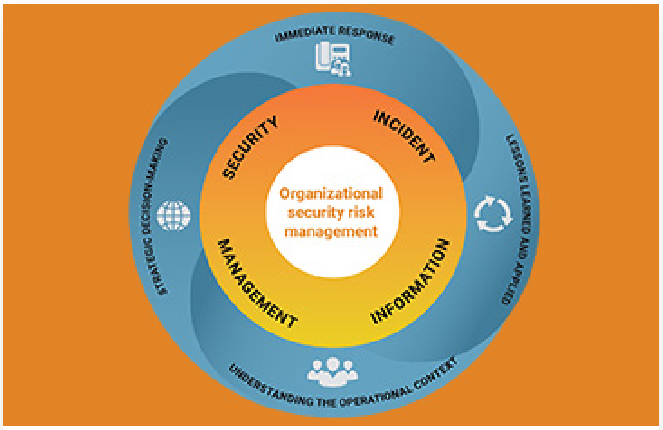
Cornerstone ondemand | foundation

Insecurity Insight
Data on People in Danger

Safety and Security Incident Information Management

READY to go
Mobile Guide

Learn how organizations can effectively manage safety and security incident information.


IMMEDIATE RESPONSE
LESSONS LEARNED AND APPLIED
UNDERSTANDING THE OPERATIONAL CONTEXT
STRATEGIC DECISION-MAKING
SECURITY
INCIDENT
INFORMATION
MANAGEMENT
Organizational security risk management

What is Safety and Security Incident Information Management?

Why Should Organizations Manage Incident Information?

There are several reasons why it is critical for organizations to manage safety and security incident information.

- Reduce the impact of an incident on the organization and its employees.
- Improve an organization's ability to prevent future incidents from happening.
- Improve an organization's ability to prepare for and mitigate the impact of future incidents.
- Allow an organization to meet its duty of care obligations by improving the safety and security of its employees and others.
- Support good decision-making for programs, safety and security, human resources, finance, and advocacy.
- Provide information that can help improve an organization's access to communities in need.

What is an Incident?

Organizations need to first clearly define an incident in order to effectively manage incident information.

Definition

An incident can be any event(s) in which:

- Employee safety or security is compromised.
- Any dependent or other third party is injured or harmed during organizational activities.
- Organizational property or assets are stolen, damaged, or put at risk.
- There is interference with programing and operations.
- The organization’s independent work is compromised.
- The organization’s reputation is at risk or damaged.

Internal vs External

An incident can affect an organization and its employees directly, or anyone external to the organization.

Severity

Incidents can be critical and non-critical:

- A **critical incident** requires an organization to respond using additional measures and resources beyond normal organizational procedures (examples: kidnapping, death).
- A **non-critical incident** can be responded to using normal organizational procedures (example: road traffic accident with no injury or severe damage).

The severity of an incident is often measured by the level of impact the event had on the organization.

Impact

An incident can impact:

- Employees' safety, security, and wellbeing
- An organization's ability to:
  - Conduct operations
  - Deliver aid and services
  - Achieve its objectives

Accident vs Intentional Act

An incident can be an accident or an intentional act:

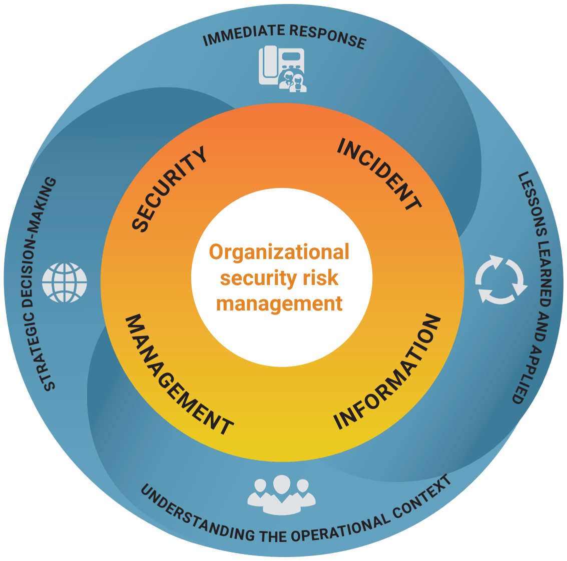
- **Safety incident** = an accident
- **Security incident** = an event that was caused intentionally by a third party to inflict harm on an organization or some other actor, or negatively impact the intended aid activity. Intentional acts that did not target the organization directly but still affected it and its employees also fall under security incidents.

Classification

Organizations should use a robust classification system that clearly defines different types of incidents.

What is Safety and Security Incident Information Management?

Safety and security incident information management (SIIM) is the process of collecting and using information related to safety and security incidents. The main objective of SIIM is to improve an organization's safety, security, and overall ability to access communities and deliver aid. This is achieved by ensuring that the right information from incidents is used to inform decision-making at all levels within the organization. All SIIM-related activities should be people-centered and should consider the diversity and diverse needs of individuals affected by incidents.


