CEN/WS IPCI

Date: 2023-04

prCWA XXXX:2023

Secretariat: UNE

Emergency management — Incident situational reporting for critical infrastructures

Contents

European foreword

Results incorporated in this CWA received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883520.

List of participants.

Introduction

Each EU Member States has unique processes and procedures for crisis management and disaster response. In the case of cross-border crises, these different approaches may cause confusion or conflict among first responders and civil protection bodies. Developing a common language and standardising procedures and interfaces across the EU is thus essential for facilitating cross-border collaboration, thereby helping to protect assets and save lives.

The EU-funded research project STRATEGY has systematically identified and prioritised gaps in standardization in crisis and disaster management and has compared them to the needs of end users and to available opportunities across a broad spectrum of disaster management activities. All standardisation items to be developed in the course of the STRATEGY project have been fully tested and validated in tabletop exercises (TTXs) and in one full-scale exercise (FSX).

The recently published DIRECTIVE 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities and repealing Council Directive 2008/114/EC [1] states (Art 15-Incident notification) that:

“Member States shall ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Member States shall ensure that, unless operationally unable to do so, critical entities submit an initial notification no later than 24 hours after becoming aware of an incident, followed, where relevant, by a detailed report no later than one month thereafter”. The notifications will include information for:

“*(a) the number and proportion of users affected by the disruption;*

(b) the duration of the disruption;

(c) the geographical area affected by the disruption, taking into account whether the area is geographically isolated.”

In the Directive 2022/2557 [1], it is also clearly mentioned that “*Where an incident has or might have a significant impact on the continuity of the provision of essential services to or in six or more Member States, the competent authorities of the Member States affected by the incident shall notify the Commission of that incident”.*

Currently, in case of an emergency incident, there is no standardised type and content of information to be sent from a critical infrastructure to a nationally designated contact point for critical entities. A standardised description with specific fields of incidents dedicated to critical infrastructures would help to support the response to the incident and the restoration of services.

Some standardised references focus on the transmission of data or alerts while incident reporting is used mainly as a situation reporting for various cases, and not for critical infrastructures.

ISO/TR 22351:2015 [2] provides a technical schema for exchanging messages mainly between first responders’ organizations while OASIS-EDXL [3] standards are technical standards which focus on providing alert messages or situation report messages that could fit a variety of situations but not specifically used for incident reporting for critical infrastructures.

Also, the M/ETHANE [4] model is a framework developed by JESIP (Joint Emergency Services Interoperability Principle) that provides a common structure for first responders and relevant control rooms to share information related to incidents, and in the end could be used for incidents related to critical infrastructures as well.

This document is designed to be used in cases where incidents occur to critical infrastructures in informative Annex A.

1 Scope

This document provides requirements and recommendations for a common set of information, datatypes and terms to be reported and provided by affected critical infrastructures to national or local coordination centres or control rooms of emergency services or competent authorities. Then coordination centres can share this information with other emergency authorities and other critical infrastructures in case of an emergency incident.

This information sharing aims at the higher command levels, i.e., strategic and operational (FEMA 2010, [5]) of crisis management and response. It is not aimed at the tactical level (forces on scene).

The incident information defined in this document is structured in a way to provide to the personnel responsible for responding to such incidents, the necessary and sufficient information that will help them to understand the severity of the incident and its potential consequences, easily and rapidly.

Recommendations for displaying this information on a computer screen or printing in a usual paper format are also provided in Annex B (informative).

In addition, the incident information could be used in order competent authorities to maintain statistics on incidents affecting critical infrastructures.

This document does not aim to provide a technical schema for the information shared between organisations or systems but to recommend on the structure and on the necessary information as well as to provide suggestions for template that easily provided insight into the situation to the intended audience.

The intended users of this document are security liaison officers of critical infrastructures, public administration, coordination centres, first responders' control rooms and first responders of a higher command level.

2 Normative references

The following documents are referred to in the text in such a way that some or all their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22324:2022, *Societal security — Emergency management — Guidelines for colour-coded alerts*

ISO 8601-1:2019*, Date and time format — Representations for information interchange — Part 1: Basic rules*

ISO 3166-1:2020*, Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

[EDXL-SitRep] *Emergency Data Exchange Language Situation Reporting (EDXL-SitRep) Version 1.0*. Edited by Rex Brooks, Timothy Grapes, Werner Joerg, and Jeff Waters. 06 October 2016. OASIS Committee Specification 02

http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/cs02/edxl-sitrep-v1.0-cs02.html

Latest version: http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html

World Geodetic System — 1984 (Geographic Coordinate System WGS 84), EPSG, Code: 4326

3 Terms and definitions

For the purpose of this document, the following terms, definitions, and abbreviations apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
cancel report
report when the event has been cancelled, for any reason, by the *critical infrastructure* (3.3)

3.2
crisis
unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property or the environment

[SOURCE: ISO 22300:2021, 3.1.60]

3.3
critical infrastructure(s)
CI(s)

asset, system, or part thereof, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, where the *disruption* (3.4) or destruction of which would have a significant *impact* (3.8) in a society as a result of the failure to maintain those function

[SOURCE: EN 17483-1:2021, 3.1]

3.4
disruption
incident (3.9), whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organisation's objectives

[SOURCE: ISO 22300:2021, 3.1.75]

3.5
emergency
sudden, urgent, usually unexpected occurrence or *event* (3.6) requiring immediate action

Note 1 to entry: An emergency is usually a disruption or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

[SOURCE: ISO 22300:2021, 3.1.87]

3.6
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences and can have several causes and several consequences.

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.

[SOURCE: ISO 31000:2018, 3.5]

3.7
final report
report that is sent when an *incident* (3.9) is finalised and services have been restored

3.8
impact
outcome of a *disruption* (3.4) affecting objectives

[SOURCE: ISO 22300:2021, 3.1.118]

3.9
incident
event (3.6) that can be, or could lead to, a disruption, loss, *emergency* (3.5) or *crisis* (3.2)

[SOURCE: ISO 22300:2021, 3.1.122]

Note 1 to entry: The unique identification of *incident* (3.9) is expressed as 'incident ID' in this document.

3.10
incident certainty
confirmation level of the *incident* (3.9), as provided by the *critical infrastructure* (3.3) operator and/or security liaison officer

3.11
incident priority
information related to priority that should be given by first responders for response actions expressed in specific levels

3.12
incident severity
measure of the possible consequences of the *incident* (3.9) expressed in specific levels

Note 1 to entry: Definition derived from ISO/IEC Guide 63:2019, 3.17 severity.

3.13
incident urgency
level of *incident* (3.9) importance related to responsive actions that should be taken in a given time frame

3.14
initial report
report sent by the *critical infrastructure* (3.3) when the *incident* (3.9) occurs and new information regarding an *incident* (3.9) or activity is reported

3.15
recovery time objective
RTO
period of time following an *incident* (3.9) within which a product and service or an activity is resumed, or resources are recovered

Note 1 to entry: For products, services and activities, the RTO is less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

[SOURCE: ISO 22300:2021, 3.1.203]

3.16
update report
report that provides updates information superseding or complementing the *initial report* (3.14)

4 The incident report

4.1 General

The structure of the incident report as well as the set of information items, one by one, that shall be included in the set of information sent are described.

Besides the structure, the information that is used also refers to:

— an initial report sent with the incident occurrence (initial report, 3.14);

— an updated report with the aim to update the information related to the incident (update report, 3.16);

— a report which aims to provide information related to the restoration of service (recovery time objective, 3.15) and closing of the incident (final report, 3.7); and

— a fourth type of report, for cases that the incident has been cancelled (cancel report, 3.1).

