|  |  |  |
| --- | --- | --- |
| IHTSDO Release Management Critical Incident process | | |
|  | | |
| Date | 20160201 | |
| Version | | 0.2 |
| Status: | | Draft |

Amendment History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Editor** | **Comments** |
| 0.1 | 20160201 | Andrew Atkinson | Creation of draft Release Management process |
| 0.2 | 20160217 | Andrew Atkinson | Updated after internal review |
|  |  |  |  |

Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Approver** | **Comments** |
|  | YYYYMMDD |  |  |

Future Review Timetable

|  |  |  |
| --- | --- | --- |
| **Review date** | **Responsible owner** | **Comments** |
| YYYYMMDD | Person/group responsible | Summary of action |
|  |  | (remove or add rows if necessary) |

© International Health Terminology Standards Development Organization 2016. All rights reserved.

Table of Contents

1 Introduction 4

2 Scope 4

2.1 In Scope 4

2.2 Out of Scope 4

3 Glossary of Terms 5

4 Definition of Critical Incident 5

5 Critical Incident Framework 6

6 Critical Incident Management Stages 7

6.1 Stage 1: Report 8

6.2 Stage 2: Assess 8

6.3 Stage 3: Response 8

6.4 Stage 4: Recovery 8

6.5 Stage 5: Investigation 8

6.6 Stage 6: Learning and Prevention 8

7 Critical Incident Process 9

Appendix A: Categories of Critical Incidents 10

Appendix B: Assessing Severity of Critical Incidents 11

# Introduction

The IHTSDO Release Management Critical Incident process defines the procedure for managing Critical Incidents within the scope of IHTSDO Release Management. It is important to manage Critical Incidents and be prepared when they occur, in order to ensure that the IHTSDO products and services are maintained and that Members and consumers are therefore not adversely impacted. The IHTSDO Release Management Critical Incident process defines the procedure that IHTSDO would implement in the case of a Critical Incident, in order that all stakeholders are aware of what to do and/or expect. It may also refer to other Critical Incident Management documentation that can be used to inform how Critical Incidents are managed.

# Scope

## In Scope

Critical Incidents as defined in section 4 which impact on the operations of the IHTSDO organization, the delivery and quality of IHTSDO products are in scope. The IHTSDO Release Management Critical Incident process does not relate to an individual; it relates to the IHTSDO organization and its products and services.

## Out of Scope

Out of scope are incidents that do not impact directly or indirectly on IHTSDO products or its partners. Incidents impacting the following examples are regarded as out of scope except where they may indirectly create a potential risk for IHTSDO its products or partners:

* Management of assets outside of IHTSDO control
* Management of data breaches outside of IHTSDO
* Disruption to the delivery of healthcare i.e. hospitals and clinical data
* Disruption to the function of Healthcare Delivery Organizations.
* Disruption to organizations linked to IHTSDO that do not impact the operation of the IHTSDO
* Vendors and suppliers linked to IHTSDO that do not impact the products of the IHTSDO or have not been impacted by the products of the IHTSDO.

# Glossary of Terms

This following table is a glossary of terms being used; this will be updated and expanded as more items are incorporated.

**Table 1 – Glossary of Terms**

| **Term** | **Definition** |
| --- | --- |
| Critical | This is the ranking of an event that has or will impact the IHTSDO organization and the IHTSDO products and services. As the event is critical in nature it requires immediate action to be taken. |
| Incident | This is the failure of an existing identified risk control process or the occurrence of an event or outcome from an uncontrolled or not previously identified risk. An event that has or will occur that will impact the operation of IHTSDO organization, products and services and requires immediate action to mitigate damage to the IHTSDO organization, clients or customers. |
| Product | This is an outcome of IHTSDO for example, but not limited to; SNOMED CT, mappings, translations, tooling. |
| Information Asset | Body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively |

# Definition of Critical Incident

A Critical Incident is an event that has or will affect the IHTSDO core operations, and/or interrupts or reduces the quality of IHTSDO products or services that fall under the remit of Release Management within IHTSDO.