IMMEDIATE RESPONSE
LESSONS LEARNED AND APPLIED
UNDERSTANDING THE OPERATIONAL CONTEXT
STRATEGIC DECISION-MAKING
SECURITY
INCIDENT
INFORMATION
MANAGEMENT
Organizational security risk management

Immediate Response

Reporting an incident in order to immediately respond and assist the individuals affected by the incident.

Lessons Learned and Applied

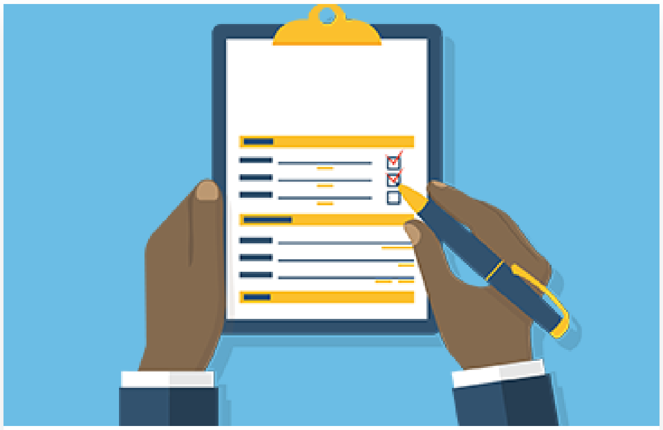
Using information collected to implement lessons learned after an incident to support organizations in the **prevention** of and **preparedness** for future incidents.

Understanding the Operational Context

Using internal and external incident data to identify trends and gain a better understanding of the context to inform operational decisions.

Strategic Decision-making

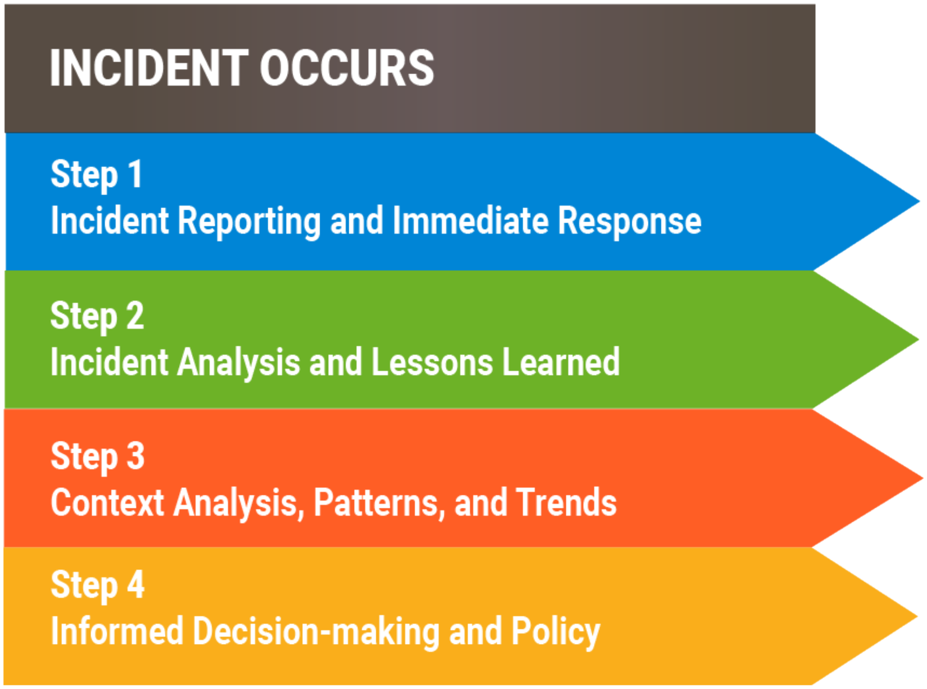
Using incident data to inform appropriate decision-making for organizational activities related to safety and security, programs, finance, human resources, and advocacy.



Managing Incident Information

Managing Incident Information

Managing safety and security incident information is a cycle of continuous learning. The response and analysis of one incident should inform the response and analysis of future incidents. There are key steps organizations and employees should follow when managing incident information. The order of the steps and the person responsible for each activity may vary according to the situation and the organization. It is critical for organizations to provide all employees with clear, specific guidelines and procedures to follow when managing safety and security incident information.



INCIDENT OCCURS

Step 1
Incident Reporting and Immediate Response

Step 2
Incident Analysis and Lessons Learned

Step 3
Context Analysis, Patterns, and Trends

Step 4
Informed Decision-making and Policy

Step 1: Incident Reporting and Immediate Response

Report the Incident

Organizations should have a framework in place to:

- Report severe incidents immediately following organizational reporting procedures (by phone or radio).
- Provide essential information that is needed for the immediate response:
  - ✓ Who is involved
  - ✓ What happened
  - ✓ Where the incident occurred
  - ✓ When the incident occurred
  - ✓ What has been done about the incident
  - ✓ What help is needed
- Provide updates for ongoing incidents as needed.