4.2 Structure of the incident report

The incident report form contains various information ranging from the type of information necessary to identify the person that fills it in and some contact details that could be valuable during an emergency, to more detailed information that could be useful for other organisations and the continuation of the provided services.

The following sections shall be included in the incident report:

(a) user and incident identifier,

(b) incident description, and

(c) risk description.

Additionally, the following information should be included in the incident report, if considered necessary:

(a) actions, and

(b) resources.

4.2.1 User and incident identifier

The person or group of persons responsible for reporting the identified incident shall provide the set of information and data through which the organisation and person or group of persons responsible for reporting the incident are identified. This shall include contact details and key information about the incident.

NOTE In all the document the required/recommended information in the incident report will be completed by a person or group of persons (team). To simplify the text ‘person’ is included referring to one person or the whole team responsible.

4.2.2 Incident description

The person responsible for reporting the incident shall describe the incident occurrence with the following information:

— date, time and location;

— confidence level of the information shared (certainty);

— the area, geographical data and accessibility to the location of the incident; and

— high level description of the incident in a free text format.

The high level description in a free format could also include, briefly, information such as the cause of the incident, actions taken in place and potential resources needed.

4.2.3 Risk description

The person responsible for the incident notification and report shall provide the following information related to the incident:

— the hazards and threats;

— potential casualties; and

— the impacts to the critical infrastructure and the services provided to other interconnected critical infrastructures, and to society (i.e., citizens, area, environment, etc.).

These are considered to be estimations, at least for the incident initiation (initial report), while for the other report types these should be based on observations and the final outcome of the incident (see 4.3.2).

4.2.4 Actions

The person responsible for the notification and reporting should provide information related to the actions and measures that the critical infrastructure has taken to restore the services and to minimize the impacts.

The aim is to improve situation awareness for emergency and first responders’ services. The critical infrastructure operator should fill in this section with the goal that it is an additional support for the emergency services in order to understand the current situation.

In relation with 4.2.5, this information will support the processes for the mobilisation of the proper emergency response forces (types and amounts of units).

4.2.5 Resources

The person responsible for reporting incidents should provide information related to the resources currently used by the critical infrastructure and any necessary additional resources.

4.3 Content of the incident report

The incident report is meant to be sent by the critical infrastructure and more specifically by the infrastructure security liaison officer or the infrastructure operator (person or group of persons).

The recipients are the coordination centre of a competent authority that monitors and supervises critical infrastructures or an emergency control room of first responders' organisations.

The content of the report may be different according to the report type (see 4.1). For the initial report, it is considered that estimations are provided; for update and especially for the final report of an incident the observations should be sent, if possible.

The information to be sent is presented in 4.3.1 while 4.3.2 includes the discrimination of that information based on the report type.

4.3.1 Set of information sent

The information is clustered according to the structure described in Clause 4.2.

4.3.1.1 User and incident identifier

4.3.1.1.1 Incident report type

This sub-clause describes the four different report types. The person responsible to send the report shall provide information on the report type. The following options shall be selected:

— Initial report (3.14).

— Update report (3.16).

— Final report (3.7).

— Cancel report (3.1).

NOTE 1 These options are similar and can be matched to the various options used in OASIS EDXL-SitRep standard [3] and ISO/TR 22351:2015-EMSI [2].

4.3.1.1.2 Incident ID

This information is used for identifying the incident in various databases. In case the report is done through an automatic system, a unique identifier shall be given automatically by the system.

This set of information shall be filled in by the person or system responsible for reporting the incident.

When an automatic number is provided shall be confirmed by the person or system responsible for reporting the incident.

The incident ID format shall remain constant.

The following text structure includes the ID format that should be used:

XXXX – YYYYMMDD – NN – T

where

XXXX	is the CI name in 4 letters.
YYYYMMDD	is the date.
N	is the number of the event, (e.g. 01 or 99).
T	is the first letter of the report type:

R	for initial report.
U	for update report.
F	for final report.
C	for cancellation report.

4.3.1.1.3 Report recipients

This information is referred to the organisations that will receive the report of the incident. This set of information provides some options to whom the critical infrastructure operator or security officer may send the report. This also supports the coordination procedure as any organisation that receives the report is aware instantly for other organisations that have been notified.

The national and EU legislation, organisational structures and procedures should be taken into account in preparation of the potential recipients.

Some possible recipients are:

- NCIP: National Contact Point for critical infrastructures.
- Police authorities.
- Fire Service.
- Medical emergency services.
- Civil protection.
- Coastguard.
- Other: this option, includes other critical entities that may be affected.

4.3.1.1.4 Linked incident

This information provides the necessary input for the correlation of the reporting incident to another one registered and should be given by the person responsible to send the report. The following options shall be selected, if known:

- Yes.
- No.
- Unknown.

4.3.1.1.5 Linked incident ID

This information is an identification of the linked incident and is requested mainly to be used for storage in systems and databases. This linked incident ID should be sent only in the case that there is a link between various incidents and the person sending the report is aware of such an incident. If there is such information, the linked incident ID shall follow 4.3.1.1.2.

In case there is no linked incident, no information should be sent.

4.3.1.1.6 Incident report creation date and time (local)

The date and time when the incident report was created shall be provided, expressed in local time, and not when the incident occurred.

The following schema shall be followed:

YYYY-MM-DD Thh:mm:ss (Local date and time) [following ISO 8601-1:2019]

NOTE If a specific tool is considered to be used as the means to populate such a report, then this set of information could be filled in automatically by the system. Local date and time can be used for printed versions, or forms presented in a pc screen.

4.3.1.1.7 Incident report creation date and time (UTC)

The date and time when the incident report was created and not when the incident occurred in UTC shall be provided. UTC date and time should be the main time used in databases or other software tools.

The following schema shall be followed:

YYYY-MM-DD Thh:mm:ss (Date and time are in UTC) [following ISO 8601-1:2019]

NOTE If a specific tool is considered to be used as the means to populate such a report, then this set of information could be filled in automatically by the system.

4.3.1.1.8 Critical infrastructure business name

The person responsible for reporting incidents shall declare the official business name of the critical infrastructure or at least a widely known abbreviation of the critical entity.

4.3.1.1.9 Critical infrastructure sector

The person responsible for incident reporting shall provide information on the type of the critical infrastructure. The list of critical entities mentioned in the Directive EU 2022/2557 [1] should be used (see A.2.).

4.3.1.1.10 Person/group reporting

This set of information describes the name or the position of the person or group of persons (team) responsible for the contact and reporting, e.g., security liaison officer or the infrastructure operator and shall be given to the competent authorities.

4.3.1.1.11 Person authorized

This set of information should be provided and describes the position of the person responsible for the contact and reporting, e.g., security liaison officer or the infrastructure operator.

NOTE This type of information could be set automatically in case the report is completed through a software or a dedicated computer tool.

4.3.1.1.12 Contact details/telephone number

The telephone number (landline or cell phone) shall be communicated to the competent authorities. It includes the telephone number with country telephone code.

NOTE This type of information could be set automatically in case the report is completed through a software or a dedicated computer tool.

4.3.1.1.13 Contact details/email

The email address of the person responsible for reporting emergency incidents shall be shared with the competent authorities.

NOTE This type of information could be set automatically in case the report is completed through a software or a dedicated computer tool.

4.3.1.1.14 Country (code)

This describes the country where the incident occurred and consequently the country where the critical infrastructure is located. The person reporting should provide information on the country.

In case this is done, this information shall be provided according to ISO 3166-1:2020.

NOTE 1 This type of information could be set automatically in case the report is completed through a software or a dedicated computer tool.

