

ISO/IEC JTC 1/SC 27  
IT Security techniques  
Secretariat: DIN (Germany)

**Replaces:** N 11973

**Document type:** Working Draft Text

**Title:** WG4N0234\_3rdWD\_27035-3\_20130708

**Status:** As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

PLEASE submit your comments on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27> **by the due date 2013-09-13.**

Secretariat's note:

This request for comments is also concurrently being circulated as WG 4 document N0234 for test purposes ONLY as part of the WG 4 Livelink trial via the Working Group Consultation application accessible at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

For the test purposes the National Bodies and liaison organizations of SC 27/WG 4 are kindly invited to send their responses to the hereby attached document via the above-mentioned WG 4 Working Group Consultation application.

Any responses received are greatly appreciated and will be taken into account when assessing the trial results and preparing a report for consideration at the next SC 27 Heads of Delegation meeting in Incheon, Republic of Korea, 24<sup>th</sup> October 2013.

**Date of document:** 2013-07-12

**Source:** Project editors

**Expected action:** COMM

**Action due date:** 2013-09-13

**No. of pages:** 1 + 1 + 48

**Email of secretary:** [krystyna.passia@din.de](mailto:krystyna.passia@din.de)

**Committee URL:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**ISO/IEC JTC 1/SC 27/WG 4**  
**Security controls and services**  
**Secretariat: SABS (South Africa)**

**Replaces:** N 78

**Document type:** Request for comments

**Title:** Text 3rdWD 27035-3 - Text for ISO/IEC 3rd WD 27035-3, – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations

**Status:** As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

A Working group consultation will be created for submissions to this request. Submissions should be sent directly via the SC 27/WG 4 commenting website at <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4> before the action due date.

A request for review and comment will be issued in parallel by SC 27 as SC 27 N12672.

**Date of document:** 2013-07-11

**Source:** Editors

**Expected action:** COMM

**Action due date:** 2013-09-13

**No. of pages:** 1 + 48

**Email of secretary:**

**Committee URL:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

ISO/IEC JTC 1/SC 27 N **12672**

Date: 2012-07-1

**ISO/IEC WD 27035-3.3**

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

**Information technology — Security techniques — Information security  
incident management — Part 3: Guidelines for incident response  
operations**

*Élément introductif — Élément central — Partie 3: Titre de la partie*

Document type: International Standards  
Document subtype:  
Document stage: (20) Preparatory  
Document language: E

D:\ISO\isomacroserver-  
prod\temp\DOCX2PDFISOTC\DOCX2PDFISOTC.Iliadmin@srvweb23\_749\15648705\_1.doc STD Version  
2.1c2

### Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27  
DIN German Institute for Standardization  
DE-10772 Berlin

Tel. + 49 30 2601 2652  
Fax + 49 30 2601 4 2652  
E-mail [krystyna.passia@din.de](mailto:krystyna.passia@din.de)

Web <http://www.jtc1sc27.din.de/en> (public web site)  
<http://isotc.iso.org/isotcportal/index.html> (SC27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

# Contents

Page

1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Overview .....	3
4.1	Objectives .....	3
5	Incident management phases .....	4
5.1	Detection and reporting .....	4
5.1.1	Event detection .....	4
5.1.2	Event reporting .....	4
5.2	Assessment and decision .....	6
5.2.1	Assessment and initial decision by the PoC .....	6
5.2.2	Assessment and incident confirmation by the IRT .....	8
5.3	Responses .....	9
5.3.1	Immediate responses .....	9
5.3.2	Assessment of control over information security incidents .....	12
5.3.3	Later responses .....	12
5.3.4	Responses to crisis situations .....	13
5.3.5	Information security investigation analysis .....	13
5.3.6	Communications .....	15
5.3.7	Escalation .....	16
5.3.8	Activity logging and change control .....	16
6	Incident response teams (IRT) organization .....	16
6.1	Overview .....	16
6.2	IRTs types and roles .....	Error! Bookmark not defined.
6.3	IRT staffs .....	18
7	Incident response operations .....	19
7.1	Incident criteria .....	19
7.2	Incident response processes .....	20
7.3	Detection .....	21
7.4	Incident response .....	22
7.4.1	Pre-response .....	22
7.4.2	Responses .....	22
7.5	Assessment and decision .....	23
7.6	Reporting and post-operation .....	Error! Bookmark not defined.
8	General example of incident response .....	25
8.1	Denial of Service (DoS) .....	25
8.2	Malicious code .....	25
8.3	Information gathering .....	25
8.4	Inappropriate usage .....	26
8.5	Unauthorized access .....	26
Annex A	(informative) Example of the incident criteria based on computer security events and incidents .....	27
A.1	Computer security events and incidents .....	27
A.1.1	Fundamental incident criteria .....	Error! Bookmark not defined.
A.1.2	Impacts according to each incidents types .....	27
A.1.3	Damage scale of incidents .....	28
A.1.4	Importance of the Information/system .....	28
A.2	Incident alarm level .....	28

<b>Annex B (informative) Example information security event, incident and vulnerability reports and forms .....</b>	<b>29</b>
<b>B.1 Introduction .....</b>	<b>29</b>
<b>B.2 Example items in records .....</b>	<b>29</b>
<b>B.2.1 Example items of the record for information security event .....</b>	<b>29</b>
<b>B.2.2 Example items of the record for information security incident .....</b>	<b>30</b>
<b>B.2.3 Example items of the record for information security vulnerability.....</b>	<b>31</b>
<b>B.3 How to use forms.....</b>	<b>31</b>
<b>B.3.1 Format of date and time .....</b>	<b>31</b>
<b>B.3.2 Notes for completion .....</b>	<b>31</b>
<b>B.4 Example forms .....</b>	<b>33</b>
<b>B.4.1 Example form for information security event report.....</b>	<b>33</b>
<b>B.4.2 Example form for information security incident report .....</b>	<b>34</b>
<b>B.4.3 Example form for information security vulnerability report.....</b>	<b>40</b>

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27035-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27035 consists of the following parts, under the general title *Information technology - Security techniques — Information security incident management*:

*Part 1: Principles of Incident Management*

*Part 2: Guidelines to Plan and Prepare for Incident Response*

*Part 3: Guidelines for Incident Response Operations*

## Introduction

The organizational structures for information security vary depending on the size and business field of enterprises and organizations. As various and numerous network incidents (e.g. intrusion and hacking) occur and the number of incidents keeps increasing, higher concerns on information security have been raised by enterprises. However, it is not easy to manage the networks and systems securely, and to handle various types of attacks (such as DoS, Worms and viruses) with network security equipment such as Firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

In order to guarantee protection of information and to handle incidents efficiently, dedicated organization is required. However, it is not easy to establish incident response teams (IRTs), and operate tasks of IRTs such as monitoring, detection, analysis, etc. In addition, it requires proper monitoring, detection, analysis, and response activities for the collected data or security events.

Therefore, this International Standard provides guidance on information security incident management in Clause 5 to Clause 8. The clauses consist of several sub-clauses, which include detailed incident response operations.



# Information technology — Security techniques — Information security incident management — Part 3: Guidelines for incident response operations

## 1 Scope

This International Standard provides the guidelines for incident management, response and incident response team (IRT) operations. It also includes the following:

- a) Basic roles and responsibilities of the IRT staff
- b) Practical incident response activities (Monitoring, Detection, Assessment, Analysis, Response, Report and Lessons Learnt).

The principles given in this International Standard are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this International Standard according to their type, size and nature of business in relation to the information security risk situation. This International Standard is also applicable to external organizations providing information security incident management services.

## 2 Normative references

The following referenced documents are indispensable for the application 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/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27035-1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

ISO/IEC 27035-2, *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to Plan and Prepare for Incident Response*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

### 3.1

#### **Incident Response Teams**

##### **IRT**

a team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle.

NOTE 1 to entry: The IRT as described in this International Standards is an organizational function that covers the process for information security incidents and is focused mainly on IT related incidents. Other common functions (with similar abbreviations) within the incident handling may have a slightly different scope and purpose. The following are commonly used abbreviations, though not exactly the same:

- CERT®: A Computer Emergency Response Team mainly focuses on Information and Communications Technology (ICT) incidents. There may be other specific national definitions for CERT®.
- CSIRT: A Computer Security Incident Response Team is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. These services are usually performed for a defined constituency, which could be a parent entity such as a corporation, governmental organization, or educational organization; a region or country; a research network; or a paid client.

### 3.2

#### **information security incident**

one or multiple related and identified information security events that may compromise operations

### 3.3

#### **information security event**

occurrence indicating a possible breach of information security, policy or failure of controls

### 3.4

#### **information security incident management**

exercise of a consistent and effective approach to the handling of information security incidents

### 3.5

#### **incident handling**

actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents

### 3.6

#### **incident response**

actions taken to protect and restore the normal operational conditions of an information system and the information stored in it when an information security incident occurs

[Adapted from ISO/IEC 3rd WD 27039]

### 3.7

#### **Point of Contact**

##### **PoC**

Previously-identified person and/or department serving as the coordinator or focal point of information concerning a specific resource, through whom communication regarding the specific resource should take place

### 3.8

#### **information security investigation**

application of investigation and analysis techniques to capture, record and analyse information security incidents

### 3.9

#### **Coordinated Universal Time**

##### **UTC**

time scale which forms the basis of a coordinated radio dissemination of standard frequencies and time signals; it corresponds exactly in rate with international atomic time, but differs from it by an integral number of seconds

**3.10****Telnet**

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

**3.11****X.25**

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

**3.12 Abbreviated terms**

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
DoS	Denial of service
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
FTP	File transfer Protocol
HTTP	HyperText Transfer Protocol
IDS	Intrusion detection system
IPS	Intrusion prevention systems
ISDN	Integrated Services Digital Network
IP	Internet Protocol
ICMP	Internet Control Message Protocol
OSPF	Open Shortest Path First
PBX	Private Branch eXchange
RIP	Routing Information Protocol
SNMP	Simple Network Management Protoco
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

**4 Overview****4.1 Objectives**

As the computer and communication technologies continuously advances, types of cyber threats are also evolving that make the cyber information more vulnerable than before. Today, many IT organizations are creating separate security divisions or teams to tactically address the concern. The main role of those organizations is focused on information security and responses to cyber threats and cyber attacks. In addition

to those organizations, IRTs consisting of incident response experts are required to manage various incidents efficiently. Thus, practical guidelines for IRTs on management, operation, and response should be provided. This standard provides the role of an IRT, qualification and responsibilities of IRT members, incidents response procedures and operation, etc.