Critical Incidents can be further distinguished from significant and routine incidents in that a Critical Incident:

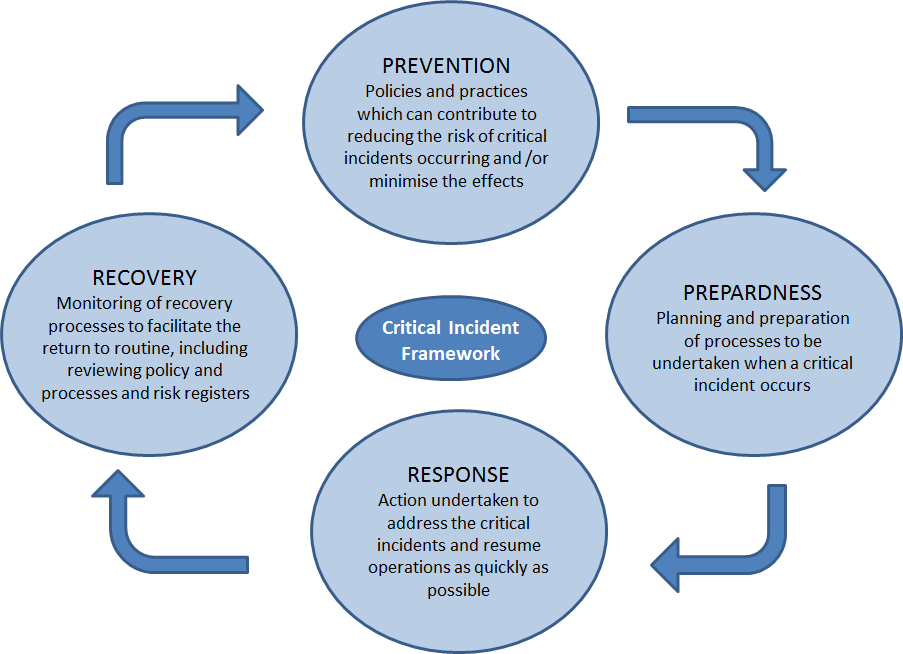
* significantly disrupts the operations of IHTSDO, or a major part of it, putting at risk the efficient and effective provision of its products and services;
* impacts critical IT service availability, with a potential down time of greater than 2 hours;
* has the potential to impact clinical safety for our customers;
* has a significant impact on the reputation of IHTSDO;

The objective of Critical Incident Management is to restore normal operations (whether this be products or services) as quickly as possible with the least possible impact on IHTSDO, product or the Members/users, at a cost-effective price.

# Critical Incident Framework

The following diagram illustrates the main process steps in managing Critical Incidents in the IHTSDO. The following proposed framework defines four (4) main areas: Prevention, Preparedness, Response and Recovery.

**Diagram 1 – Critical Incident Framework**



1. **Prevention** is the policies and practices that contribute to reducing the likelihood of a Critical Incident occurring; and the management of risk to ensure that Critical Incident can be prevented.
2. **Preparedness** is the Planning and preparation of process to be undertaken when a Critical Incident occurs; this includes the Critical Incident Emergency Response Manual and the testing of Response Plans to ensure they are effective when a Critical Incident Occurs.
3. **Response** is the actions that are undertaken to address the Critical Incident and resume operations as quickly as possible, this is determined by the Critical Incident Emergency Response Manual.
4. **Recovery** is the monitoring of recovery processes to resume operations.

# Critical Incident Management Stages

When a Critical Incident occurs it is important that there is a structured approach to managing the Critical Incident. As part of the IHTSDO Release Management Critical Incident process stages have been defined that are to be followed when a critical incident occurs. Stages describe how to assess and respond to the critical incident in line with the overall Critical Incident Policy Framework. The following flow chart and explanation below defines a high level process for management of Critical Incidents. The Process section below defines the full and detailed process for management of Critical Incidents.

**Diagram 2– Critical Incident Process Flow Chart**

Stage 1 Report

Stage 2 Assess

Stage 3 Response

Stage 4 Recovery

Stage 5 Investigation

Stage 6 Learning and Prevention

Critical Incident Occurs

## Stage 1: Report

A Critical Incident occurs and is reported via the organization’s internal reporting mechanism to the organization’s central recording system and via information flows from distribution centres; or via or member of staff, in the absence of both. Incident details are communicated internally as necessary. The category of Critical Incidents can be found in Appendix A, this table will be used when reporting a Critical Incident.

## Stage 2: Assess

Assess the actual Critical Incident severity (using Table 3 in Appendix B). A Critical Incident will often have multiple aspects, considering all these aspects (see Table 4 in Appendix C) decide the level of severity. The initial assessment of a Critical Incident should be performed quickly, even when all facts may not be available.