NOTE 2 The country codes in ISO 3166-1 and their definition can be consulted in the ISO Online Browsing Platform (BOP) available at http://www.iso.org/obp

4.3.1.2 Incident detailed description

The following subclauses are related to the necessary information for the incident description that identifies the date, time and location of the incident as well as a short description of the incident, and the persons responsible to send the report that shall provide this information.

4.3.1.2.1 Incident occurrence date and time (local)

The date and time that the incident occurred in local time shall be provided following the ISO 8601-1:2019 format:

— YYYY-MM-DD, Thh:mm:ss (Local date and time) [following ISO 8601-1:2019]

NOTE If a specific tool is considered to be used as the means to populate such a report, then this set of information could be filled in automatically by the system. Local date and time can be used for printed versions, or the ones presented in a pc screen.

4.3.1.2.2 Incident occurrence date and time (UTC)

The date and time that the incident occurred in UTC time shall be provided following the ISO 8601-1:2019 format.

— YYYY-MM-DD, Thh:mm:ss (Local date and time) [following ISO 8601-1:2019]

NOTE If a specific tool is considered to be used as the means to populate such a report, then this set of information could be filled in automatically by the system.

4.3.1.2.3 Incident certainty

The certainty shall be used in a way that represents as far as possible the confidence level of incident command for report accuracy of current situation, ranging from simple hypotheses to real observations. Incident certainty should be directly related to the overall impacts of the incident, if possible, and not necessarily to the incident itself. From the moment that a security liaison officer or the critical infrastructure operator makes use of such a report, the incident is considered as a true and confident event. Thus, confidence should be related to impacts.

In order to be aligned and interoperable with other international standards, the options of OASIS EDXL-SitRep [3] shall be used as reference:

— HighlyConfident: is the topmost level of confidence. For the purposes of this CWA, this must be used for validated (real) observations.

— SomeWhatConfident: corresponds to a medium level of confidence and must be used when the details of the incident and specifically of the impacts are estimations.

— Unsure: corresponds to a low confidence level and must be used when the details of the incident and specifically of the impacts are estimations.

— NoConfidence: corresponds to information that has not been verified in any extent. It is suggested not to use this option for cancellation of previous events.

NOTE For the estimations, it is up to person responsible for the reporting to select which type of option to use based on their experience, expertise and available information.

4.3.1.2.4 Area (geographic)

The person reporting shall provide the name of the (broader) area in which the affected critical infrastructure is located and/or the incident occurred.

4.3.1.2.5 Geographic coordinates

The geographical coordinates of the affected critical infrastructure shall be in WGS 84 (EPSG:4326).

This could be directly selected through a map in case of the availability of a technical reporting tool.

Latitude and longitude are considered to be the centre point of the affected infrastructure, building, incident or area and shall be provided.

Elevation, radius and polygon should be provided, if possible.

Radius and polygon should support the fact of knowing an affected area and not a single point.

- Latitude.
- Longitude.
- Elevation: provide the elevation of the site in meters, if known or available.
- Radius: provide a distance around the centre point that define an area, if known or available. Distance should be provided in meters. Nevertheless, other measurement units may be used but the person reporting shall denote the measurement unit as well. In case, no measurement unit is clearly denoted, then the number representing radius is considered to be in meters.
- Polygon: provide geographic coordinates that define a polygon of the affected area, if known or available.

NOTE In case a computer tool is used for the reporting this information could be selected through a mapping application.

4.3.1.2.6 Incident description

A brief description of the incident (what happened) shall be provided in a free text format. The operator shall describe briefly not only the incident but also what has been affected, e.g., earthquake occurrence, central pipeline damaged, service interrupted.

4.3.1.2.7 Accessibility status

The person or group of persons reporting should provide briefly the current status of access and/or evacuation routes (land, sea, air). Provide specific information on routes that are not accessible, if known and anything considered important or necessary for responders to approach and/or evacuate and they should be aware prior to their response.

4.3.1.3 Risk description

The following subclauses provide more detailed information on the incident occurrence and the impacts and consequences to the critical infrastructure itself and other interconnected critical infrastructures, to the society and the environment.

4.3.1.3.1 Incident type

The user shall provide information whether the incident reported is a true incident or a potential threat. The following values shall be used:

- Minor level threat.
- Moderate level threat.
- High/critical level threat.
- True incident.

4.3.1.3.2 Hazard type

The person reporting shall provide the information on the hazard type that caused the incident. This set of information is a free text.

Widely accepted terms shall be used, for example, in an earthquake incident, the hazard could be a single word: “earthquake” or “seismic event”. Avoid other, more simplified, terms such as “quake”.

Annex C (informative) includes an indicative table of the OASIS Event Terms [6] (see C.2) that can be used, if appropriate.

4.3.1.3.3 Incident severity

This set of information provides an overview of the severity of the incident from the perspective of the critical infrastructure and should be provided by the person (group of persons) sending the report. The options available to the OASIS EDXL-SitRep shall be used.

In cases when no information regarding the severity of the incident is available or not able to be estimated, the option “Unknown” shall be selected.

- Extreme.
- Severe.
- Moderate.
- Minor.
- Unknown.

4.3.1.3.4 Incident urgency

Incident urgency from the perspective of the critical infrastructure should be provided. Critical infrastructure reporting person should fill this information based on the overall knowledge for the incident.

According to ISO/TR 22351:2015 [2] incidents are distinguished between urgent and not urgent. Based on the open OASIS EDXL-SitRep [3] urgency is related to actions that should or not be taken immediately. Level of urgency should be in line with the respective priority and severity.

The following values adopted from OASIS EDXL-SitRep [3] should be used:

- Immediate – Responsive actions should be taken immediately.
- Expected – Responsive actions should be taken within the next hour.

- Future – Responsive actions should be taken in the near future.
- Past – Actions to respond are no longer required.
- Unknown.

4.3.1.3.5 Incident priority

This set of information mainly targets first responders in order to provide them with information relevant to situational awareness. Critical infrastructure operator should provide this information in relation to urgency and severity, based on the options provided in ISO/TR 22351:2015 [2], in order to enhance interoperability with other standards.

This information should be provided to extent possible at the time of the reporting. One of the following options should be selected:

- Priority not assessed.
- No estimated priority for mission accomplishment.
- Minor priority to mission completion due to no aggravation.
- Standard priority due to possible limited aggravation in absence of mission accomplishment.
- Critical priority due to possible fatal worsening without mission accomplishment.
- Extremely critical priority due to possible fatal mass worsening without mission accomplishment.

4.3.1.3.6 Description of impacts

The critical infrastructure operator/security liaison officer shall use this set of information to describe in a free text format the impacts related to the incident and provide more details than the “Incident description” in 4.3.1.2.6.

Here, the responsible person shall describe any unplanned deviations from the usual service provision.

The user(s) shall describe not only the disruption of service but also the consequences inside the stricken critical infrastructure. Information such as the status of services, the type of damage, mechanical, structural or other damage (inside or outside the critical infrastructure) shall be described.

EXAMPLE If a leak of a CBRN agent has been occurred, the type of the substances, the type of the leak (in the water, in the air or in the soil) has been observed.

Depending on the incident form type (see 4.3.1.1.1) the impact is either estimated or observed. These impacts can be anticipated or unanticipated.

4.3.1.3.7 Scale of impacts

This information shall be provided form the critical infrastructure even if it is an estimation at the time of the reporting. It shall consider the above provided information. For this, the following impact levels options from the EDXL-SitRep shall be used in order to facilitate the process:

- Unknown.
- No damage.
- Minor.

- Moderate.
- Large.
- Massive.

4.3.1.3.8 Critical Infrastructure service affected

The person responsible to fill in and send the report shall. briefly, describe the service that has been or will be affected.