Tips for Immediate Reporting

- Focus on the facts. Avoid making judgments or focusing on why the incident happened.
- Keep incident information confidential.
- Follow specific reporting mechanisms for sensitive cases such as sexual assault (if applicable).

Respond to the Incident

After receiving the initial incident report, organizations should:

- Ensure that individuals affected by the incident receive the assistance and support needed.
- Ensure that the response timeframe matches the severity and impact of the incident.
- Prioritize assistance to those affected and protect them and others from further harm.
- Consider any personal circumstances (ethnicity, personal status, gender identity) which may require a customized response approach.

Complete Formal Incident Report

After the initial response to an incident occurs, organizations should ensure that a formal incident report is completed and stored in a reporting system.

The report may require gathering additional information about the incident.

Organizations should follow these reporting procedures:

- Use a simple incident reporting system to collect incident information.
- Provide staff with easy-to-use templates and training to reduce underreporting.
- Train staff on how to report incidents directly in the system or assign a designated staff member to enter reports into the system.
- Explain clearly to staff about what happens to incident information following a report.
- Ensure confidentiality to protect those affected by the incident.

Tips for Formal Incident Reports

- Comply with organizational procedures.
- Depending on the severity of the incident, consider not punishing staff if they admit to having broken organizational rules.
- Include personal information (ethnicity, status, gender identity) to ensure that the incident response and analysis consider the diversity of staff. Collect this information only if the organization can ensure it is kept confidential and does not place affected staff members at risk of further harm.
- Share reports only with the appropriate colleagues while maintaining confidentiality.

Step 2: Incident Analysis and Lessons Learned

Follow Up

Organizations should follow up on an incident report.

Responsible staff members should:

- Obtain any additional information needed for analysis that goes beyond the initial incident report.
- Conduct a factual de-brief with the individual(s) affected by the incident to learn from what occurred.
- Find the right balance between rewarding staff for reporting failures and enforcing disciplinary procedures.
- Consider the individual needs of staff members involved in the incident de-brief and ensure the process accommodates their needs, including any language or access constraints to psychological or medical support services.

Tips for an Incident De-brief

- Focus on the facts.
- Use the de-brief to learn from the incident for the whole organization.
- Avoid turning a factual de-brief into an emotional de-brief.
- Avoid finding fault with those involved in the incident.

Analyze the Incident

The appropriate staff member analyzes the information collected in the formal incident report to understand why the incident occurred. Understanding the motivation behind incidents, whether it was an attack by others or caused by an employee not following procedures, is key to future prevention and preparedness.

Organizations should consider the following when analyzing an incident:

- Consider the impact and causes of the incident.
- Assess whether similar incidents have occurred in the past.
- Assess whether organizational procedures were followed.
- Analyze the effectiveness of the incident management response.
- Consider any personal characteristics of the individuals involved in the incident (gender, religion, ethnicity) that could be a factor or motive for the incident.

Implement Lessons Learned

After the analysis of the incident, senior management and decision-makers in the organization should:

- Identify and implement new or improved actions to prevent and prepare for similar incidents in the future.
- Task the development of an action plan to ensure that recommended actions are implemented.

Step 3: Context Analysis, Patterns, and Trends

Record Incidents

Organizations should record incidents in an incident database. If staff members are required to file their own incident reports directly into a database, then organizations must provide clear guidelines and training to ensure consistency in reporting.

An **incident database**:

- Is a software system or spreadsheet that is specifically set up for SIIM.
- Uses technology that matches the organization's size and needs.
- Keeps logged information confidential to protect the privacy of affected individuals.
- Has defined access credentials of who can view the information and for what purposes.
- Follows consistent reporting procedures.
- Allows for the analysis of multiple incidents.

Access External Incident Information

Organizations can benefit from comparing their incident trends to those from similar organizations. External incident information can be used to support analysis. This information can be obtained from open sources or through subscriptions from commercial providers or incident data sharing agreements.

Organizations should consider the following when analyzing external incident information:

- Consider the **reliability of the source**: Does the source have a history of authenticity, trustworthiness, and competence?
- Consider the **validity of the information**: Is the information consistent with other relevant data and confirmed by independent sources?

Share Incident Information Externally

Organizations can gain further insight from external incident data by agreeing to cross share key trend data with other organizations in an anonymized format, either directly through forums or pooled databases. However, differences in incident categories can make sharing and analyzing shared data more challenging.

Examples of external incident data sharing resources:

- Aid in Danger by Insecurity Insight
- Aid Worker Security Database (AWSD)
- International NGO Safety Organisation (INSO)
- Saving Lives Together Framework

Analyze Multiple Incident Data

Analyzing multiple internal and external incidents can help organizations better understand the operational context by identifying patterns and trends as well as subtle changes in the operating environment that might have otherwise gone unnoticed. Context analysis can support access and implementation of an acceptance strategy.