This International Standard is intended to provide the guidelines for efficient incident management, planning, preparing response and practical operation along with ISO/IEC 27035-1 and ISO/IEC 27035-2.

## 5 Incident management operational phases

### 5.1 Detection and reporting

#### 5.1.1 Event detection

Information security events could be detected directly by a person or persons noticing something that gives cause for concern, whether technical, physical or procedural related. Detection could be, for example, from fire/smoke detectors or intruder (burglar) alarms, with the alerts notifying at pre-designated locations for human action. Technical information security events could be detected by automatic means, for example, alerts made by audit trail analysis facilities, firewalls, intrusion detection systems, and anti-malicious code (including viruses) tools, in each case stimulated by pre-set parameters.

Possible information security event detection sources include the following:

- a) users,
- b) line managers and security managers,
- c) customers,
- d) IT department, including Network Operations Center and Security Operations Center (through 2<sup>nd</sup> level support),
- e) IT help desk (through 1<sup>st</sup> level support),
- f) managed service providers (including ISPs, telecommunication service providers, and suppliers)
- g) IRTs,
- h) other units and staff that may detect anomalies during their daily work,
- i) mass media (news paper, television, etc.), and
- j) websites (public security information websites, websites by security researchers, defacement archive websites, etc.);

#### 5.1.2 Event reporting

Whatever the source of the detection of an information security event, the person notified by automatic means, or directly noticing something unusual, is responsible for initiating the detection and reporting process. This could be any member of an organization's personnel, whether permanent or contracted personnel.

The person should follow the procedures and use the information security event reporting form, specified by the information security incident management scheme (See ISO/IEC 27035-2), to bring the information security event to the attention of the PoC and management. Accordingly, it is essential that all personnel are well aware of, and have access to, the guidelines for reporting the different types of possible information security events. This includes the format of the information security event reporting form and details of the personnel who should be notified on each occasion (all personnel should at least be aware of the format of the

information security incident reporting form, to aid their understanding of the scheme). It should be noted that fixed telephones, cordless telephones and mobile telephones, without being safeguarded for tapping, are considered not safe. When dealing with highly confidential or secret information, the additional safeguards should be taken.

The following information can be used as the basis for an incident tracking system form:

- time/date for detection,
- observations, and
- contact information (optional).

The completed form (either paper-based or electronic) should be used by IRT personnel only when registering information security events (possibly incidents) or vulnerabilities in the Incident Tracking System. It is more crucial to obtain knowledge/reports of a suspected/experienced/detected information security event than being complete with all information.

Information security event (possibly incident) tracking should be supported, whenever possible, by an automated application. The use of an information system is essential to force personnel to follow established procedures and checklists. It is also extremely helpful to keep track of “who did what and when”, details that could be missed by mistake during an information security event (possibly incident).

How an information security event is handled is dependent upon what it is, and the implications and repercussions that may flow from it. Thus, the person reporting an information security event should complete the information security event reporting form, with as much narrative and other information as is readily available at the time, liaising with his/her local manager if necessary. That form should be securely communicated to the designated PoC, with a copy to the responsible IRT. The PoC should preferably provide a 24-hour service for 7 days per week. Annex B shows an example template for the information security event reporting form.

The IRT should appoint one team member or delegate per shift to be responsible for all incoming reports via e-mail, phone, fax, automated information sharing programs, forms and direct conversation. This responsibility may rotate between team members on a weekly basis. The appointed team member makes the assessment and takes proper actions to inform responsible and involved parties as well as resolve the information security incident.

It is emphasized that not only accuracy, but also timeliness, is important in the content filled in the information security event reporting form. It is not good practice to delay the submission of a reporting form in order to improve the accuracy of its content. If the reporting person is not confident with the data in any field on the reporting form, it should be submitted with appropriate notation, and revisions communicated later.

Automated information sharing data formats (IETF RFC 5070) and protocols (IETF RFC 6545, IETF RFC 6546) provide a confidence rating with the data shared. The confidence rating combined with information on the organization providing the data should be considered to determine the accuracy and valuation of the information provided.

It should also be recognized that some reporting mechanisms (e.g. e-mail and automated information sharing protocols) are themselves visible targets for attack. When problems exist, or are considered to exist, with the electronic reporting mechanisms (e.g. e-mail), alternative means of communication should be used. This includes when it is thought possible that the system is under attack and unauthorized people could read reporting electronic forms. Alternative means could include in person, by telephone or text messaging. Such alternative means should be used particularly when it becomes evident early in an investigation that an information security event appears likely to be classified as an information security incident, particularly one that may be significant.

Whilst in many cases an information security event has to be reported onwards for action by the PoC, there may be occasions where an information security event is handled locally, possibly with the help of local management. It is advisable that local management be trained to make the same assessment as the IRT and

take similar/same countermeasures as well as use the same incident tracking system, in order to successfully use locally resources. This will prevent the IRT from doing duplicate work .

An information security event may be quickly determined as a false alarm, or it may be resolved to a satisfactory conclusion. In such cases a reporting form should be completed and forwarded to local management, to the PoC and to the IRT for recording purposes, i.e. into the information security event/incident/vulnerability database. In such circumstance, the person reporting closure of an information security event may be able to complete some of the information required for the information security incident reporting form – if this is the case then the information security incident reporting form should also be completed and forwarded. The use of automatic tools can assist with completion of some fields, for example, time stamps. It can also assist with the sharing/transfer of necessary information.

## **5.2 Assessment and decision**

### **5.2.1 Assessment and initial decision by the PoC**

The receiving person in the PoC should acknowledge receipt of the completed information security event reporting form, enter it into the information security event/incident/vulnerability database, and review it. He/she should seek any clarification from the person reporting the information security event, and collect any further information required and known to be available, whether from the reporting person or elsewhere. Then, the PoC should conduct an assessment to determine whether the information security event should be classified as an information security incident or is in fact a false alarm (including through use of the organization's agreed incident classification scale). If the information security event is determined to be a false alarm, the information security event reporting form should be completed and communicated to the IRT for addition to the information security event/incident/vulnerability database and review, and copied to the reporting person and his/her local manager.

Information and other evidence collected at this stage may need to be used at a future time for disciplinary or legal proceedings. The person or people undertaking the information collection and assessment tasks should be trained in the requirements for collection and preservation of evidence.

In addition to recording the date(s) and time(s) of actions, it is necessary to fully document the following:

- a) what was seen and done (including tools used) and why,
- b) the location of the potential evidence,
- c) how evidence is archived (if applicable),
- d) how evidence verification was performed (if applicable), and
- e) details of storage/safe custody of material and subsequent access to it.

If the information security event is determined as a likely information security incident, and if the person at PoC has the appropriate level of competence, further assessment may be conducted. This may require remedial actions, for example, identifying additional emergency controls being and referral for action to the appropriate person. It may be evident that an information security event is determined to be a significant information security incident (using the organization's pre-determined severity scale), in which case the IRT manager should be informed directly. It may be evident that a crisis situation should be declared and, for example, the crisis management manager be notified for possible activation of a crisis management plan, as well as the IRT manager and senior management be informed. However, the most likely situation is that the information security incident needs to be referred directly to the IRT for further assessment and action.

Whatever the next step is determined to be, the PoC should complete as much as possible of the information security incident reporting form. The information security incident reporting form should contain narrative and, as far as possible, should confirm and describe the following:

- a) what the information security incident is,

- b) how it was caused and by what or whom,
- c) what it affects or could affect,
- d) the impact or potential impact of the information security incident on the business of the organization,
- e) an indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined classification scale), and
- f) how it has been dealt with so far.

When considering the potential or actual adverse effects of an information security incident on the business of an organization, the following are some examples:

- a) unauthorized disclosure of information,
- b) unauthorized modification of information,
- c) repudiation of information,
- d) unavailability of information and/or service,
- e) destruction of information and/or service, and
- f) reduced performance of service.

The first step is to consider which of a number of consequences is relevant. For those considered relevant, the related category guideline should be used to establish the potential or actual impacts for entry into the information security incident report. Example guidelines are given in Part 2 Annex A (Example approaches to the categorization and classification of information security events and incidents) and Annex B. Example categories are the following:

- a) financial loss/disruption to business operations,
- b) commercial and economic interests,
- c) personal information,
- d) legal and regulatory obligations,
- e) management and business operations,
- f) loss of goodwill,
- g) injury or loss of life, and
- h) societal disruption.

If an information security incident has been resolved, the report should include details of the controls that have been taken and any lessons learned (e.g. controls to be adopted to prevent re-occurrence or similar occurrences). Once completed as far as possible, the reporting form should then be referred to the IRT for entry into the information security event/incident/vulnerability database for review.

If an investigation is likely to be longer than a time period defined in the information security incident management policy, an interim report should be produced within a time period specified by the policy.