4.3.1.3.9 Human losses

This information shall be related to direct and indirect impact to the population (internal and external to the infrastructure) due to the incident. Critical infrastructure operators or security liaison officers shall provide information regarding the casualties related to their jurisdiction or their immediate nearby locations for which they are aware of. In case there is no information, the option "Unknown" shall be selected.

Primarily, and especially in the initial report (this shall be considered as an estimation. In the final report (incident terminated and service restored) this information should be related to the real circumstances.

The user should follow the OASIS EDXL-SitRep "Casualty & illness element" [3] options as most appropriate for the purposes of this document. The following options are proposed, not being exhaustive:

- Fatalities – number of fatalities.
- Hospitalized – number of persons hospitalized.
- Injured – number of injured.
- In need of rescue – number of persons in need of rescue.
- Missing – number of missing persons.
- Evacuated – number of persons evacuated from the incident scene.
- Sheltered in Place – number of persons sheltered in place of incident.
- In temporary shelters – number of persons transferred to temporary shelters.
- Quarantined – number of persons in quarantine due to the incident.
- Unknown – if there is no information at all about human loss, then this option may be used.
- Not applicable – in case this is not applicable for the infrastructure, then this option must be selected.

Alternatively, if the above information is difficult to be used by the person reporting, then one of the most common triage system (START – Simple Triage And Rapid Treatment, 1983, [7]) should be used:

- P1 – number of injured people requiring immediate care.
- P2 – number of injured people requiring delayed care.
- P3 – number of injured people requiring minimal care.
- Dead – number of dead people (if any).

- Unknown.

4.3.1.3.10 Expected external impacts (impacts to other critical infrastructures)

This information should be related to any knowledge or estimation of the impacts of the incident to other interconnected critical infrastructures. This is an information on an estimation level, for all types of reports. In the closing report of the incident, the operator may declare according to his/her knowledge any potential impacts to other critical infrastructures, if known. The use shall provide this information in a free, narrative text format.

4.3.1.3.11 Recovery time objective

This information is related to estimations, mainly for the initial report of the incident, from the critical infrastructure regarding the restoration time of the service affected. This is a free text set of information. The critical infrastructure operator shall provide information on when the service or a specific percentage of the service will be restored, expressed either on specific date and time or an extent of the time. For example, the operator shall provide a wording such as: "Service fully restored in the next 2 hours" or "Service restored to 50 % of the users in the next 12 hours" or "service restored at YYYY-MM-DD, Thh:mm:ss (Local date and time)".

4.3.1.4 Actions

Basic actions taken by the critical infrastructure in order to minimize the impacts of the incident should be provided by the critical infrastructure.

4.3.1.4.1 Specific actions already in place

The user should select among the following simple options:

- Yes.
- No.
- Will be initiated immediately.

4.3.1.4.2 Alternative infrastructure in place for same service provision

The user should select among the following options:

- Another unit internally from the same operator.
- Other operator via collaboration.
- No.
- Not applicable.

4.3.1.4.3 Description of the actions

Briefly describe the necessary actions taken or the ones that will be taken to minimize the impacts of the incident. The person reporting this information should provide it in a free, narrative text format.

4.3.1.5 Resources

The basic information related to the resources used by the critical infrastructure should be provided. Detailed request of resources is out of the scope of this CWA. For such type of request, the ISO/TR 22351 [2] or the open OASIS EDXL-SitRep [3] technical standards can be used.

4.3.1.5.1 Resources used by the critical infrastructure

The type and number of resources used to minimize the impacts of the incident should briefly mentioned.

4.3.2 Set of information based on the report type

The information sent for the case of update, final or cancellation of the incident is mainly the same as in the incident initiation report. It is up to the person in charge or group of persons to fill in the necessary information that will provide update for situation awareness purposes or for the finalisation or cancellation of the incident and the restoration for services. Nevertheless, some of the information that is required for the report (initial incident report) can be exactly the same or without any difference for the update, the finalisation or cancellation type.

EXAMPLE Information such as the incident occurrence date and time or incident priority are not necessarily important or without any use for the update or cancellation type, especially when the reporting is made through a computer software and not by hand.

Thus, Table 1 resumes the various information that is required and recommended for the four incident report types.

Table 1 — Characterisation of type of information based on the report type

Incident report type	Report	Update	Final	Cancel
Incident ID (4.3.1.1.2)	a, d	a, d	a, d	a, d
Report recipients (4.3.1.1.3)		b	c	Not applicable
Linked incident (4.3.1.1.4)		b	c	c
Linked incident ID (4.3.1.1.5)	a	b	c	c
Incident report creation date and time (local) (4.3.1.1.6)	a, d	b, d	c, d	c, d
Incident report creation date and time (UTC) (4.3.1.1.7)	a, d	b, d	c, d	c, d
CI business name	a, d	b, d	c, d	c, d
CI sector (4.3.1.1.8)	a, d	b, d	c, d	c, d
Person/group reporting (4.3.1.1.9)	a, d	b, d	c, d	c, d
Person authorized (4.3.1.1.10)	a, d	b, d	c, d	c, d

Incident report type	**Report**	**Update**	**Final**	**Cancel**
Contact details / telephone number **(4.3.1.1.11)**	a, d	b, d	c, d	c, d
Contact details / email **(4.3.1.1.12)**	a, d	b, d	c, d	c, d
Country (code) **(4.3.1.1.13)**	a, d	b, d	c, d	c, d
Incident occurrence date and time (local) **(4.3.1.2.1)**	🟦	b	c	Not applicable
Incident occurrence date and time (UTC) **(4.3.1.2.2.)**	a	b	c	Not applicable
Incident certainty **(4.3.1.2.3)**	🟦	b	c	Not applicable
Area (geographic) **(4.3.1.2.4)**	🟦	b	c	Not applicable
Geographic coordinates **(4.3.1.2.5)**	🟦	b	c	Not applicable
Incident description **(4.3.1.2.6)**	🟦	b	c	c
Accessibility status **(4.3.1.2.7)**	🟩	b	c	Not applicable
Incident type **(4.3.1.3.1)**	🟦	b	c	Not applicable
Hazard type **(4.3.1.3.2)**	🟦	b	c	Not applicable
Incident severity **(4.3.1.3.3)**	🟩	b	c	Not applicable
Incident urgency **(4.3.1.3.4)**	🟩	b	🟦	Not applicable
Incident priority **(4.3.1.3.5)**	🟩	b	Not applicable	Not applicable
Description of impacts **(4.3.1.3.6)**	🟦	b	c	Not applicable
Scale of impacts **(4.3.1.3.7)**	🟦	b	c	Not applicable

Incident report type	Report	Update	Final	Cancel
CI service affected (4.3.1.3.8)	🟦	🟦 [b]	🟦 [c]	Not applicable
Human Losses (4.3.1.3.9)	🟦	🟦 [b]	🟦 [c]	Not applicable
Expected external impacts (4.3.1.3.10)	🟩	🟩 [b]	🟩 [c]	Not applicable
Recovery time objective (4.3.1.3.11)	🟦	🟦 [b]	🟩 [c]	Not applicable
Specific actions already in place (4.3.1.4.1)	🟩	🟩 [b]	🟩 [c]	Not applicable
Alternative infrastructure in place for same service provision (4.3.1.4.2)	🟩	🟩 [b]	🟩 [c]	Not applicable
Description of the actions (4.3.1.4.3)	🟩	🟩 [b]	🟩 [c]	Not applicable
Resources used by the CI (4.3.1.5.1)	🟩	🟩 [b]	🟩 [c]	Not applicable

Key

🟦	#3c73a8-Mandatory information that is required in the relevant subclause.
🟩	#3c73a8-Optional information that is recommended in the relevant subclause.