Multiple incident data analysis:

- Is a structured approach to analyze multiple (internal and external) incidents.
- Compares an organization's trend data with external safety and security incident data (from public sources or shared by other organizations).
- Compares an organization's incidents with data from similar organizations.
- Accounts for how underreporting can affect data.

Step 4: Informed Decision-making and Policy

Share Incident Information Internally

Organizations gain insight from sharing and using incident data internally across departments and teams. When sharing data, organizations should **anonymize data** by removing personally identifiable information, and **main confidentiality** to protect the privacy of individuals affected by incidents. Incident data supports informed decision-making across all organizational departments, including programs, finance, human resources, and advocacy.

Incident data can be used for:

- Context analysis
- Development of action plans
- Access and program planning
- Funding proposals
- Risk assessments
- Job descriptions in specific areas

Inform Operational Decisions

Robust incident data collection and analysis allows senior management to make operational decisions at the field, country, regional, and international levels. These decisions may include:

- Where and how to operate, including how to negotiate access
- What security risk management measures to implement and prioritize
- Which activities and resources to finance

Tips for Using Information Analysis for Operational Decision-making

- Analyze the real or potential impact of the incident information.
- Identify departments or colleagues that would be impacted by or benefit from this information.
- Define the mechanism and templates to share information across multiple departments that protect the privacy of affected individuals.
- Share anonymized incident data with follow-up recommendations across different departments.

Inform Organizational Policy

Robust incident data collection and analysis can allow senior management to make strategic and policy-level decisions. These decisions may include:

- In which countries to operate
- Security strategies to prioritize (acceptance, protection, or deterrence)
- Ways to communicate about programs to beneficiaries, donors, the public, and other stakeholders
- When to use incident information for advocacy purposes

Incident data can evidence:

- Violence against aid workers
- Disruption of aid
- Humanitarian access restrictions
- Violence against or challenges faced by local populations

This information can lead to policy activities related to:

- Improving humanitarian access
- The protection of aid workers
- Adherence to international humanitarian law
- Raising awareness of operational constraints and security issues with donors, stakeholders, and other actors
- Seeking justice for victims of breaches of criminal, humanitarian, or human rights law

Individuals or specific cases should never be exposed for the purpose of making a political point. Collective data reduces this risk through anonymity in numbers.

Inform Staff of Decisions Made

Senior managers should communicate to staff how the organization has learned from incidents and made decisions based on the data gathered. This can help address underreporting of incidents.

This will enable staff members to:

- Improve their understanding of incident information management.
- Improve their trust in the incident reporting process.
- Implement lessons learned from incidents.

Classification of Incidents

Classification of Incidents

Organizations use categories to describe different types of incidents that can happen to the organization, employees, communities they work with, and other bystanders. Organizations are encouraged to use standard definitions to facilitate analysis, data exchange, and cross-organization comparisons. Below is a list of suggested definitions. Organizations do not have to use all categories but should choose those that are most appropriate for the context in which they work.

Accident or Illness

Any accident involving employees or organizational property and other incidents that were not intentional (examples: accidents, sudden illness).

Accidental Death

Any unintentional death that cannot be attributed to natural causes. Causes of accidental death may include vehicle accidents or complications from injuries.

Illness

Any serious illness of an employee.

Other Accident

A random incident that results in harm to employees and/or damage to the organization’s property.

Natural Death

Any death that can be attributed to a natural cause (heart attack, illness, stroke).

Natural Fire

Any fire damaging the property or endangering employees of natural or unintentional cause. This may include wildfires or accidental fires (electrical fires, gas leaks).

Suicide

TThe voluntary and intentional death of an employee who has taken his/her own life.

Aid Delivery Activities

Any incident that took place at a project site or during aid distribution, including looting of aid supplies, intimidation, harassment, or threatening behavior towards staff members during aid delivery. These Incidents cover events that occurred in the context of conflict war or crime.

Armed Activity

Actions involving weapons by one state, non-state, or organized armed entities.

Beneficiary Affected

Threats and/or violence was used against a beneficiary.

Face-to-Face Harassment

Incidents in which an employee is directly harassed by a person or group of people (example: harassment over the organization's program activities or programs).

Face-to-Face Intimidation

Incidents in which an employee is directly intimidated by a person or group of people (example: an employee felt intimidated by armed actors patrolling near a food distribution).

Face-to-Face Threats

Incidents in which an employee is directly threatened by a person or group of people; should include some form of consequence for non-compliance (example: a threat of retaliation for not including someone in an organizational activity).

Looting

Theft during unrest, violence, riots, or other upheavals.

Crime

Criminally motivated incidents that affect employees, their property, or the organization's property.