It is emphasized that the PoC assessing an information security incident should be aware of the guidance provided in the information security incident management scheme documentation. It includes, for example, the following:

- a) when it is necessary to escalate matters and to whom, and
- b) change control procedures should be followed in all activities conducted by the PoC.

In a similar manner to that mentioned in Clause 5.1.1 and Clause 5.1.2 above regarding event detection and reporting, alternative means of communication of updated reporting forms should be used when problems exist, or are considered to exist, with electronic reporting mechanisms (e.g. e-mail).

### 5.2.2 Assessment and incident confirmation by the IRT

The assessment, and confirmation of the decision as to whether an information security event is to be classified as an information security incident, should be the responsibility of the IRT. The receiving person in the IRT should do the following:

- a) Acknowledge receipt of the information security incident reporting form, completed as far as possible by the PoC.
- b) Enter the form into the information security event/incident/vulnerability database if it was not done by the PoC and update the database if necessary.
- c) Seek clarification from the PoC, if necessary.
- d) Review the reporting form content.
- e) Collect any further information required and known to be available, whether from the PoC, the person who completed the information security event reporting form or elsewhere.

If there is still a degree of uncertainty as to the authenticity of the information security incident or the completeness of the reported information, the IRT member should conduct an assessment to determine whether the information security incident is real or in fact a false alarm (through use of the organization's agreed incident classification scale). If the information security incident is determined to be a false alarm, the information security event report should be completed, added to the information security event/incident/vulnerability database and communicated to the IRT manager. Copies of the report should be sent to the PoC, and the reporting person and his/her local manager.

An information security incident should be correlated to any other event/incident reported to the IRT. This important activity is to verify if the incident is connected to any other event/incident or it is simply the effect of another incident, i.e. in Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The correlation of incidents is also important in prioritizing the efforts of the IRT.

If the information security incident is determined to be real, the IRT member and colleagues as required, should conduct further assessment. The aim is to confirm the following as soon as possible:

- a) What the information security incident is, how it was caused and by what or whom, what it affects or could affect, the impact or potential impact of the information security incident on the business of the organization, an indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale). If the incident causes severe negative impact on the business, crisis activities should be initiated. (see Clause 5.3.4).
- b) The following aspects for deliberate human technical attack on an information system, service and/or network, for example:
  - 1) how deeply the system, service and/or network has been infiltrated, and what level of control the attacker has,
  - 2) what data has been accessed by the attacker, possibly copied, altered or destroyed,
  - 3) what software has been copied, altered or destroyed by the attacker,



- c) The direct and indirect effects (for example, is physical access open because of a fire, is an information system vulnerable because of some software or communications line malfunction, or because of human error), and
- d) How the information security incident has been dealt with so far and by whom.

When reviewing the potential or actual adverse effects of an information security incident on the business of an organization, from some information and/or services shown in Clause 5.2.1, it is necessary to confirm which of a number of consequences is relevant. Example categories are shown in Clause 5.2.1 and Part 2 Annex A.

A prioritizing process should be used to assign an information security incident to the most suitable person or group of persons in the IRT to facilitate an adequate response to the information security incident. In particular, when several information security incidents are being dealt with the same time, priorities have to be set to order the responses to be given to information security incidents.

Priorities should be set in accordance with the determined adverse business impacts associated with the information security incident and the estimated effort needed to respond to the information security incident. For incidents with the same priority, the required effort is one metric to determine the order in which they need to be responded. For example, an incident that is easily resolved may be dealt with before an incident requiring a greater effort.

For those considered relevant, the related category guideline should be used to establish the potential or actual impacts for entry into the information security incident report.

## 5.3 Responses

### 5.3.1 Immediate responses

#### 5.3.1.1 Overview

In the majority of cases, the next activities for the IRT member are to identify the immediate response actions to deal with the information security incident, record details on the information security incident form and within the information security event/incident/vulnerability database, and notify the required actions to the appropriate persons or groups. This may result in emergency controls (for example, cutting off/shutting down an affected information system, service and/or network, with the prior agreement of the relevant IT and/or business management), and/or additional permanent controls being identified, and notified for action to the appropriate person or group. If not already done so, the significance of the information security incident should be determined, using the organization's pre-determined classification scale, and if sufficiently significant appropriate senior management should be notified directly. If it is evident that a crisis situation should be declared, for example the crisis management manager should be notified for possible activation of a crisis management plan, with the IRT manager and senior management also informed.

The overall objectives in responding to information security incidents are the following:

- a) To confine the potential adverse impacts (of information security incidents), and
- b) To improve information security.

The primary goal of the information security incident management scheme and associated activities should be the minimization of adverse business impacts, whereas identification of the attacker should be considered a secondary goal.

#### 5.3.1.2 Example actions

As an example of relevant immediate response actions in the case of deliberate attack on an information system, service and/or network, it could be left connected to the internet, or other network. This will allow business critical applications to function correctly, and collect as much information as possible about the attacker, provided that the attacker does not know that he/she is under surveillance.

It is vitally important to follow planned processes and record action. Beware of Trojans, rootkits and kernel modules that may cause serious damage to the system. Evidence can be protected with cryptography, locks and records of access.

- a) While undertaking such a decision, it needs to be considered that the attacker may realize that he/she is being observed and may undertake actions that cause further damage to the affected information system, service and/or network, and related data, and the attacker could destroy the information that may be useful to track him/her.
- b) It is essential that it is technically possible to quickly and reliably cut-off and/or shut down the attacked information system, service and/or network, once a decision had been taken. This serves to contain the incident.

A further consideration is that the prevention of re-occurrence is usually of high priority, and it might well be concluded that the attacker has exposed a vulnerability that should be rectified, and the gains from tracking him/her do not justify the effort in doing so. This is especially relevant when the attacker is non-malicious and has caused little or no damage.

With regard to information security incidents that are caused by something other than deliberate attack, the source should be identified. It may be necessary to shut the information system, service and/or network down, or isolate the relevant part and shut it down (with the prior agreement of the relevant IT and/or business management), while controls are implemented. This may take longer if the vulnerability is fundamental to the information system, service and/or network design, or if it is a critical vulnerability.

Another response activity may be to activate surveillance techniques (for example, honeypots – see ISO/IEC 18043). This should be on the basis of procedures documented for the information security incident management scheme.

Information that may be corrupted by the information security incident should be checked by the IRT member against backup records for modifications, deletions, or insertions of information. It may be necessary to check the integrity of the logs, as a deliberate attacker may have manipulated these logs to cover his/her tracks.

### 5.3.1.3 Incident information update

Whatever the next step is determined to be, the IRT member should update the information security incident report as much as possible, add it to the information security event/incident/vulnerability database, and notify the IRT manager and others as necessary. The update may cover further information on the following:

- a) what the information security incident is,
- b) how it was caused and by what or whom,
- c) what it affects or could affect,
- d) the impact or potential impact of the information security incident on the business of the organization,
- e) changes to the indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale), and
- f) how it has been dealt with so far.

If an information security incident has been resolved, the report should include details of the controls that have been taken and any other lessons learned (e.g. further controls to be adopted to prevent re-occurrence or similar occurrences). The updated report should be added to the information security event/incident/vulnerability database, and notified to the IRT manager and others as required.

It is emphasized that the IRT is responsible for ensuring the secure retention of all information pertaining to an information security incident for further analysis, and potential legal evidential use. For example, for an IT oriented information security incident, the following actions should be taken.

After the initial discovery of the incident, all volatile data should be collected before the affected IT system, service and/or network is shut down, for a complete information security investigation. Information to be collected includes contents of memory, cache and registers, and detail of any activities running, and the following.

- a) A full information security investigation duplication of the affected system or a low level backup of logs and important files should be undertaken depending on the nature of the information security incident.
- b) Logs from neighbouring systems, services and networks, for example including from routers and firewalls, should be collected and reviewed.
- c) All information collected should be stored securely on read only media.
- d) Two or more persons should be present when information security investigation duplication is performed, to assert and certify that all activities have been carried out in accordance with relevant legislation and regulation.
- e) Specifications and descriptions of the tools and commands used to perform the information security investigation duplication should be documented and stored together with the original media.

An IRT member is also responsible for facilitating the return of the affected facility (whether IT or otherwise) to a secure operational state that is not susceptible to a compromise by the same attack, if possible at this stage.

#### **5.3.1.4 Further activities**

If an IRT member determines that an information security incident is real, then other important activities should be the following:

- a) activity to institute information security investigation analysis, and
- b) activity to inform those responsible for internal and external communications of the facts and proposals for what should be communicated, in what form and to whom.

Once an information security incident report has been completed as far as possible, it should be entered into the information security event/incident/vulnerability database and communicated to the IRT manager.

If an investigation is likely to be longer than a time period pre-agreed within the organization, an interim report should be produced.

The IRT member responding to an information security incident should be aware, based on the guidance provided in the information security incident management scheme documentation, of the following:

- a) when it is necessary to escalate matters and to whom, and
- b) change control procedures should be followed in all activities conducted by the IRT

When problems exist or are considered to exist, with electronic communications facilities (e.g. e-mail or web), including when it is thought possible that the system is under attack, the report to the relevant people should be done by alternative means such as in person, by telephone or text messaging.

If it is concluded that an information security incident is significant or a crisis situation has been determined, then the IRT manager, in liaison with the organization's information security manager and the relevant board member/senior manager, should liaise with all related parties, both internal and external to the organization.

To ensure that the liaisons are organized quickly and are effective, it is necessary to establish a secure method of communication in advance that does not wholly rely on the system, service and/or network that may be affected by the information security incident. These arrangements may include the nomination of backup advisors or representatives in the case of absence.