[a] In case a software or a computer tool is used for the reporting, this information can be filled in automatically.

[b] In case a software or a computer tool is used for the reporting, this information can be filled in automatically based on the values of the "initial" report. If the form is pre-populated, then the user can update whatever thinks appropriate.

[c] In case a software or a computer tool is used for the reporting, this information can be filled in automatically based on the values of the "update" report. If the form is pre-populated, then the user can update whatever thinks appropriate.

[d] In case a software or a computer tool is used for the reporting can be pre-populated through registered and authenticated users.

5 Rules for designing the report

The following subclauses provide requirements, recommendations and guidelines on how to design an easy-to-read incident report either as printed version or on a computer screen following ISO 22324:2022 for colour-coded alert when it comes to the use of colours in the incident report.

A template of the printed version form and an example of the reports for a case study are presented in Annex B (informative).

5.1 Report size

It is advisable the report to be printed on a single page of a usual paper size (e.g., A4 – ISO 216:2007 [8]) or fit an average computer screen without the need for the user to scroll up or down.

5.2 Fonts

According to CEN ISO/TR 22411 [9] the fonts used for the report when printed or shown as filled in, should be the Sans-Serif. The size of the fonts should be minimum 8pt. The most preferred option is 10pt. Headers can be increased by one or two points.

5.3 Structure

The printed version shall make clearly visible the five distinct sections covering user identifier, incident description, incident risk description, actions and resources as described above. The sections can be separated using thick dividing lines (e.g., 3pt lines).

5.4 Headers

Headers shall stand out from the rest of the information. To fulfil this, headers shall be at least one point (1pt) larger in size than the rest of the information, and shown in bold, as proposed in 5.2, or they shall be shown in a negative contrast as in the example below.

Section headers shall use centre alignment, whereas other headers must use left alignment. Section headers must be in bold, also when using negative contrast.

Header	or	Header

5.5 Specific fields

Information reported should be depicted in a black and white style as shown in the example below:

Header 1
Information 1

For making the report easily readable and to focus on information that has special meaning, the following information should be depicted with specific colouring style as suggested by ISO 22324:2022:

- Incident Type.
- Incident Severity.
- Scale of impacts.
- Incident Urgency.
- Incident Priority.
- Human Losses.

Any of the three colours pallets and saturation systems provided in ISO 22324:2022 shall be followed and more specifically the various options provided in ISO 22324:2022, Table B.1.

In this document the RGB saturated version of the colours irrespective of the colour specification system is included as recommendation.

The concept behind colouring specific cells is to provide the end user a way to identify very fast incidents with higher degree of severity. Thus, as the severity or the consequences get higher, the colours tend to be represented by red or darker combinations as proposed by ISO 22324:2022.

5.5.1 Incident type

The concept of providing colours on incident type is to make faster and easily understandable by the final user. The following rules in Table 2 should apply:

Table 2 — Recommendations on colours for scale of impacts

Field	Level	RGB colour
Incident Type	Minor level threat	110/185/53
	Moderate level threat	244/207/0
	High or Critical level threat	240/140/17
	True incident	199/22/30

5.5.2 Incident severity

For the incident severity the following rules should apply. In this case, the colouring does not follow the 5 categories scale of ISO 22324:2022, but a mix of the usual three categories scale (green, yellow, red) and other colours. This has been chosen because the Severity level "Uknown" does not define specific level of severity.

Table 3 — Recommendations for the colours of incident severity level (in RGB scale, saturated) according to Table B1 in ISO 22324:2015

Field	Level	RGB colour
Incident Severity	Unknown	99/101/103
	Minor	110/185/53
	Moderate	244/207/0
	Severe	240/140/17
	Extreme	199/22/30

5.5.3 Scale of impacts

For the damage extent the following rules should apply.

Table 4 — Recommendations on colours for scale of impacts

Field	Level	RGB colour
Scale of Impacts	Unknown / 0	99/101/103
	No damage / 1	0/160/60
	Minor / 2	110/185/53
	Moderate / 3	244/207/0
	Large / 4	240/140/17
	Massive / 5	199/22/30

5.5.4 Incident urgency

For incident urgency the following rules should apply.

Table 5 — Recommendations on colours for incident urgency

Field	Level	RGB colour
Incident urgency	Unknown	99/101/103
	Past	0/160/60
	Future	244/207/0
	Expected	240/140/17
	Immediate	199/22/30

5.5.5 Incident priority

For priority options, the following rules should apply according to the recommendations of ISO/TR 22351:2015 [2].

Table 6 — Recommendations on colours for incident priority

Field	Level	RGB colour
Incident Priority	Priority not assessed / -1	99/101/103
	No estimated priority / 0	0/160/60
	Minor / 1	110/185/53
	Standard priority / 2	244/207/0
	Critical priority / 3	240/140/17
	Extremely critical priority / 4	199/22/30

5.5.6 Human losses

The following colour codes should be used for human losses, especially if the common triage method is used.

Table 7 — Recommendations for use of colours for the case of human losses, with the common triage system

Field	Level	RGB colour
Human Losses	Unknown	99/101/103
	P1 – number of people immediate care	199/22/30
	P2 – number of people urgent care	244/207/0
	P3 – number of people delayed (minor) care	0/160/60
	Dead	0/0/0

Annex A
(informative)

List of critical infrastructure types

A.1 General

This annex provides a list of sectors, subsectors and categories of critical entities types according to the DIRECTIVE 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities and repealing Council Directive 2008/114/EC [1].

A.2 Critical infrastructure types

Table A.1 — EU Directive 2022/2557 [1] suggested list of critical entities

Sector	Subsector	Type of Entity
Energy	Electricity	Electricity undertakings which carry out the function of supply
		Distribution system operators
		Transmission system operators
		Producers
		Nominated electricity market operators
		Electricity market participants providing aggregation, demand response or energy storage services
	District heating and cooling	District heating and cooling
	Oil	Operators of oil transmission pipelines
		Operators of oil production, refining and treatment facilities, storage and transmission
		Central oil stockholding entities
	Gas	Supply undertakings
		Distribution system operators
		Transmission system operators
		Storage system operators
		LNG system operators
		Natural gas undertakings
		Operators of natural gas refining and treatment facilities
	Hydrogen	Operators of hydrogen production, storage and transmission
Transport	Air	Air carriers
		Airport managing bodies
		Traffic management control operators providing air traffic control (ATC) services

Sector	Subsector	Type of Entity
	Rail	Infrastructure managers
		Railway undertakings
	Water	Inland, sea and coastal passenger and freight water transport companies
		Managing bodies of ports including their port facilities and entities operating works and equipment contained within ports
		Operators of vessel traffic services
	Road	Road authorities
		Operators of Intelligent Transport Systems
Banking		Credit institutions
Financial market infrastructures		Operators of trading venues
		Central counterparties
Health		Healthcare providers
		EU reference laboratories
		Entities carrying out research and development activities of medicinal products
		Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2
		Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’)
Drinking water		Suppliers and distributors of water intended for human consumption, excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential or important services
Waste water		Undertakings collecting, disposing or treating urban, domestic and industrial waste water
Digital infrastructure		Internet Exchange Point providers
		DNS service providers
		TLD name registries
		Cloud computing service providers
		Data centre service providers
		Content delivery network providers
		Trust service providers
		Providers of public electronic communications networks or providers of electronic communications services where their services are publicly available

Sector	Subsector	Type of Entity
Public administration		Public administration entities of central governments
		Public administration entities of NUTS level 1 regions
		Public administration entities of NUTS level 2 regions
Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks
Production, processing and distribution of food		Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council (22) which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing

Annex B
(informative)

Template for printed version of the incident report

B.1 General

This annex provides a template structure for the information to be sent in a case of an incident in a critical infrastructure according to the elements of Clauses 4 and 5.