Armed Robbery

A robbery at gunpoint or when the perpetrators carried firearms that affected employees or property.

Arson

Any fire damaging property or endangering employees that is caused intentionally. Arson includes, but is not limited to, the use of incendiary devices, the intentional sabotage of electrical systems or gas lines/tanks, and the use of an accelerant to destroy the property.

Blackmail

Threats, extortion, or the manipulation of someone to compel them to do something; includes obtaining something, especially money, through force or threats.

Break-in

The act of unlawfully gaining entrance into an aid organization's premises or vehicles with the intention of theft.

Burglary

A break-in to a staff residence, usually with the intention of theft.

Classification of burglary vs robbery:

- **Burglary** = when occupants are not present or unaware during the incident (while sleeping)
- **Robbery/Armed Robbery** = when occupants are present and/or directly threatened during the incident

Carjacking/Hijacking

Any incident in which a vehicle that is owned by the organization or is being used by an employee(s), as a driver/passenger, is forcibly seized.

Cyber Attack

Deliberate exploitation of computer systems or technology-dependent enterprises and networks resulting in disruptive consequences that can compromise data and lead to cybercrimes.

Extortion

The practice of obtaining something, especially money, through force or threats, from an employee(s).

Fraud

Wrongful or criminal deception intended to result in financial or personal gain.

Intrusion

Wrongful or unauthorized entry into an organization's premises, vehicles, or staff residences by criminals or civilians (but not state authorities).

Piracy

Attacking and robbing ships at sea or boats on rivers.

Robbery

Incidents in which:

- The perpetrator was not armed
- The employee(s) was present during the incident and fully aware of being robbed and assets were taken

Damage to Property

Any damage or harm, in excess of a predefined amount, that is done to the organization's property either unintentionally (natural disasters, accidents) or intentionally (riots that cause property damage).

Theft of Property

Any situation in which personal property is stolen from an employee or location without the victim being aware of items taken.

Theft of the Organization's Property

Any situation in which property is stolen from an organization without an employee observing the act.

Vandalism

Deliberate destruction of/damage to organizational or staff property.

Conflict and War

Incidents that occur in the context of armed conflicts or situations of severe political volatility that directly or indirectly impact an organization, staff, or operations both local and international in a private or professional capacity. Incidents may or may not directly affect the organization, its staff, or infrastructure.

Armed Activity

Actions involving weapons by one state, non-state, or organized armed entities.

Crossfire

Any situation in which an employee(s) or organizational property is caught in an attack or firefight between two or more armed parties. In this situation, the involved employees and properties are not the target of the attack.

Coup

Coup, mutiny, and other rebellion by any armed force. A coup is defined as an attempt (generally armed) to remove and replace a government. Whether successful or not, violent or not, an attempted coup may be politically destabilizing.

Shooting

Deliberate shooting of people other than organizational staff.

Unexploded Ordnance (UXO) Discovery

Refers to the discovery of unexploded ordinance, explosive remnants of war that did not explode when they were deployed and still pose a risk of detonation.

Killed, Injured, or Kidnapped (KIK)

Any incident that results in an employee being killed, injured, or kidnapped. These are usually considered critical Incidents.

Abduction/Hijacking/Hostage-taking/Kidnapping

Any incident in which employees are forcibly seized. This incident may or may not involve a ransom demand. Employee(s) killed while in captivity are included as ‘kidnapped’ and not ‘killed’.

Beaten

Incident in which an employee was assaulted by someone using their fists, feet, or other body parts, or by objects (sticks or blunt objects).

Killed

Any death which has been intentionally caused (shooting, physical attack, poisoning). Intentional deaths do not include suicides. Employee(s) killed while in captivity are included as ‘kidnapped’ and not ‘killed’.

Missing

An incident in which an employee has disappeared or went missing.

The distinction between missing and kidnapping include:

- **The actor**: non-state actors tend to kidnap while state actors tend to ‘disappear’ people who are then referred to as ‘missing’.
- **How the perpetrator communicates about the employee that has been taken:** kidnappers tend to make demands (ransom) while disappeared and missing people are usually never heard from again.
- **The motive**: kidnapping tends to be for a specific demand while disappearances tend to occur to silence a staff member, often for political reasons.

Torture

Intentional physical maiming/injury that is explicitly characterized as torture of staff.

Wounded

An incident in which an employee was injured with a weapon as opposed to being beaten.

Deprivation of Liberty

Details and the outcomes of any action that deprives individuals of their liberty: kidnapping, hostage-taking, abduction, arrest, or detention.

Escaped

The victim escaped or attempted to escape which may have resulted in death or liberty.

Freed

The incident was resolved through the victim being freed.

Killed

The victim was killed in captivity or during a rescue mission or attempted escape.

In Captivity

The victim is still in captivity.

Missing

The victim is reported as missing.

No Information

There is no further information of what happened to the victim.