### 5.3.2 Assessment of control over information security incidents

After the IRT member has instigated the immediate responses and relevant information security investigation analysis and communications activities, it needs to be quickly ascertained whether the information security incident is under control. If necessary, the IRT member may consult with colleagues, the IRT manager and/or other persons or groups.

If the information security incident is confirmed as being under control, the IRT member should institute any required later responses, and information security investigation analysis and communications, to end the information security incident and restore the affected information system to normal operations.

If the information security incident is confirmed as not being under control, then the IRT member should institute crisis activities.

If the information security incident is related to loss of availability, the metric to assess whether an information security incident is under control could be the time elapsed before recovering to a normal situation further to the occurrence of an information security incident. The organization should determine for each asset, based upon the results of the information security risk assessment, its acceptable interruption window that supports the recovery time objective before resumption of the service or the access of the information. As soon as the response exceeds the acceptable interruption window of the targeted asset, the information security incident may not be under control anymore and the decision to escalate the information security incident should be taken.

Information security incidents related to loss of confidentiality, integrity etc. needs other types of judgements to determine if the situation is under control and possible related metrics according to organization crisis management plans.

### 5.3.3 Later responses

Having determined that an information security incident is under control, and not subject to crisis activities, the IRT member should identify if and what further responses are required to deal with the information security incident. This could include restoring the affected information system(s), service(s) and/or network(s) back to normal operation. He/she should then record details on the information security incident reporting form and in the information security event/incident/vulnerability database, and notify those responsible for completing the related actions. Once those actions have been successfully completed, details should be recorded on the information security incident reporting form and in the information security event/incident/vulnerability database, and then the information security incident should be closed and appropriate personnel notified.

Some responses are directed at preventing information security incident re-occurrence or similar occurrence. For example, if it is determined that the cause of an information security incident is an unknown vulnerability, the supplier should be notified immediately. If a known IT vulnerability was involved in an information security incident, it should be patched with the relevant information security update. Any IT configuration related problems highlighted by the information security incident should be dealt with thereafter. Other measures to decrease the possibility of re-occurrence or similar occurrence of an IT information security incident may include changing system passwords and disabling unused services.

Another area of response activity may involve monitoring the IT system, service and/or network. Following the assessment of an information security incident, it may be appropriate to have additional monitoring controls in place to assist in detecting unusual and suspicious events that would be symptomatic of further information security incidents. Such monitoring may also reveal a greater depth to the information security incident, and identify other IT systems that were compromised.

It may well be necessary for activation of specific responses documented in the relevant crisis management plan. This could apply for both IT and non-IT related information security incidents. Such responses should include those for all business aspects, not just directly IT related but also key business function maintenance and later restoration – including, as relevant, of voice telecommunications, and personnel levels and physical facilities.

The last area of activity is the restoration of the affected information system(s), service(s) and/or network(s) to normal operation. The restoration of an affected system(s), service(s) and/or network(s) to a secure

operational state may be achieved through the application of patches for known vulnerabilities or by disabling an element that was the subject of the compromise. If the entire extent of the information security incident is unknown, due to the destruction of the logs during the incident, then a complete system, service and/or network rebuild may be necessary.

It may well be necessary for activation of parts of the relevant crisis management plan. If an information security incident is non-IT related, for example caused by a fire, flood or bomb, then the recovery activities to be followed are those documented in the relevant crisis management plan.

#### 5.3.4 Responses to crisis situations

As discussed in Clause 5.3.2, it may be that the IRT determines an information security incident is not under control and needs to be escalated to crisis situation, using a pre-designated plan.

The best options for dealing with all possible types of information security incidents that might affect availability and to some extent integrity of an information system, should have been identified in the organization's crisis management plan. These options should be directly related to the organization's business priorities and related timescales for recovery, and thus the maximum acceptable outage time periods for IT, voice, people and accommodation. The strategy should have identified the following:

- a) the required preventive, resilience and crisis management measures,
- b) the required organizational structure and responsibilities for responding to crisis, and
- c) the required structure and outline content for the crisis management plan or plans.

The crisis management plan(s) and the controls put in place to support the activation of those plan(s), once tested satisfactorily, form the basis for dealing with most escalated incidents once so designated.

Depending on the type of incident and if it is not under control, the escalation may lead to serious activities to deal with the incident and activate the crisis management plan if such is in place. Such activities may include, but are not limited to, the activation of:

- a) fire suppression facilities and evacuation procedures,
- b) flood prevention facilities and evacuation procedures,
- c) bomb handling and related evacuation procedures,
- d) specialist information system fraud investigators, and
- e) specialist technical attack investigators.

#### 5.3.5 Information security investigation analysis

Where identified by prior assessment as required for evidential purposes, de facto in the context of a significant information security incident, information security investigation analysis should be conducted by the IRT. It should involve the use of IT based investigative techniques and tools, supported by documented procedures, to review the designated information security incident(s) in more detail than has been the case hitherto in the information security incident management process. It should be conducted in a structured manner, and, as relevant, identify what may be used as evidence, whether for internal disciplinary procedures or legal actions.

The facilities needed for information security investigation analysis is likely to be categorized into technical (e.g. audit tools, evidence recovery facilities), procedural, personnel and secure office facilities. Each information security investigation analysis activity should be fully documented, including relevant photographs, audit log analysis reports, and data recovery logs. The proficiency of the person or people performing the information security investigation analysis should be documented along with records of proficiency testing. Any other information that demonstrates the objectivity and logical nature of analysis should also be

documented. All records of the information security incidents themselves, the information security investigation analysis activities, etc. and associated media, should be stored in a physically secure environment and controlled by procedures to prevent unauthorized people from accessing, altering or rendering it unavailable. Information security investigation analysis IT based tools should comply with standards such that their accuracy cannot be legally challenged, and should be kept up-to-date in line with technology changes. The IRT physical environment should provide demonstrable conditions that ensure the evidence is handled in such a way that it cannot be challenged. Enough personnel should be available, if necessary on an on-call basis, to be able to respond at any time.

Over time, new requirements may arise to review evidence of a variety of information security incidents, including fraud, theft, and vandalism. Thus, to assist the IRT there needs to be a number of IT based means and supporting procedures available for uncovering information hidden in an information system, service or network, including information that on an initial inspection appears to have been deleted, encrypted, or damaged. These means should address all known aspects associated with known types of information security incidents and be documented in the IRT procedures.

In today's environment, information security investigation analysis is frequently needed to encompass complex networked environments, where investigation needs to encompass an entire operating environment, including a multitude of servers (e.g. file, print, communications and e-mail), as well as remote access facilities. There are many tools available, including text search tools, drive imaging software and information security investigation suites. The main focus of information security investigation analysis procedures is to ensure that evidence is kept intact and checked to ensure that it stands up to any legal challenge.

It is emphasized that information security investigation analysis should be performed on an exact copy of the original data, to prevent the analysis work prejudicing the original media integrity. The overall information security investigation analysis process should encompass, as relevant, the following activities:

- a) Activity to ensure that the target system, service and/or network is protected during the information security investigation analysis from being rendered unavailable, altered or otherwise compromised, including by malicious code (including viruses) introduction, and that there are no or minimal effects on normal operations.
- b) Activity to prioritize the acquisition and collection of evidence i.e. proceeding from the most volatile to the least volatile (this depends in large measure on the nature of the information security incident).
- c) Activity to identify all relevant files on the subject system, service and/or network, including normal files, password or otherwise protected files, and encrypted files.
- d) Activity to recover as much as possible discovered deleted files, and other data.
- e) Activity to uncover IP addresses, host names, network routes and web site information
- f) Activity to extract the contents of hidden, temporary and swap files used by both application and operating system software.
- g) Activity to access the contents of protected or encrypted files (unless prevented by law).
- h) Activity to analyze all possibly relevant data found in special (and typically inaccessible) disc storage areas.
- i) Activity to analyze file access, modification and creation times.
- j) Activity to analyze system/service/network and application logs.
- k) Activity to determine the activity of users and/or applications on a system/service/network.
- l) Activity to analyze e-mails for source information and content.
- m) Activity to perform file integrity checks to detect Trojan horse files and files not originally on the system.

- n) Activity to analyze, if applicable, physical evidence, for example fingerprints, property damage, video surveillance, alarm system logs, pass card access logs, and interview witnesses.
- o) Activity to ensure that extracted potential evidence is handled and stored in such a way that it cannot be damaged or rendered unusable, and that sensitive material cannot be seen by those not authorized. It is emphasized that evidence gathering should always be in accordance with the rules of the court or hearing in which the evidence may be presented.
- p) Activity to conclude on the reasons for the information security incident, the actions required and in what timeframe, with evidence including lists of relevant files included in an attachment to the main report.
- q) Activity to provide expert support to any disciplinary or legal action as required.

The method(s) to be followed should be documented in the IRT procedures.

The IRT should accommodate sufficient combinations of skills to provide wide coverage of technical knowledge (including of the tools and techniques likely to be used by deliberate attackers), analysis/investigative experience (including regarding the preservation of usable evidence), knowledge of relevant legislation and regulation implications, and ongoing knowledge of incident trends.

The following should be recognized:

- a) some organizations may not have all such resources available and that such organisations may need to out-source information security investigation analysis work to specialists,
- b) collecting information security investigation material may only be a resort (i.e. the effort and expense justified) where serious loss has occurred and/or criminal proceedings are likely, and

not using specialist resources to capture information security investigation material may render the findings as being inadmissible if court action is required.

### 5.3.6 Communications

In many cases when an information security incident has been confirmed by the IRT as real, there is a need for certain people to be informed both internally (outside of normal IRT/management lines of communication) and externally, including the press. This may need to occur at a number of stages, for example when an information security incident is confirmed as real, when it is confirmed as under control, when it is designated for crisis activities, when it is closed and when post incident review has been completed and conclusions reached.