In assessing the severity of a Critical Incident, consider the outcome of the incident in terms of harm to people / resources / environment / reputation and quality as defined in Appendix C Table 4 – Example Assessment of Critical Incidents.

## Stage 3: Response

Once the level of severity has been assessed; determine the response to the Critical Incident. The Response Plan will be determined using the Critical Incident Emergency Response Manual. The Response Plan identifies the owner of the implementation of the response plan.

## Stage 4: Recovery

Test recovery from the Critical Incident; if the implemented response is not working go back to Stage 2. Recovery should resume normal operations

## Stage 5: Investigation

Initiate Critical Incident investigation using the Critical Incident Investigation Process (to be defined). Following investigation re-consider in the light of further information whether it is appropriate to report to external organizations.

## Stage 6: Learning and Prevention

Determine learning from the Critical Incident and communicate them within the organization and with the appropriate regional / national bodies. Following the outcome and learning from the investigation, determine what further action should be taken, for example considering whether it requires investment in technology, or to be entered on the risk register, and/or what if any further organization-wide actions are required.

# Critical Incident Process

Solution consumed

Solution consumed

Communications consumed

Communications consumed

Communications plan agreed and implemented:

* All impacted users should be informed of the action taken
* Ensure the Incident is reported in detail
* Ensure all impacts are reported
* Ensure the reasons for taking the agreed action are carefully documented and explained in full
* Ensure all changes (both content & technical) included in the Recall/Update release are detailed in full

**IHTSDO**

Appropriate action agreed between IHTSDO and Terminology Release Advisory Group (T.R.A.G.), Tested & implemented.

For example, if the product/service has already been consumed, publish a Recall release, otherwise publish an Update release

* Ensure patient safety is considered paramount
* Ensure all impacted users are identified and considered
* Ensure all SLA’s are met, & action taken in a timely manner (according to the Severity of the Incident)
* Detailed plan of action to be created and approved

Detailed analysis + severity assigned

Standard Incident management process

Incident analyzed + prioritized – Critical Incident?

Incident reported

**AFFILIATES**

**MEMBERS**

**T.R.A.G.**

# Appendix A: Categories of Critical Incidents

The following table defines the categories of Critical Incidents and describes examples in which these would become Critical Incidents:

**Table 2 – Critical Incident Categories**

| **Category** | **Example of critical incident** |
| --- | --- |
| **Technology** | * Server and Local Area Network failure of greater than 2 hours * Failure of distribution of a product * Undetected errors in a product * Loss of back-ups * Telecommunications failure * Loss of backups * Information security breaches |
| **Information Asset** | * Failure to transfer data according to ISO standards (27001 and 27002) * Person identifiable data transfer and sharing * Data dissemination patient confidentiality compromised (non-compliance with Data Protection Act 1998) * Data loss * Incorrect coding of IHTSDO product data * Changes in data outside of IHTSDO control * Inappropriate use of data and data transfer |
| **Product Service** | * Whole or part of Service is unavailable * Adverse clinical outcome consequent to or associated with an error in the clinical use of a SNOMED CT code or conceptual interpretation * Failure to correctly implement SNOMED CT results in incorrect or inappropriate information being presented * Failure to distribute products * Undetected errors in products * Failure of the update and deprecation of systems * Failure of translation and distribution of systems * Intentional and malicious changes in the SNOMED CT Codes |

# Appendix B: Assessing Severity of Critical Incidents

The assessment of Critical incidents is important as it determines the severity on the IHTSDO organization, products and services. The ranking of critical Incidents will determine the level of response that will be implemented. There are three (3) main rankings of critical incidents – Catastrophic, Major and Moderate.

The following table defines the severity of critical incidents and takes into account near misses and warnings.

*NB: There will be instances where an incident is a near miss or a warning to IHTSDO and would be investigated to ensure that process are in place to ensure that do not become a Critical Incident.*

**Table 3 – Severity of Critical Incidents**

|  |  |
| --- | --- |
| **Severity of critical incident** | **High Level Descriptors** |
| **Catastrophic** | Incident with widespread implications to operations |
| **Major** | Significant disruption to operations |
| **Moderate** | Minor disruption to operations |
|  | |
| **Near Miss** | No interruption to operations or near miss |
| **Warning** | No critical outcome but risk potential evident |