Rescue Mission

A rescue mission attempted or carried out which may have resulted in death or liberty.

Operational Space

Direct or indirect actions taken, or threats made, by a state or non-state actor that affect humanitarian access.

Abuse of Power

The use of legislated, executive, or otherwise authorized powers by government officials for illegitimate private gain. An illegal act by an office-holder constitutes abuse of power only if the act is directly related to their official duties.

Access Denied

Acts that:

- Prevent an organization from reaching beneficiaries or potential beneficiaries for needs assessments or direct service provision.
- Prevent beneficiaries from reaching services provided by an organization.

Accusations

A charge of wrongdoing by the authorities of the host country.

Application of Laws

Application of existing or new laws, executive orders, decrees, or regulations that, when applied, have an actual effect on the delivery of aid. This may include confiscation of equipment or putting people/organizations on watch lists.

Arrest

Arrests of employees. The arresting party must be operating in a governmental capacity (such as the police) in order to differentiate this incident from a hostage-taking incident. Arrests usually follow formal charges.

Attack on Another Organization

Reported attack on another organization that did not affect the organization directly.

Charges

A formal legal charge made by a governmental authority asserting that an employee or the organization has committed a crime.

Checkpoint

A non-border or frontier checkpoint erected in areas under control by the military, paramilitary, or an armed group to monitor or control the movement of people and materials that impact the delivery of aid.

Denial of Visa

Delay or denial of an official stamp, visa, or other permit granting permission to enter a country or territory within a country required to deliver aid.

Detention

Keeping an employee in custody prior to official charges or without any official charges; includes temporary detention for hours or days.

Expulsion

Act of forcing an employee or organization to leave a country or territory.

Face-to-Face Harassment

Incidents in which an employee is directly harassed by a person or group of people (example: harassment over the organization's program activities or programs).

Face-to-Face Intimidation

Incidents in which an employee is directly intimidated by a person or group of people (example: a staff member felt intimidated by armed actors patrolling near a food distribution).

Face-to-Face Threats

Incidents in which an employee is directly threatened by a person or group of people; should include some form of consequence for non-compliance (example: a threat of retaliation for not including someone in an organizational activity).

Fine

Money that must be paid by the organization as a punishment for not obeying a rule or law.

Forced Closure

Order by the government or other authorities to halt operations in a country or territory; includes closure affecting only one or multiple programs.

Government Action

Action by host or donor government that has a direct or indirect impact on the financial ability of an agency to deliver aid; includes freezing of funds, introducing taxes, or ending subsidies.

Imprisonment

Holding of an employee in a known official or unknown location, such as a prison, often following formal charges.

Introduction of Laws

The drafting of or voting on laws, executive orders, decrees, or regulations that, when applied, will have a potential or actual effect on the delivery of aid. This may include, but is not limited to, restrictive registration procedures, import regulations, or regular disclosure of financial sources.

Investigation

The process or act of examining facts related to allegations against employees or the organization.

Natural Disaster

Actual or forecasted natural disaster that occurs, or is predicted to occur, in a city or country in which the organization has an office. Natural disasters may include earthquakes, volcanoes, hurricanes, tornadoes, damage producing storms (hail, flash floods), floods, or tsunamis.

Property Entry Search

Search of a premise by external authorities.

Remote Threat Against Agency

Incidents in which the organization or an employee receives a threat not delivered face-to-face but by some remote mechanism (email, SMS, phone, or general threats issued on a website or social media). May include direct threats shouted by civilians during demonstrations.

Reputational Risk

Incidents involving a perceived, real, actual, or potential risk to the organization's branded logo/ emblem, image, or reputation.

Takeover/Occupation of Organizational Offices

The seizure and occupation of any organizational building, warehouse, or compound by civilian or government agents.

Threat of Closure

Incidents involving the threat of forced closure to an activity, program, or organization.

Witness

Events in which a staff member witnesses an attack or crime against another staff member, family members, or beneficiaries.

Other

Other Incident

An incident that cannot be adequately described by any of the pre-defined incident categories in this list. If this category is selected, the reporter should provide a full description of the incident in the 'incident description' field.

Near Miss

Incidents that could have caused harm or otherwise affected the delivery of aid. Includes any situation in which a security incident almost happened but did not happen, happened near an aid worker/organization/program, or where those affected were able to avoid any serious harm. If harm results, the incident should be classified under a different category.

Crime Near Miss

The near miss occurred in the context of a crime incident.

Killed/Injured/Kidnapped (KIK) Near Miss

The incident narrowly avoided an employee being killed, injured, or kidnapped.

Road Safety Accident (RSA)

Any road safety accident involving organization vehicles. Vehicle refers to any form of transportation, including, but not limited to, cars, trucks, buses, motorcycles, or others (bicycles, boats), occurring on and off duty.

Motorcycle Fatalities

Motorcycle accident with employee fatalities.