When communication is needed, due care should be taken to ensure who needs to know what and when. Stakeholders that are affected should be determined and preferably divided into groups such as:

- a) direct internal stakeholders (crises management, management staff etc.),
- b) direct external stakeholders (owners, customers, partners, suppliers etc.), and
- c) other external contacts such as press and/or other media.

Each group may need special information that should come through the appropriate channels of the organization. One of the most important task for communication after an information security incident is to ensure that direct external and direct internal stakeholders will have the information prior to that it comes through other external contacts such as press.

To aid this activity when the need arises, it is sensible practice to prepare certain information in advance such that it is quickly adjusted to the circumstances of a particular information security incident and issued to each relevant group and in particular the press and/or other media. If any information pertaining to information security incidents is to be released to the press it should be done in accordance with organization's

information dissemination policy. Information to be released should be reviewed by the relevant parties, which may include senior management, public relations co-ordinators and information security personnel.

**NOTE** The communications of information security incident may vary depending on the incident and its impact in combination with the organization relations and type of business. The type of business may also set specific rules for how communication should be done, for example if the organization is listed on a public stock market.

### 5.3.7 Escalation

In extreme circumstances, matters may have to be escalated to accommodate incidents that are out of control and a potential danger for unacceptable business impact. These incidents need to be escalated to activate the business continuity plan if in place by reporting to either senior management, another group within the organization or persons or groups outside of the organization. This may be for a decision to be made on recommended actions to deal with an information security incident or for further assessment to determine what actions are required. This could be following the assessment activities described above in Clauses 5.2.1 and 5.2.2, or during those activities if some major issue becomes evident early. Guidance should be available in the information security incident management scheme documentation for those who are likely at some point to need to escalate matters, i.e. PoC and IRT members.

### 5.3.8 Activity logging and change control

It is emphasized that all involved in the reporting and management of an information security incident should properly log all activities for later analysis. This should be included with the information security incident reporting form and in the information security event/incident/vulnerability database, continually kept up-to-date throughout the cycle of an information security incident from first reporting to completion of post-incident review.

This information should be retained provably secure and with an adequate back-up regime. Further, all changes made in the context of tracking an information security incident and updating the information security incident reporting form and the information security event/incident/vulnerability database should be under a formally accepted change control scheme.

## 6 Incident Response Teams (IRTs) Organization

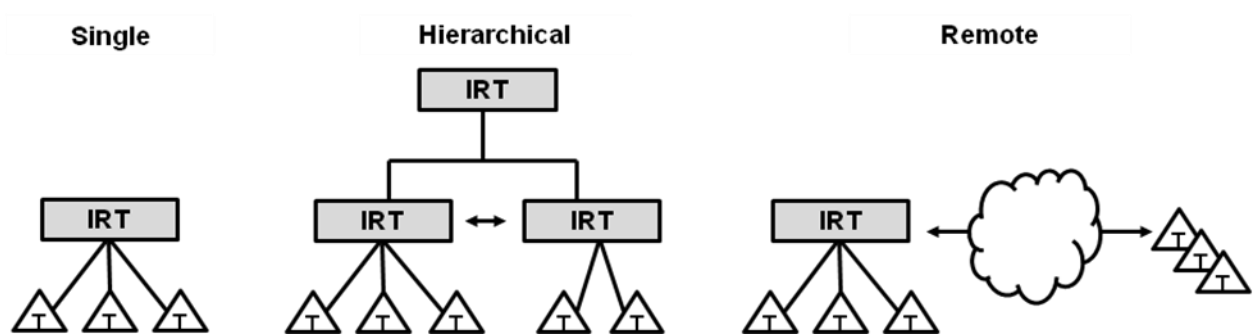
### 6.1 Overview

IRTs are teams of appropriately skilled and trusted members of the organization that provide proper responses, analysis, and preventions of various incidents that occur on computer networks. In order to establish an IRT, the size of the dedicated organization, monitoring targets, and coverage have to be defined. The effectiveness of an IRT is critical. Therefore, the roles and responsibilities of IRT members should be clearly defined. The prompt response and correct decision by the IRT members are critical such that spread of damage caused by incidents are rapidly contained and addressed.

### 6.2 IRTs types and roles

Generally, IRTs can be classified into three different types as shown in Figure 1: single, hierarchical, and remote types, based on the desired goal of the organizations. To establish a proper IRT, the size of the organization, the importance of the information, and interoperability with other organizations should be considered. In Figure 1, the T refers to targets which are monitored by the particular IRT.





**Figure 1 —Types of the IRTs**

- Single (Single type of IRT):** The monitoring scope is a single organization, or a single IRT performing monitoring of multiple organizations or targets 24 hours, 7 days and 365 days. This type is generally used for the incident management, response and operation activities.
- Hierarchical (Hierarchical type of IRT):** One or more IRTs overlap monitoring scopes. It can increase the reliability for incident response activities.
- Remote (Remote type of IRT):** By collecting the security events from remote locations, this type is generally used for out-sourcing enterprise (specialized information security enterprise) to monitor the targets.

In order to provide prompt response to various threats, IRTs require a response policy, response procedures and operation activities. The main roles of IRTs are as follows:

- Managing Integrated security systems**
  - Monitoring and information security event management of agents installed on heterogeneous systems (e.g. intrusion detection system, intrusion prevention system, firewall, network resource, etc.).
- Implementing a consistent policy**
  - Minimizing risks for the security system by a consistent policy.
- Responding promptly**
  - Reinforcing prevention activities against incidents (e.g. monitoring, pre-responses, security policy, etc.).
- Operating the optimized security structure**
  - Providing effective security plan for information properties.

Fundamental duties of an IRT are summarized as follows:

- Integrated management and monitoring:** 24 x 7 x 365 hours monitoring of targets, proactive monitoring and responses against incidents, logs management.
- Reports management:** Periodic security reporting, security patches management, incident reporting.
- Administrative management:** Policy management for various system environments including task control and IRT operations.
- Technical management:** Network, system, application, contents, and service security management.

- e) *System operation and management*: System capacity, performance, security configuration, and environment configuration management.

### 6.3 IRT staff

An IRT should respond if it detects malicious code flowing into the monitored area and performs proper actions for minimizing and removing vulnerabilities. Furthermore, those detected security events should be notified to a system and/or network manager for effective response.

IRTs can be structured differently depending on the organization size, its staff members and industry type. The incident responses are usually dependent on the capability and reliability of the staff members in an IRT.

IRT staff members and their capabilities become even more important when the activities of IRTs include establishing the security policy for preventing incidents, auditing, coordinating with other departments as well as technical activities. The skills required for the members are as follows:

- a) Personal skills: communication, problem solving, team interactions, time management.
- b) Technical skills: security principles, risks analysis, vulnerability, network protocol, security/virus issue, application.
- c) Incident response skills: team policy/procedure, communication, incident analysis, recording, tracking information.
- d) Specialized skills: presentation, leadership, expert technology, programming.

In addition, the staff members are required to operate and response to various incidents. Therefore, the members in an IRT should possess skills for:

- a) General data communication techniques (Telephone, ISDN, X.25, PBX, ATM, Frame relay etc.).
- b) Network protocols (IP, ICMP, TCP, UDP etc.).
- c) Network application protocols (SMTP, HTTP, FTP, TELNET etc.).
- d) Network-based systems (DNS, IDS, firewall, router, mail server etc.).
- e) Type of attack and Vulnerability (IP sniffing, sniffer and computer virus etc.).
- f) Cryptography, hash algorithm, digital signature, etc.
- g) System security patches and backup, etc.
- h) Computer/Network threat and risk.
- i) Security rule of organization
- j) Network security issues.

To organize an IRT, the roles of members should be defined as shown in Table 1.

**Table 1 — Roles of Members**

Roles	Description
IRT Manager	The leadership role is responsible for managing the staff members, defining the job scope, and reporting the status to higher-level organizations.

Roles	Description
Planning	<p>Responsible for operating an IRT. It establishes or plans various security policies, reports them to higher-level authorities, cooperate with third parties, and register and approve vulnerability reports. Its roles are:</p> <ul style="list-style-type: none"> <li>a) Establishing and planning security policies</li> <li>b) Implementing security processes</li> <li>c) Adjusting the risk priorities</li> <li>d) Communicating with higher-level organizations and other third-parties organizations</li> <li>e) Supporting administration</li> <li>f) Discussing/registering/approving vulnerability reports on the target organizations</li> <li>g) Performing other activities directed by the IRT manager</li> </ul>
Monitoring	<p>Responsible for real-time monitoring and actual operation activities such as security event monitoring/detection/identification, incident registration, and prevention. It performs the real-time security monitoring activities and the followings:</p> <ul style="list-style-type: none"> <li>a) 24 x 365 hours monitoring and operation</li> <li>b) Intrusion trial detection, registering incidents, and pre-responses</li> <li>c) Performing the security patches and upgrades</li> <li>d) Implementation of the security policy and backup management</li> <li>e) Help desk</li> <li>f) Facility management</li> <li>g) Performing other activities directed by the IRT manager</li> </ul>
Response	<p>Takes over the case from the monitoring agents for incidents related to intrusion, performs secondary further analysis and actions including investigation efforts, performs recovery actions and establishes adequate strategy. Services such as real-time responses, technical support, and the following are also provided:</p> <ul style="list-style-type: none"> <li>a) Propagating and reporting incidents</li> <li>b) Correlation analysis between monitoring systems</li> <li>c) Incident investigation and recovery supports</li> <li>d) Vulnerability analysis on the target organization and IRT</li> <li>e) Performing other activities directed by the IRT manager</li> </ul>
Analysis	<p>In cooperation with the response team, it performs in-depth analysis including correlation analysis for the incidents. Analysis on incidents and the following are also provided:</p> <ul style="list-style-type: none"> <li>a) Planning vulnerability analysis for the target organization and IRT</li> <li>b) Improving the security analysis tools and checklist</li> <li>c) Improving the monitoring rules</li> <li>d) Publication of newsletter</li> <li>e) Performing other activities directed by the IRT manager</li> </ul>

## 7 Incident response operations

### 7.1 Incident criteria

For efficient response and operation against incidents, the criteria to determine the handling of incidents should be defined. Moreover, the reference guidelines should be set for security incidents according to the priority of information and information system, impact of each intrusion types, damage scale, intrusion alarm level, and its severity. To define the criteria, see Annex A.