A specific example for three report types (initial report (3.14), update report (3.16) and final report (3.7)) are also provided. This template is only included as a recommendation. The template fits an A4 (ISO 216:2007 [8]) paper size.

B.2 Example of the template structure

Table B.1 — Example for the template structure of incident reporting when printed or depicted on a computer screen

User and incident Identifier					
Incident Report type	Incident ID	Classification level	Linked incident	Linked incident ID	CI Business name
Information 1	Information 1	Information 1	Information 1	Information 1	Information 1
Incident Creation Date/Time (Local)	Report recipients	CI Sector	Person or group reporting		Person authorized
YYYY-MM-DD, Thh:mm:ss	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXXXX		XXXXXXXXX
Contact email	XXXXX@XXXXX	Contact tel	+30 210 21 02 210	Country (code)	e.g. GR
Incident basic information description					
Incident type			Incident certainty		
XXXXXXXX			XXXXXXXX		
Incident Occurrence Date/Time (local)	Area	Latitude (WGS84)	Longitude (WGS84)	Elevation (m)	Radius
YYYY-MM-DD, Thh:mm:ss	Information 1	Information 1	Information 1	Information 1	Information 1
Incident description	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX				
Accessibility status	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX				
Incident hazard and impacts					
Hazard type		Incident severity (a)	Incident urgency (a)	Incident priority (a)	
Information 1		Information 1	Information 1	Information 1	
Impact description (a)			Scale of impacts (a)		
Information 1			Information 1		
CI Service affected	Human losses	Expected external impacts (to other CIs)	Other CI sector affected		Restoration time
Information 1	Information 1	Information 1	Information 1		Information 1
Actions					
Actions in place			Alternative infrastructure for service provision		
Information 1					
Description of the actions					
Resources					
Resources used by the CI					
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX					

(a) For the fields of incident severity, impact description, scale of impacts, incident urgency and incident priority the colour codes in clause 5.5 should be followed.

B.3 Example of an incident and relevant incident reports

Example of a hazard that affects a critical entity, the hypothetical scenario as well as three types of incident reports are provided in order to present an example for demonstrating the use of this document and the printed version.

Hypothetical scenario: An earthquake occurs in Greece. The earthquake affects a large area and power, water and telecommunications service provision has stopped. The state officially announces that the earthquake is of magnitude of M=6.7 located in Southern Greece at 2022/05/10 - 15:05:10 local time. The focal depth of epicentre is estimated at 10km from the first simulations. So far, expected damage is significant based on ground motion modeling, nevertheless nothing is still verified. At this point a critical entity of water provision which is located in the area, reports a service disruption due to the earthquake. The three types of report, an initial report, an update and the closing/cancellation of the incident.

B.3.1 Initial incident report

User and incident Identifier					
Incident Report Type	Incident ID	Classification level	Linked incident	Linked incident ID	CI Business name
Initial report	WPSG - 20220510 - 01 - R	Unclassified			Water Provision Southern Greece (WPSG)
Incident Creation Date/Time (Local)	Report recipients	CI Sector	Person or group reporting		Person authorized
2022-05-10 T15:25:00	Civil protection	Drinking Water, Supplier and distributor of water	Danai Kazantzidou, Head of technical department		Georgios Sakkas, Infrastructure Security Liaison Officer
Contact email	technical@WPSG.gr	Contact tel	+302107710 805	Country (code)	GR
Incident description					
Incident type			Incident certainty		
True incident			SomeWhatConfident		
Incident Occurrence Date/Time (local)	Area	Latitude (WGS84)	Longitude (WGS84)	Elevation (m)	Radius
2022-05-10 T15:05:10	Southern Greece - Tripoli	37.518	22.363	650	30 km
Incident description	An earthquake occurred in the area, approximately at15:00 local time. The earthquake caused significant ground movement which in turn caused the triggering of landslides. Water pipes located in the area of landslides have been broken. SCADA system has recorded a loss of pressure in the water flow. The water pipe that broke provides water only to the west, thus not affecting the town of Tripolis.				
Accessibility status	The road network from the town of Tripoli to the village of Mainalo, close to Mainalo village is closed due to rock falling and landslides in various parts.				
Risk description					
Hazard type		Incident Severity	Incident urgency	Incident priority	
Landslide		Severe	Immediate	Critical priority	
Impact description			Scale of impacts		
Water provision services stopped to the west of town of Tripolis in a radius of 70 km. Approximately 300,000 clients do not have access to drinking water through the water network.			Large		
CI Service Affected	Human losses		Expected external impacts (to other CIs)		Restoration time
Main water pipeline broken	Unknown		Unknown		6 to 12 hours
Actions					
Actions in place			Alternative infrastructure for service provision		
Yes			No		
Description of the actions	First land team has been sent to identify exactly the location and the extent of the problem.				
Resources					
Resources used by the CI					
Internal resources used. Civil protection, fire service and local municipalities have been informed.					

B.3.2 Update incident report

User and incident Identifier					
Incident Report Type	Incident ID	Classification level	Linked Incident	Linked Incident ID	CI Business Name
Update report	WPSG - 20220510 - 01 - U	Unclassified			Water Provision Southern Greece (WPSG)
Incident Creation Date/Time (Local)	Report recipients	CI Sector	Person or group reporting		Person authorized
2022-05-10 T16:10:00	Civil protection	Drinking Water, Supplier and distributor of water	Danai Kazantzidou, Head of technical department.		Georgios Sakkas, Infrastructure Security Liaison Officer
Contact email	technical@WPSG.gr	Contact tel	+302107710 805	Country (code)	GR

Incident description					
Incident type			Incident Certainty		
True incident			HighlyConfident		
Incident Occurrence Date/Time (local)	Area	Latitude (WGS84)	Longitude (WGS84)	Elevation (m)	Radius
2022-05-10 T15:05:10	Southern Greece - Tripoli	37.53	22.364	700	32 km
Incident description	An earthquake occurred in the area, approximately at15:00 local time. The earthquake caused significant ground movement which in turn caused the triggering of landslides. Water pipes located in the area of landslides have been broken. SCADA system has record a loss of pressure in the water flow. The water pipe that broke provides water only to the west, thus not affecting the town of Tripolis.				
Accessibility status	The road network from the town of Tripoli to the village of Mainalo, close to Mainalo village is closed due to rock falling and landslides in various parts.				

Risk description					
Hazard Type		Incident Severity	Incident Urgency	Incident Priority	
Landslide		Moderate	Immediate	Critical priority	
Impact description			Scale of impacts		
Water provision services stopped to the west of town of Tripolis in a radius of 30 km. Approximately 20,000- 40,000 clients do not have access to drinking water through the water network.			Moderate		
CI Service Affected	Human Losses		Expected External Impacts (to other CIs)		Restoration Time
Water pipeline broken, not the main one	Not applicable		Unknown		2 to 6 hours

Actions					
Actions in place			Alternative infrastructure for service provision		
Yes			No		
Description of the actions	Problem identified. Works for the restoration of service have started. Additional personnel and equipment from the CI will be sent in the next 30 minutes.				

Resources
Resources used by the CI
Internal resources used. Civil protection, fire service and local municipalities have been informed.