Motorcycle Injuries

Motorcycle accident with employee injuries.

Motorcycle No Injuries

Motorcycle accident with no employee injuries.

Other Traffic Accident

Other road traffic accident not listed here. If this category is selected, the reporter should provide the details in the 'incident description' field.

Vehicle Fatalities

Vehicle accident with employee fatalities.

Vehicle Injuries

Vehicle accident with employee injuries.

Vehicle No Injuries

Vehicle accident with no employee injuries.

Security Measures

Actions taken by agencies in response to generalized insecurity or a security incident.

Evacuation: Medical

An evacuation of an employee for medical reasons, generally involving injuries or illness that cannot be treated adequately at the local hospital, doctor's office, or treatment center.

Evacuation: Non-medical

An evacuation of an employee for security reasons. Evacuation refers to the removal of employees from the country of operation. The shifting of employees to another location within the country for security reasons is called relocation.

Hibernation

Process of sheltering in place until the danger has passed or further assistance is rendered.

Imposed Curfew

The imposition of a curfew in a city or country in which the organization has an office.

Office Closure

Decision to close an office in response to the general security context or a specific incident.

Ongoing Monitoring

Process of actively monitoring a security situation with a view to potentially changing the security measures.

Program Suspension

Process of significantly modifying planned activities usually by halting a specific activity or program.

Relocation

The movement of staff to another city or office within the country of operation for security reasons.

Restricted Travel - No Curfew

Any restrictions on travel that affect staff. This type of incident is similar to a travel advisory and may be the result of political or social unrest, outbreaks of disease, or natural disasters.

Sexual Violence and Abuse

Any sexual act or attempt to commit a sexual act, sometimes done using violence or coercion. Sexual violence can range from unwanted sexual comments and harassment to rape.

Unwanted Sexual Comments

Verbal advances that include whistling, shouting, and/or saying sexually explicit or implicit phrases or propositions that are unwanted.

Unwanted Sexual Touching

Unwanted touching of a sexual nature regardless of the intensity of the touch. May include massage, groping, grabbing, or grazing of any part of another person's body.

Sexual Harassment

Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature that affects the employment of the targeted person. Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Examples:

- Submission to such conduct is made either explicitly or implicitly regarding the terms/conditions of an individual's employment.
- Submission to or rejection of such conduct by an individual is used as a basis for employment decisions affecting the individual.

Aggressive Sexual Behavior

Potentially violent behavior focused on gratifying sexual drives.

Stalking

When a person carries out unwanted or repeated surveillance or acts towards another person.

Sexual Assault

Act of sexual contact on the body of another person without his/her consent.

Rape

Sexual intercourse (oral, vaginal, or anal penetration) against the will and without the consent of the person.

Attempted Sexual Assault

Attempted act of sexual contact on the body of another person without their consent.

Other Sexual Acts

When a person takes or shares nude pictures or videos of another person without permission.

Unrest

Civil or political unrest as well as tumultuous or mob-like behavior including: looting, prison uprisings, crowds setting things on fire, or general fighting with police (typically by protestors).

Demonstration

Any demonstration (protests, marches, sit-ins, picketing) that is nonviolent. Mass gathering of people for a political or social purpose.

Looting

Theft during unrest, violence, riots, or other upheavals.

Other

Any other activity not listed above.

Strike/No Show

Deliberate decision by staff not to come to work for reasons other than illness.

Weapons Use

The type of weapon(s) used in an incident that affected staff, infrastructure, or the delivery of aid.

Chemical, Biological, Radiological, and Nuclear Weapons (CBRN)

Any use of biological, chemical, nuclear, or radiological weapons in a city or country where the organization has an office.

Explosives

Any use of explosive weapons which involves the organization's employees or property.

Firearm

Any use of firearms or handheld weaponry which involves the organization's employees or property.

No Information

Weapons used in the incident, but the type of weapon is unclear.

Other

Any use of blunt, fire, knife, or stone which involves the organization's employees or property.

Explosive Weapons Use

The type of explosive weapon(s) used in the incident that affected staff, infrastructure, or the delivery of aid.

Aerial Bombs

Air-dropped explosive weapons, including incendiary weapons. Excludes cluster bombs and surface to surface missiles.

Cluster Bomb

Air-dropped or ground-launched explosive weapons ejecting smaller sub-munitions.

Hand Grenade

Small explosive device thrown by hand, designed to detonate after impact or after a set amount of time.

Mines

Any mine explosion that involves staff.

Other

Any other explosive weapon not listed or a combination of the above. If this category is selected, the reporter should provide the details in the 'incident description' field.

Radio-Controlled Improvised Explosive Device (RCIED)

Radio-controlled improvised explosive device, such as a bomb reported to have been left at the roadside and detonated when the target is near.

Surface Launched

Missiles, mortars, or shells that are launched from a mobile or stationary launch system, including rocket propelled grenades.