Incidents are generally classified into the followings based on the work properties, organization size, and its information importance:

- a) General incidents

- 1) Incidents caused by malicious software (e.g.Worms, viruses, backdoor, Trojan horse etc.).
- 2) Unauthorized intrusions to network and/or system.
- 3) General property theft, loss, and destruction.
- 4) Abnormal system operation caused by security vulnerabilities.
- 5) Unauthorized access and/or information access allowed to unapproved personnel.
- 6) access attempted by unauthorized personnel.
- 7) Abnormal services caused by modification and/or damage due to unauthorized access.

b) Major incidents

- 1) Stop services by unauthorized access to the system, which causes modification and/or destruction.
- 2) Exposure to confidential resource and/or Serious damage to reputation/brand.
- 3) Serious damage to the organizational operation caused by intentional and/or mistakes.
- 4) Modification and/or destruction to the security equipment (entrance security, intrusion detection system, locking devices, surveillance camera, etc.).

## 7.2 Incident response processes

As shown in Figure 2, the real-time incident-response processes are performed in the order of detection, assessment and decision, response, and reporting/post-operation.

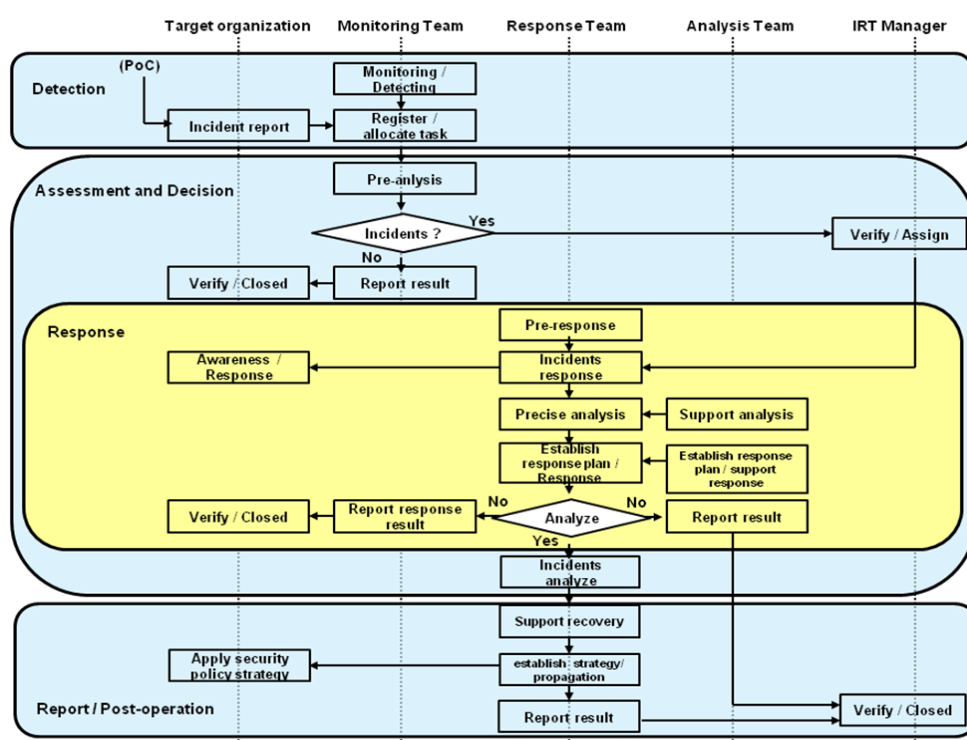


Figure 2 —Typical Incident response processes

### 7.3 Detection

As the first step, it monitors the security events, detects incidents, and/or receives the report of the incidents from the monitoring site (or domain) of the organization. It performs the following tasks:

a) Monitoring

- 1) Monitoring security events from the target organization for 24 x 365 hours.
- 2) Monitoring by the console (e.g. security devices does not support inter-operation).
- 3) Verify incident occurrences (e.g. Broadcasting and Internet News).
- 4) Reinforce and/or alter rules set of the monitoring system while any intrusion is in progress.

b) Detection

- 1) Verify incidents (positives and/or negatives) by collecting and analysing security events.
- 2) Verify incident occurrences and operation status of monitoring equipment with staff in target organization.
- 3) In case of one or more incidents, register the case. Otherwise alter the detection rules and record the case.

c) Registration

- 1) Register and verify the incident occurrences.
- 2) Report the incident occurrences.

**NOTE** Verify incident reporter information (organization, name, contact, etc.), damaged system (host name, IP etc.), detailed description of the incidents, incident detected date/time, post-response, attack types and etc.

For the incident registered through detection and/or report, the monitoring team verifies whether the case is real incident through pre-analysis. It performs the following tasks:

- a) After verifying security events and status, the monitoring team makes a decision on incident occurrence, and its initial severity such as incident type, the importance of the damaged system, alarm level, etc. (See Annex A).
- b) In the case that the alarm level is identified as “Serious” or “Alert,”
  - 1) Report the case to the IRT manager, and register it.
  - 2) The IRT manager verify the case and whether it is considered “Serious” or “Alert,”
    - Using emergency contacts, call the related staff members and organizations.
- c) In the case that the alarm level is identified as “Cautious,”
  - 1) Report the case to the IRT manager and request the actions to response teams according to the direction from the manager.
- d) In the case that the alarm level is identified as “Concerned,” report the case to the IRT manager and monitoring teams and/or staffs directly take proper responses.

## 7.4 Incident response

### 7.4.1 Pre-response

To minimize the damage caused by incidents, incident response include the following activities: pre-response, establishing the incident response policy by analysis, and planning the security strategies in cooperation with monitoring teams, response teams, and analysis teams.

After detecting incidents, the monitoring team should take over the pre-response as follows:

- a) In the case that the incident type is a worm and/or virus (Expandable attacks):
  - 1) Isolate and/or disconnect system from the infected network.
  - 2) Block access (such as a inbound traffic) and/or control the access permission through the firewall or router.
- b) In the case that the incident type is a network intrusion (Unauthorized attacks):
  - 1) Separate the victim system to prevent additional damage.
  - 2) In the case that the system is not able to disconnected:
    - Backup the victim system.
    - Remove the vulnerabilities such as a backdoor, etc.
  - 3) In the case that the concerning evidence is damaged:
    - Request to the staff in charge to conduct preservation of evidence and backup.

Monitoring teams perform pre-response (and register incidents) and transfer to response teams the information as follows:

- e) Incident occurrence and registration date/time, description of the incident, damaged content, etc.
- f) System and network information, damage type and severity, etc.

### 7.4.2 Responses

After taking over the incident information from monitoring teams, response teams report it to the IRT manager. The teams inform the organization's security staff of the case, and perform the further analysis. After identifying the incident type, the teams conduct the assessment of the damage with the following references:

- a) Importance of exposed information and infected system.
- b) Importance of exposed information and infected system.
- c) Exposed incident related information to public and/or other organizations.
- d) Attack skills or level.
- e) Service operation status (e.g. halt time).
- f) Cost of the damage.

If the alarm level is over "Cautious," the cause and other effects should be precisely analyzed. If accurate analysis is not possible by internal staffs, response teams request external experts or supports from other

organizations. Through the analysis report, the teams double-check the severity of the incidents, and establish a response plan with the consideration of the severity, attack types, damage coverage, priority, analysis data, etc.

Table 2 describes an example of the response tactic by incident types. The response team must guess the expected results and establish an effective counter plan as shown in Table 2. All incident response activities must be notified and approved by the IRT manager.

**Table 2 — Example of the response tactic by Incident types**

Incident type	Example of the response
DoS	To minimize the flooding effect, adjust access policy the router and/or firewall
Unauthorized use	Preserve evidence and interview with the incident suspect
Exposed Information	Preserve evidence and verify scope of the exposed information
Unauthorized access	Monitoring the attacker activities, blocking unauthorized access and reconfiguring / recovering victim system

The response team must report the result of actions taken for the intrusion case (intrusion date, type, seriousness, root cause, symptom, required compensating items, etc.) and keep the records for registration, detection, action, and result.

## 7.5 Assessment and decision

By analyzing the root cause after collecting the data for attack type and evidences, the spread of damage can be blocked, a prevention policy is established, and quick and effective recovery of the system is followed.

In the assessment and decision step, be careful not to let publicly known information related to the incident to hinder the investigation. Analysis teams should investigate the following data through remote or field investigation.

### a) Data collection

#### 1) Host-based data collection

- Perform the system backup.
- Analyze and remove the vulnerabilities such as a backdoor.
- First off, collect volatile data that can be easily damaged by system shutdown or reboot.
- Collect the data in use (such as logs, records, data, etc.).
- Verify using program and/or data backup, and collect the integrity data.
- Preserve the evidences, and back up the incidents for referencing.

**EXAMPLE** System date/time, running applications and open ports, network status, network interface status, memory status, open files, backdoor, hacking programs, etc.