B.3.3 Final incident report

User and incident Identifier					
Incident Report Type	Incident ID	Classification level	Linked incident	Linked incident ID	CI Business Name
Final report	WPSG - 20220510 - 01 - C	Unclassified			Water Provision Southern Greece (WPSG)
Incident creation Date/Time (Local)	Report recipients	CI Sector	Person or group reporting		Person authorized
2022-05-10 T21:00:00	Civil protection	Drinking Water, Supplier and distributor of water	Danai Kazantzidou, Head of technical department.		Georgios Sakkas, Infrastructure Security Liaison Officer
Contact email	technical@WPSG.gr	Contact tel	+302107710805	Country (code)	GR

Incident description					
Incident type			Incident certainty		
True incident			Highly confident		
Incident Occurrence Date/Time (local)	Area	Latitude (WGS84)	Longitude (WGS84)	Elevation (m)	Radius
2022-05-10 T15:05:10	Southern Greece - Tripoli	37.53	22.364	700	32km
Incident description	Service restored				
Accessibility status	The road network from the town of Tripoli to the village of Mainalo, close to Mainalo village is closed due to rock falling and landslides in various parts.				

Risk description				
Hazard type		Incident severity	Incident urgency	Incident priority
Landslide		Moderate	Past	
Impact description			Scale of impacts	
Water provision services stopped to the west of town of Tripolis in a radius of 30 km. 35,000 clients did not have access to drinking water for approximately 6 hours.			Moderate	
CI Service affected	Human losses		Expected external impacts (to other CIs)	Restoration time
	Not applicable		Unknown	

Actions	
Actions in place	Alternative infrastructure for service provision
Description of the actions	

Resources
Resources used by the CI

Annex C
(informative)

List of potential hazard types

C.1 General

This annex provides an indicative list of event terms that can be used for the Hazard type set of information. The table provided is the OASIS Event Terms [6]. Nevertheless, other terms that are widely accepted can be used.

C.2 OASIS Event Terms list

Table C.1 — OASIS Event Terms [6] adopted in this document

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-000	other	other	Other
OET-001	accumulating ice	safety	Safety; Transport
OET-002	active shooter	criminal activity	Safety; Security
OET-003	administrative action	testing & system activity	Other
OET-004	air hazard	aviation hazard	Meteorological; Transport
OET-005	poor air quality	health hazard	Environmental; Health
OET-006	stagnant air	air hazard	Meteorological
OET-007	aircraft crash	aviation hazard	Transport
OET-008	aircraft incident	aviation hazard	Transport
OET-009	airport closure	aviation hazard	Transport
OET-010	airspace closure	aviation hazard	Transport
OET-011	airspace restriction	aviation hazard	Transport
OET-012	ambulance	health issue	Health
OET-013	animal disease	health issue	Health
OET-014	animal feed	health issue	Health
OET-015	animal health	health issue	Health
OET-016	arctic outflow	temperature hazard	Meteorological
OET-017	ashfall	air hazard; marine; aviation	Geological; Health; Meteorological; Safety; Transport
OET-018	avalanche		Geological
OET-019	aviation hazard	aviation hazard	Transport
OET-020	aviation security	aviation hazard	Transport; Security

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-021	beach hazard	marine	Safety
OET-022	biological	biological hazard	CBRNE
OET-023	blizzard	winter weather	Meteorological
OET-024	blood supply	health issue	Health
OET-025	blowing dust	air hazard	Meteorological
OET-026	blowing snow	winter weather	Meteorological
OET-027	blue-green algae	water hazard	Environmental
OET-028	bomb threat	criminal activity	CBRNE
OET-029	bridge closure	road hazard	Transport
OET-030	bridge collapse	road hazard	Transport
OET-031	building collapse	infrastructure issue	Infrastructure
OET-032	building structure hazard	earthquake	Geological
OET-033	bush fire	fire	Fire
OET-034	cable service issue	utility issue	Infrastructure
OET-035	canal issue	utility issue	Infrastructure
OET-036	chemical fire	fire	CBRNE; Fire
OET-037	chemical hazard		CBRNE
OET-038	chemical smoke		Health; CBRNE
OET-039	child abduction	criminal activity	Safety; Security
OET-040	Civil issue	civil issue	Security
OET-041	civil protest	civil issue	Safety
OET-042	coal gas	utility issue	Infrastructure
OET-043	coastal flood	flood	Meteorological
OET-044	cold	temperature hazard	Meteorological
OET-045	cold weather	winter weather	Meteorological
OET-046	communications service disruption	utility issue	Infrastructure
OET-047	contagious disease	health hazard	Health
OET-048	contaminated water	health hazard	Health
OET-049	contamination		CBRNE; Health
OET-050	criminal activity	criminal activity	Safety
OET-051	cybercrime threat	criminal activity	Safety; Security
OET-052	cyclone	tropical storm	Meteorological

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-053	dam break	flood	Geological; Meteorological
OET-054	dam issue	infrastructure issue	Infrastructure
OET-055	dangerous animal	civil issue	Safety
OET-056	dangerous person threat	criminal activity	Safety
OET-057	debris flow	geophysical	Geological
OET-058	demonstration	testing & system activity	Other
OET-059	dense fog	air hazard	Meteorological
OET-060	dense smoke	air hazard	Meteorological
OET-061	diesel fuel issue	utility issue	Infrastructure
OET-062	disease	health issue	Health
OET-063	disease outbreak	health issue	Health
OET-064	drought	weather	Meteorological
OET-065	drug safety issue	public health	Health
OET-066	drug supply issue	public health	Health
OET-067	dust storm	air hazard	Meteorological
OET-068	dyke break	flood	Meteorological
OET-069	earthquake	earthquake	Geological
OET-070	electronic infrastructure issue	infrastructure issue	Infrastructure
OET-071	emergency responder incident	criminal activity	Safety
OET-072	emergency responder threat	criminal activity	Safety
OET-073	emergency support facilities incident	infrastructure issue	Infrastructure
OET-074	emergency support services incident	infrastructure issue	Infrastructure
OET-075	emergency telephone outage	infrastructure issue	Infrastructure
OET-076	environmental issue	environment	Environmental
OET-077	explosion threat	civil issue	CBRNE
OET-078	falling object	safety hazard	Safety
OET-079	fire	fire	Fire
OET-080	flash flood	flood	Meteorological
OET-081	flash freeze	winter weather	Meteorological

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-082	flood	flood	Meteorological
OET-083	fog	air hazard; winter weather	Meteorological
OET-084	food contamination	biological hazard	Health
OET-085	food safety issue	public health	Health
OET-086	food supply issue	public health	Health
OET-087	forest fire	fire	Fire
OET-088	freeze	winter weather	Meteorological
OET-089	freezing drizzle	winter weather	Meteorological
OET-090	freezing rain	winter weather	Meteorological
OET-091	freezing spray	winter weather; marine	Meteorological
OET-092	frost	winter weather	Meteorological
OET-093	fuel issue	utility issue	Infrastructure
OET-094	geophysical issue	geological	Geological
OET-095	grass fire	fire	Fire
OET-096	hail	severe weather	Meteorological
OET-097	hazardous seas	marine	Transport
OET-098	health issue	health issue	Health
OET-099	heat	temperature hazard	Meteorological
OET-100	heating oil issue	utility issue	Infrastructure
OET-101	high seas	marine	Meteorological
OET-102	high surf	marine	Meteorological
OET-103	high tide	marine	Transport
OET-104	high water	utility issue; marine	Infrastructure; Transport
OET-105	home crime	criminal activity	Safety
OET-106	humidity issue	temperature hazard	Meteorological
OET-107	hurricane	tropical storm; tropical cyclone	Meteorological
OET-108	ice	winter weather	Meteorological
OET-109	ice pressure issue	ice issue	Meteorological
OET-110	ice storm	winter weather	Meteorological
OET-111	iceberg	ice issue	Meteorological
OET-112	industrial crime	criminal activity	Safety
OET-113	industrial facility issue	safety hazard	Safety

