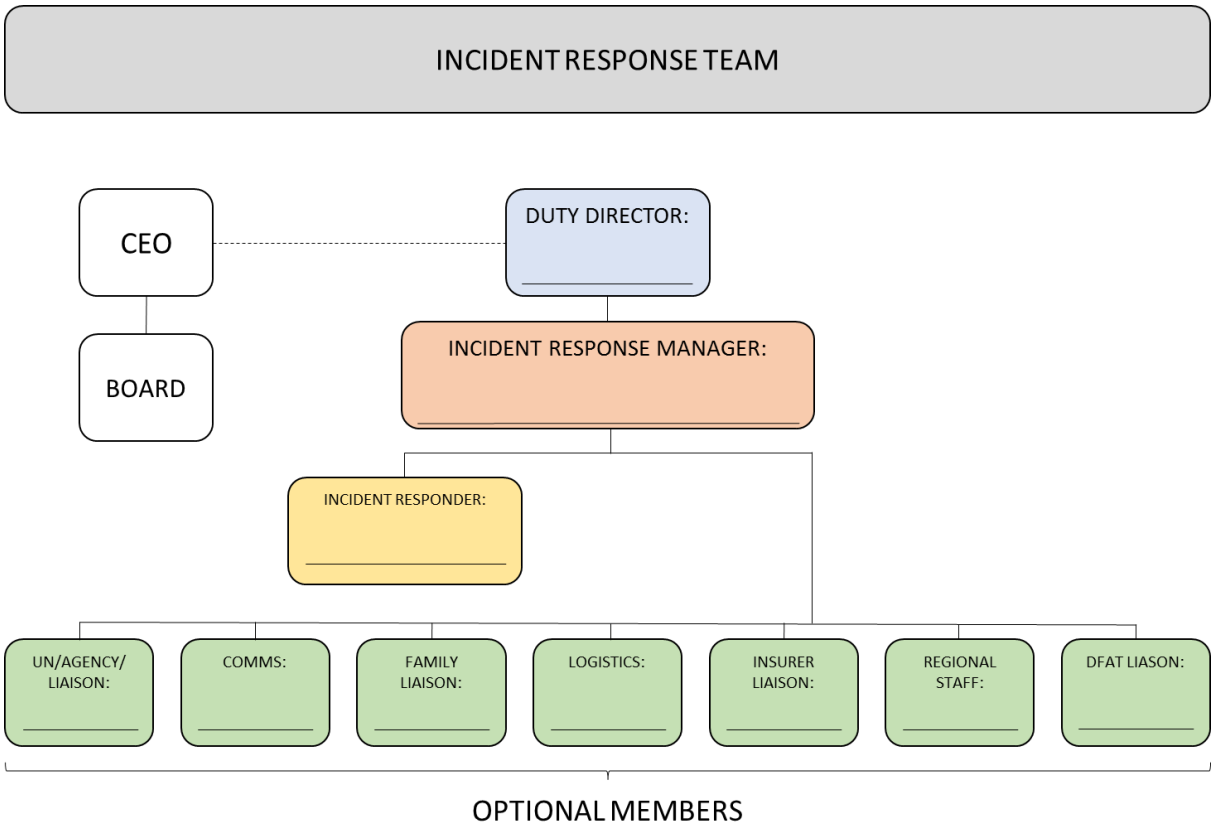
The IRM will pro-actively ensure that communications channels are streamlined, and messaging is clear and consistent. This includes designating specific personnel as focal points as required. The IRM is responsible for ensuring all reporting is completed and lessons learned are documented according to approved processes.

Incident Response Team (IRT). Activated by the IRM, the IRT draws upon RedR Australia's overall expertise and resources to control and manage the organisational response to, and recovery from, an incident. Specific roles within the IRT can be tailored to the specific requirements of a given operational response. These may include (though are not limited to):

- UNDSS Liaison Officer (note that this will, dependant on the incident, likely be the IRM).
- Communications Officer.
- Family Liaison Officer.
- Logistics Officer (necessary flights, accommodation bookings etc, as required).
- Insurance Liaison Officer (including liaison with ISOS as required).
- DFAT Liaison Officer.
- Host Agency Liaison Officer.

The IRT is not a Standing Committee but activated as required by the appointed IRM and staffed by required personnel to manage a specific incident. Note that some roles may be filled by the same individual (e.g., the Head of Risk, Safety and Security is likely to be UNDSS Liaison Officer and Insurance Liaison Officer, whilst the DO may be the Logistics Officer and Host Agency Liaison Officer).

Duty Director (DD). The DD is initially responsible for authorising the IRM to form the IRT; this includes changing the IRM if required. From there, the DD's primary responsibility is providing corporate strategic oversight to the operational focus of the IRT. The DD will keep the Chief Executive Officer (CEO – note the CEO may also assume the role of DD) and other senior stakeholders informed as required.



Sample IRT structure.