#### 2) Network-based data collection

### b) Data analysis

- 1) After investigating the collected data (log files, system configurations, history data, emails and attached files, installed applications, etc.) from the damaged system and network, analysis teams analyze the cause and trace of incidents.

- 2) Perform the data analysis activities such as software vulnerability analysis, time/date stamps analysis, etc.
- 3) If necessary, perform the low level investigation.

NOTE The International Standards (ISO/IEC 27037) provides more detailed information on the identification, collection, acquisition and preservation of digital evidence.

**Table 3 — Examples of Analysis information**

Item	Analysis Description
Window System	Verify system and process time/status, network information, user/group, sharing information, login information etc.
	Root kit (process, network, hidden registry check), etc.
	Registry analysis, auto execution, event/log analysis, file system created time, intrusion method analysis, Internet temporary files, etc.
	Detected malicious codes and/or hacking programs, etc.
Unix System	System information(e.g. operating system type, version, usage, services), process information, open files and ports, network information, accessed users, etc.
	Password file, log file, root kit, hacking-related files, etc.
Network	Data collection for each incidents types (use of illegal resources, DoS, data loss and modification, exposed information), etc.
	Packet, traffic statistics, decoded packet, etc.
	Attack patterns, cause of overload, etc.
Database	Use of the default password, remote access, etc.
	Access permission and/or authorization, access control list, etc.

The incident evidences should be preserved safely for the future reference, and the collected data (such as a log file, process information, network connection status, file system, worm/virus, database, etc.) should be backed up with image data (such as a database dump, history file, screen shot, disk image, picture, etc.).

#### c) Incident report

- 1) Through the investigated result, the causes, attack route, and intruders should be identified or traced to check the damage's coverage and impact (see Annex table - A.1.2).
- 2) Report the result to the staff in charge and the IRT manager.
- 3) If additional incidents are expected, or suspected of damage, proper actions and/or extra supports should be provided to the staff of the damaged organizations in order to prevent the spread of damage.

## 7.6 Reporting and post-operation

All incident response and analysis results should be reported to the IRT manager and archived in the result reports. According to the alarm level (See Annex A.2), the response procedures and actions should be included in the reports. In case of "Cautious" and "Concerned", the case should be reported to the IRT manager. In case of "Serious" and "Alert", the IRT manager should report the integrated result to the higher-level organizations and/or related organizations, and establish a cooperative response strategy.

If additional incidents are not found through the analysis result, report or inform it to the organization, and close the case.

#### a) Post operations



- 1) If there are suspected of additional incidents by similar vulnerabilities, perform the vulnerability analysis
- 2) Perform the response-related training for the prevention
- 3) After closing the incident, the collected data and information should be disposed

## 8 General example of incident response

### 8.1 Denial of Service (DoS)

Incidents contain various types of attacks including unauthorized system and/or file access, unauthorized network information gathering, unauthorized use of services using network vulnerabilities, service interferences, abnormal services, malicious code, viruses, etc. Intelligent and automatic attacks are increasing, and their features are as follows:

- a) Large scale (attacks multiple systems at the same time)
- b) Distribution (attacks the target system from multiple servers)
- c) Popularization (easy acquisition of hacking-related information)
- d) Criminal tendency (financial gain, industrial information pillage, political intention)

The above-mentioned attacks are enabled by using various complicated technologies. Accordingly, prompt and efficient incident response and operations are required. According to Clause 7.2, incident response processes, IRTs should take a cooperative response with the network and system administrator of the damaged organizations referring to incidents (see Annex A).

By DoS attack, huge amounts of traffic are transmitted to the target system to interfere and/or stop services (such as a web application). In order to handle DoS, the following responses are required.

- a) Trace and block source IP address.
- b) Block additional flow of traffic in cooperation with ISP.
- c) Prompt responses (such as build up a DNS sinkhole, routing traffic to a null, move the system to safety zones and/or load balanced firewalls etc.).
- d) Register the source (attacker's) IP address(es) in the security devices (such as firewall, IDS, IPS, etc.).

### 8.2 Malicious code

The following responses are required to address malicious code that includes worms, viruses, backdoor, Trojan horse, etc.:

- a) Respond promptly (see Clause 7.4).
- b) Trace and block source IP address.
- c) In case of internal attack, analyze the vulnerability in cooperation with the anti-virus provider and apply the security patches/update to the up-to-date version of anti-virus program.

### 8.3 Information gathering

Information is collected on the target system by using vulnerability-analyzing tools or system commands. The following responses are required:

- a) Respond promptly (see Clause 7.4).
- b) Trace and block source IP address through the firewall.

#### **8.4 Inappropriate usage**

When software vulnerability (buffer overflow, configuration vulnerability etc) and/or protocols vulnerability (TCP, IP, ARP, DNS, RIP, OSPF, DHCP, SNMP) are exposed in an attack, the following responses should be required:

- a) Respond promptly (see Clause 7.4).
- b) Trace and block source IP address through the firewall.

#### **8.5 Unauthorized access**

When unauthorized attempts to access a system, service and/or network is occur, the following responses should be required:

- a) Respond promptly (see Clause 7.4).
- b) Trace and block source IP address through the firewall.

## Annex A (informative)

### Example of the incident criteria based on computer security events and incidents

#### A.1 Computer security events and incidents

##### A.1.1 Fundamental incident criteria

For all the incidents that can cause damage and interferences to running services, the incident criteria are determined based on the type, impact, system priority, damage scale, etc.

Incident criteria should be established that are proper to organizations as shown in Table A.1, A.2, A.3, A.4, and A.5.

**Table A.1 — Example of fundamental incident criteria**

Category	Description	Reference
Importance of Information	"Moderate", "Important", "Very Important"	Table A.4
Impact of the incident type	"Moderate" or beyond	Table A.2
Intrusion damage scale	"Moderate" or beyond	Table A.3
User Definition	Security event is detected by User-defined rule set	Other than integrated analysis, ESM, and TMS, etc.

##### A.1.2 Impacts according to each incidents types

**Table A.2 — Example of impacts according to each Incident**

Incident types	Impact			
	Low	Moderate	Important	Very Important
Information gathering	x			
Simple intrusion trials	x			
Security policy violation	x	x		
Causing traffic network	x	x		
Attack trials		x		
Website incidents		x		
Website forgery		x	x	
Worms and Viruses		x	x	
DoS	x	x	x	
Damage resource		x	x	
Exposed Information		x	x	
System destruction			x	x
Network Failure			x	x

### A.1.3 Damage scale of incidents

**Table A.3 — Example of Damage Scale of Incident**

Criteria	Description of Damage Scale
Very Important	<ul style="list-style-type: none"> <li>- The credit rating of the monitoring organization is expected to be lowered</li> <li>- Core services are stopped</li> <li>- Financial loss is fatal</li> </ul>
Important	<ul style="list-style-type: none"> <li>- Core services are jammed</li> <li>- Huge amount of information is exposed</li> <li>- Financial loss is considerable</li> </ul>
Moderate	<ul style="list-style-type: none"> <li>- The impact to core services is partial</li> <li>- Information leakage is minor</li> <li>- Financial loss is minor</li> </ul>
Low	-Impact to core services is potentially possible

### A.1.4 Importance of the Information/system

**Table A.4 — Example of Information/System importance**

Criteria	Description
Very Important	Operate majority tasks, Core tasks are processed through the information system (Core tasks are jammed in case of incident)
Important	Core tasks are partially processed through the information system (Core tasks are partially jammed in case of incident)
Moderate	Few core tasks are processed through the information system (Impact is low in case of incident)
Low	No core task is processed through the information system (No impact is applied in case of incident)

## A.2 Incident alarm level

Incident alarm level is classified into four levels: Concerned (Blue), Cautious (Yellow), Alert (Orange), and Serious (Red), (Normal is exempted).

**Table A.5 — Examples of Incident alarm level**

Criteria	Description
Serious (Red)	The incidents is spread out over the entire country
Alert (Orange)	Incident is verified to impact numerous organizations network/system failures and/or spread out to other organizations
Cautious (Yellow)	Incident is verified to impact several organization network/system failures and/or their vulnerability is increased.
Concerned (Blue)	<ul style="list-style-type: none"> <li>- The damage possibility is increased by worms, viruses, and hacking trials</li> <li>- System's damage is concerned by the spread of overseas attacks</li> <li>- The damage is verified similar vulnerability causes by exposed vulnerabilities</li> </ul>

## **Annex B**

### **(informative)**

## **Example information security event, incident and vulnerability reports and forms**

### **B.1 Introduction**

This annex contains example items to be recorded for information security events, incidents and vulnerabilities and example forms for reporting on information security events, incidents and vulnerabilities, with related notes. It is emphasized that these are examples. There are others, such as form the Schema from Incident Object Description and Exchange Format (IODEF) standard.

### **B.2 Example items in records**

#### **B.2.1 Example items of the record for information security event**

This includes basic information of the information security event, such as when, what, how and why the event occurred, as well as the contact information of the reporting person.

- Basic information
  - Date of event
  - Event number
  - Related event and/or incident numbers (if applicable)
- Reporting person details
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Event description
  - What occurred
  - How occurred
  - Why Occurred
  - Initial views on components/assets affected
  - Adverse business impacts
  - Any vulnerability identified
- Event details
  - Date and time the event occurred
  - Date and time the event was discovered
  - Date and time the event was reported

### B.2.2 Example items of the record for information security incident

This includes basic information of the information security incident, such as when, what, how and why the incident occurred, as well as the incident category, impact, and result of incident response.