Suicide Vehicle Borne Improvised Explosive (SVIED)

Person-borne improvised explosive device (explosive suicide belt, explosive in a backpack).

Vehicle-Borne Improvised Explosive Device (VBIED)

Vehicle-borne improvised explosive device (car bomb, a car containing an explosive device).

Type of Location

The type of location where the incident took place.

Administration

During an administrative procedure or while the victim was obeying an order from a recognized/ government authority.

Airstrip

On an airstrip, including airport or in the air.

Checkpoint

At a checkpoint, gate, or roadblock.

Communication

In the form of a communication (phone call, SMS, letter, email).

Compound

At or in a compound of the provider concerned.

Crowded Area

In a crowded area, such as a market, bazaar, or an open public space where people are moving about.

Health Building

At or in a health building, hospital, clinic, hospital office, or first aid post.

IDP or Refugee Camp

At or in a temporary or permanent camp for refugees or Internally Displaced Persons (IDPs).

No Information

It is unclear where the incident took place from the available information.

Office Building

At or in an office compound.

Other

In any area not listed here. If this category is selected, the reporter should provide the details in the 'incident description' field.

Police Station

At a police station or compound.

Project Site

At the location of a project.

Public Building

At or in a public building (restaurants, churches, mosques, hotels).

Residence

At or in a residence of an aid worker; includes incidents that occurred immediately outside residences.

Road

On a road, including:

- Unspecified locations during a road journey
- Any mode of transportation (foot, motorbike, vehicle)
- Any incident that takes place between places or in transit

School

At a school or place of education.

Ship

On a boat or ship.

Warehouse

At or in a warehouse, including docks.

Water

On or beside water (river, lake, sea, ocean).

Perpetrator

The classification of the perpetrator(s) reportedly responsible for the incident.

Administration

An administrator/authority of a country/territory, the high command level of an armed force, or individuals within an armed group that has assumed the de-facto control of a territory and who determines laws, regulations, and/or orders enforcement.

Beneficiary

A direct beneficiary of aid.

Civilian

A civilian (refugee, IDP, villager, settler), but not a direct beneficiary.

Criminal

A criminal either acting alone or as part of organized crime.

Employee or Former Employee

A current or former employee of the organization.

Law Enforcement

Individual or organs of the law enforcement apparatus of the state (police and ‘security forces’) but not military forces or private security who act under orders of the state’s law enforcement system.

Multiple

Multiple perpetrators from different categories involved in the attack.

No Information

The report does not identify the perpetrator, or the perpetrator is unknown.

Non-State Armed Groups

A named armed group who are not part of the state’s law enforcement, military, or security apparatus. Includes, private armies, vigilantes, rebel, guerrilla or terrorist groups. This does not include private security actors.

Private Security

The perpetrator belongs to a private security firm or functions as a bodyguard or security guard.

Relative or Associate

A family member, friend, or other person(s) known by an employee(s).

State Actor

Soldiers of a state army who act under orders of the state military command.

Sub-Contractor

A sub-contractor to the agency.

Unspecified Non-Military Armed Actors(s)

A group of unidentified or unnamed armed people or the report refers in a generic sense to rebels, extremists, or groups in some form affiliated with military or using military type of structures (wearing army fatigues) without indication that they were linked to any state army.

Motive

The classification of the motive of the perpetrator(s).

Assumed Selective

A targeted action used specifically against an employee, organization, or beneficiary, but the motive remains unclear.

Indiscriminate

A targeted action used against civilians and not specifically towards an employee, organization or beneficiary.

Selective Assets

A targeted action used against an employee, organization, or beneficiary but with the motive of material gain, or access to goods or infrastructure rather than the intention to hurt the employee, organization, or beneficiary.

Selective Military Action

Someone or something was selectively targeted (including troop movements, a weapons factory) and the employee, organization, or beneficiary was affected as a result. This category is specific to events that occur during active conflict.

Selective Other

Someone or something was selectively targeted, and the employee, organization, or beneficiary was affected as a result.

Selective Program

A targeted action used against an employee, organization, or beneficiary because they provided (the program or service) or used (the beneficiary) a particular program or service.

Selective Provider

A targeted action used against an employee, organization, or beneficiary because of the identity or core values of the organization.

No Information

The report does not contain enough information to determine if the event was targeted or not.

Information about the Victim(s)

When recording information about the victim(s) involved in an incident, consider including the categories below. This information should be kept confidential and any decisions made on the basis of this information should be non-discriminatory and in accordance with equality, diversity and inclusion policies, and relevant legislation.

Gender

Classify victims by their biological sex or chosen gender identity (depending on your organization's policy).

Ethnicity

Where relevant and appropriate, consider including information on ethnicity if this can help identify underlying patterns of threats or violence.

Diversity

Where relevant and appropriate, consider including information on other diversity factors such as sexual orientation or disabilities if this can help to identify underlying patterns of threats or violence.