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-114	industrial fire	fire	Fire
OET-115	infrastructure issue	infrastructure	Infrastructure
OET-116	internet service issue	utility issue	Infrastructure
OET-117	lake effect snow	winter weather	Meteorological
OET-118	lake wind	air hazard	Meteorological
OET-119	landline service issue	utility issue	Infrastructure
OET-120	landslide	geophysical	Geological
OET-121	law enforcement issue	civil issue	Security
OET-122	levee break	flood	Meteorological
OET-123	lightning	thunderstorm; severe weather	Meteorological
OET-124	limited visibility	air hazard	Transport
OET-125	low tide	marine	Transport
OET-126	low water	utility issue; marine	Infrastructure; Transport
OET-127	low water pressure	utility issue	Infrastructure
OET-128	meteoroid	space	Transport
OET-129	meteorological issue	meteorological	Meteorological
OET-130	missile threat	national hazard	CBRNE
OET-131	missing child	safety hazard	Safety
OET-132	missing person	safety hazard	Safety
OET-133	mobile communication issue	utility issue	Infrastructure
OET-134	monsoon	weather	Meteorological
OET-135	mudslide	geophysical	Geological
OET-136	natural gas	utility issue	Infrastructure
OET-137	network message notification	testing & system activity	Other
OET-138	nuclear power plant issue	infrastructure issue	Infrastructure; CBRNE
OET-139	oil leak	beach hazard, environmental	Environmental
OET-140	oil spill	beach hazard, environmental	Environmental
OET-141	overland flood	flood	Meteorological
OET-142	pipeline rupture	utility issue	Infrastructure

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-143	plant health issue	health issue	Health
OET-144	heavy rain	health issue	Health
OET-145	pollen	health issue	Health
OET-146	potable water issue	utility issue; water hazard	Infrastructure
OET-147	power outage	infrastructure issue	Infrastructure
OET-148	power utility issue	utility issue	Infrastructure
OET-149	product safety	safety hazard	Safety
OET-150	public facility issue	infrastructure issue	Infrastructure
OET-151	public health	health issue	Health
OET-152	public service issue	infrastructure issue	Infrastructure
OET-153	public transit issue	infrastructure issue	Transport
OET-154	pyroclastic flow	volcano hazard	Geological
OET-155	radiation issue	radiological hazard	CBRNE
OET-156	radio transmitter	safety hazard	Infrastructure
OET-157	radioactive material release	radiological hazard	CBRNE
OET-158	radiological fire	fire	CBRNE; Fire
OET-159	railway issue	infrastructure issue	Transport
OET-160	rain	weather	Meteorological
OET-161	rapid ice closing of water passage	ice issue	Transport
OET-162	red tide	health issue; marine issue	Health
OET-163	rescue	rescue	Rescue
OET-164	retail crime issue	criminal activity	Safety
OET-165	rip current issue	beach hazard	Safety
OET-166	road closure	road hazard	Transport
OET-167	road issue	road hazard	Transport
OET-168	road vehicle accident	road hazard	Transport
OET-169	rogue wave	marine	Geological
OET-170	safety	safety hazard	Safety
OET-171	sandstorm	air hazard; weather	Meteorological
OET-172	satellite debris	space	Other
OET-173	satellite service	utility issue	Infrastructure

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-174	school bus issue	infrastructure issue	Transport
OET-175	school closing	infrastructure issue	Infrastructure
OET-176	school lockdown	infrastructure issue	Infrastructure
OET-177	search	search	Rescue
OET-178	security	security	Security
OET-179	sewer	utility issue	Infrastructure
OET-180	shoreline threat	beach hazard	Safety
OET-181	sinkhole	safety hazard	Safety
OET-182	sleet	winter weather	Meteorological
OET-183	smoke	air hazard	Meteorological; Transport; Health
OET-184	snow	winter weather	Meteorological
OET-185	snowstorm	weather	Meteorological
OET-186	space debris	space	Other
OET-187	space weather	space	Other
OET-188	squall	weather; marine	Meteorological
OET-189	storm	weather; marine	Meteorological
OET-190	storm drain	utility issue	Infrastructure
OET-191	storm surge	weather; flood	Meteorological
OET-192	structure fire	fire	Fire
OET-193	swells	marine	Safety; Transport
OET-194	telephone	utility issue	Infrastructure
OET-195	terrorist incident	criminal activity	Safety
OET-196	thin ice	safety	Safety
OET-197	thunderstorm	weather	Meteorological
OET-198	tornadic waterspout	severe weather	Meteorological
OET-199	tornado	severe weather; tornado	Meteorological
OET-200	toxic plume	contamination hazard	CBRNE
OET-201	toxic spill	contamination hazard	CBRNE
OET-202	traffic	road hazard	Transport
OET-203	transport issue	transport	Transport
OET-204	tropical depression	tropical storm; tropical cyclone	Meteorological
OET-205	tropical storm	weather; tropical cyclone	Meteorological

OASIS Event Code	OASIS Event Term	Grouping	CAP Category Code(s)
OET-206	tsunami	marine	Geological
OET-207	typhoon	tropical cyclone	Meteorological
OET-208	ultraviolet	safety	Safety
OET-209	utility	utility issue	Infrastructure
OET-210	vehicle crime	criminal activity	Safety
OET-211	volcanic activity	volcano hazard	Geological
OET-212	volcanic eruption	volcano hazard	Geological
OET-213	volcanic lahar	volcano hazard	Geological
OET-214	volcanic lava	volcano hazard	Geological
OET-215	waste management	utility issue	Infrastructure
OET-216	water	utility issue; water hazard	Geological; Transport
OET-217	water main break	utility issue; water hazard	Infrastructure
OET-218	waterspout	marine	Meteorological
OET-219	weather	weather	Meteorological
OET-220	wildfire	fire	Fire
OET-221	wind	air hazard	Meteorological
OET-222	wind change	air hazard	Meteorological
OET-223	wind chill	temperature hazard	Meteorological
OET-224	wind shear	air hazard	Meteorological
OET-225	winter storm	winter weather	Meteorological
OET-226	winter weather	weather	Meteorological

Bibliography

[1] DIRECTIVE 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[2] ISO/TR 22351:2015, *Societal Security — Emergency management — Message structure for exchange of information.*

[3] [OASIS EDXL-SitRep] *Emergency Data Exchange Language Situation Reporting (EDXL-SitRep) Version 1.0*. Edited by Rex Brooks, Timothy Grapes, Werner Joerg, and Jeff Waters. 06 October 2016. OASIS Committee Specification 02. http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/cs02/edxl-sitrep-v1.0-cs02.html. Latest version: http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html.

[4] JESIP M/ETHANE model. Joint Emergency Services Interoperability Programme.

[5] FEMA, US Department Homeland Security. *Developing and Maintaining Emergency Operations Plans, Cophrehensive Preparedness Guide (CPG) 101, Version 2.0, November 2010*.

[6] OASIS Event Terms List Version 1.0 (https://docs.oasis-open.org/emergency/etl/v1.0/etl-v1.0.html).

[7] START – Simple Triage And Rapid Treatment. Newport Beach (CA.) Fire & Marine Department (1983).

[8] EN ISO 216:2007, *Writing paper and certain classes of printed matter — Trimmed sizes — A and B series, and indication of machine direction.*

[9] CEN ISO/TR 22411, *Ergonomics data for use in the application of ISO/IEC Guide 71:2014 (ISO/TR 22411:2021).*