- Basic information
  - Date of incident
  - Incident number
  - Related event and/or incident numbers (if applicable)
- Reporting person
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Pointy of Contact (PcC) member
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- IRT member details
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Incident description
  - What occurred
  - How occurred
  - Why Occurred
  - Initial views on components/assets affected
  - Adverse business impacts
  - Any vulnerability identified
- Incident details
  - Date and time the incident occurred
  - Date and time the incident was discovered
  - Date and time the incident was reported
- Incident category
- Components/assets affected
- Adverse business impact/effect of incident
- Total recovery cost from incident
- Incident resolution
- Person(s)/perpetrator(s) involved (if incident caused by people)
- Description of perpetrator
- Actual or perceived motivation
- Actions taken to resolve incident
- Actions planned to resolve incident
- Actions outstanding

- Conclusion
- Internal individuals/entities notified
- External individuals/entities notified

### B.2.3 Example items of the record for information security vulnerability

This includes basic information of the information security vulnerability, such as when, what and how the vulnerability was identified, as well as the potential impact and the resolution

- Basic information
  - Date of vulnerability identified
  - Vulnerability number
- Reporting person details
  - Name
  - Contact information such as address, organization, department, telephone and e-mail
- Vulnerability description
- Vulnerability resolution

## B.3 How to use forms

### B.3.1 Format of date and time

Dates should be entered in the format CCYY-MM-DD (and if required HH-MM-SS). If relevant, UTC should be used for ready comparison when many events could be occurring across time zones (and at the least state the UTC offset applied to the time) (See ISO8601).

### B.3.2 Notes for completion

The purpose of the information security event and incident report forms is to provide information about an information security event, and then, if it is determined to be an information security incident, about the incident, to the appropriate people.

If you suspect that an information security event is in progress or may have occurred – particularly one which may cause substantial loss or damage to the organization's property or reputation, you should *immediately* complete and submit an information security event report form (see the first part of this Annex) in accordance with the procedures described in the organization's information security incident management scheme.

The information you provide will be used to initiate appropriate assessment, which will determine whether the event is to be classified as an information security incident or not, and if it is any remedial measures necessary to prevent or limit any loss or damage. Given the potentially time-critical nature of this process, *it is not essential to complete all fields in the reporting form at this time.*

If you are a PoC member reviewing already completed/part-completed forms, then you will be required to take a decision as to whether the event needs to be classified as an information security incident. If an event is classified as such, you should complete the information security incident form with as much information as you are able and forward both the information security event and incident forms to the IRT. Whether the information security event is classified as an incident or not, the information security event/incident/vulnerability database should be updated.

If you are an IRT member reviewing information security event and incident forms forwarded by a PoC member, then the incident form should be then updated as the investigation progresses and related updates made to the information security event/incident/vulnerability database.

The purpose of the information security vulnerability report form is to provide information about a perceived vulnerability, and to act as the repository of information on the resolution of the reported vulnerability.

Please observe the following guidelines when completing the forms:

- The form is recommended to be completed and submitted electronically<sup>1</sup>. (When problems exist, or are considered to exist, with electronic reporting mechanisms (e.g. e-mail), including when it is thought possible that the system is under attack and report electronic forms could be read by unauthorized people, then alternative means of reporting should be used. Alternative means could include in person, by telephone or text messaging.)
- Only provide information you know to be factual – do not speculate in order to complete fields. Where it is necessary to provide information you cannot confirm, please clearly state that the information is unconfirmed, and what leads you to believe it may be true.
- You should provide your full contact details. It may be necessary to contact you – either urgently or at a later date – to obtain further information concerning your report.

If you later discover that any information you have provided is inaccurate, incomplete or misleading, you should amend and re-submit your form.

---

<sup>1</sup> For example in secure web page form with linkage to the electronic information security event/incident/ vulnerability database. In today's world, to operate a paper-based scheme would be time consuming. However, paper-based scheme is also needed to prepare for the case which electronic scheme can not be used.



B.4 Example forms

B.4.1 Example form for information security event report

Information Security Event Report

1. Date of Event

2. Event Number<sup>2</sup>

3. (If Applicable)  
Related Event  
and/or Incident  
Identity Numbers

Page 1 of 1

4. REPORTING PERSON DETAILS

4.1 Name

4.2 Address

4.3 Organization

4.4 Department

4.5 Telephone

4.6 E-mail

5. INFORMATION SECURITY EVENT DESCRIPTION

5.1 Description of the Event:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

6. INFORMATION SECURITY EVENT DETAILS

6.1 Date and Time the Event Occurred

6.2 Date and Time the Event was Discovered

6.3 Date and Time the Event was Reported

6.4 Is the Response to this Event Closed?  
*(tick as appropriate)*

YES☐

NO☐

6.5 If yes, Specify How Long the Event has  
Lasted in Days/Hours/Minutes

<sup>2</sup> Event numbers should be allocated by the organization's IRT Manager.

## B.4.2 Example form for information security incident report

## Information Security Incident Report

1. Date of Incident

Page 1 of 6

2. Incident Number<sup>3</sup>3. (If Applicable)  
Related Event  
and/or Incident  
Identity Numbers

## 4. POINT OF CONTACT MEMBER DETAILS

4.1 Name

4.2 Address

4.3 Organization

4.4 Department

4.5 Telephone

4.6 E-mail

## 5. IRT MEMBER DETAILS

5.1 Name

5.2 Address

5.3 Organization

5.4 Department

5.5 Telephone

5.6 E-mail

## 6. INFORMATION SECURITY INCIDENT DESCRIPTION

## 6.1 Further Description of the Incident:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

## 7. INFORMATION SECURITY INCIDENT DETAILS

7.1 Date and Time the Incident Occurred

7.2 Date and Time the Incident was Discovered

7.3 Date and Time the Incident was Reported

7.4 Identity/Contact Details of Reporting Person

7.5 Is the Incident Over? (tick as appropriate)

YES ☐NO ☐7.6 If yes, Specify How Long the Incident has  
Lasted in Days/Hours/Minutes

<sup>3</sup> Incident numbers should be allocated by the organization's IRT Manager, and linked to the associated event numbers.

# Information Security Incident Report

Page 2 of 6

## 8. INFORMATION SECURITY INCIDENT CATEGORY

(Tick one, then  
complete related  
section below.)

**8.1 Actual**  
(incident has occurred)

☐

**8.2 Suspected**  
(incident thought to have occurred but not  
confirmed)

☐

(One of) **8.3 Natural disaster**

☐

(indicate threat types involved)

☐ Earthquake  
☐ Lightning

☐ Volcano  
☐ Tsunami

☐ Flood  
☐ Collapse

☐ Violent wind  
☐ Other

Specify:

(One of) **8.4 Social unrest**

☐

(indicate threat types involved)

☐ Protest

☐ Terrorist assault

☐ War

☐ Other

Specify:

(One of) **8.5 Physical damage**

☐

(indicate threat types involved)

☐ Fire

☐ Water

☐ Electrostatic

☐ Abominable environment (such as pollution, dust, corrosion, freezing)

☐ Destruction of equipment

☐ Destruction of media

☐ Theft of equipment

☐ Theft of media

☐ Loss of equipment

☐ Loss of media

☐ Tampering with equipment

☐ Tampering with media

☐ Other

Specify:

(One of) **8.6 Infrastructure failure**

☐

(indicate threat types involved)

☐ Power-supply failure

☐ Networking failure

☐ Air-conditioning failure

☐ Water-supply failure

☐ Other

Specify:

(One of) **8.7 Radiation disturbance**

☐

(indicate threat types involved)

☐ electromagnetic radiation

☐ Electromagnetic pulse

☐ Electronic jamming

☐ Voltage fluctuation

☐ Thermal radiation

☐ Other

Specify:

(One of) **8.8 Technical failure**

☐

(indicate threat types involved)

☐ Hardware failure

☐ Software malfunction

☐ Overloading (saturating the capacity of information systems)

☐ Breach of maintainability

☐ Other

Specify:

# Information Security Incident Report

Page 3 of 6

## 8. INFORMATION SECURITY INCIDENT CATEGORY

(One of) **8.9 Malware** ☐ (indicate threat types involved)

- ☐ Network worm    ☐ Trojan horse    ☐ Botnet    ☐ Blended attacks  
☐ Malicious code embedded web page    ☐ Malicious code hosting site    ☐ Other

Specify:

(One of) **8.10 Technical attack** ☐ (indicate threat types involved)

- ☐ Network scanning    ☐ Exploitation of vulnerability    ☐ Exploitation of backdoor  
☐ Login attempts, Interference    ☐ Denial of Service (DoS)    ☐ Other

Specify:

(One of) **8.11 Breach of rule** ☐ (indicate threat types involved)

- ☐ Unauthorized use of resources    ☐ Breach of copyright    ☐ Other

Specify:

(One of) **8.12 Compromise of functions** ☐ (indicate threat types involved)

- ☐ Abuse of rights    ☐ Forging of rights    ☐ Denial of actions    ☐ Mis-operations  
☐ Breach of personnel availability    ☐ Other

Specify:

(One of) **8.13 Compromise of information** ☐ (indicate threat types involved)

- ☐ Interception    ☐ Spying    ☐ Eavesdropping    ☐ Disclosure  
☐ Masquerade    ☐ Social engineering    ☐ Network phishing    ☐ Theft of data  
☐ Loss of data    ☐ Tampering with data    ☐ Data error    ☐ Data flow analysis  
☐ Position detection    ☐ Other

Specify:

(One of) **8.14 Harmful contents** ☐ (indicate threat types involved)

- ☐ Illegal contents    ☐ Panic contents    ☐ Malicious contents  
☐ Abusive contents    ☐ Other

Specify:

**8.15 Others** ☐ (If not yet established whether incident belongs to the above category, tick here)

Specify:

# Information Security Incident Report

Page 4 of 6

## 9. COMPONENTS/ASSETS AFFECTED<sup>4</sup>

Components/ Assets Affected (if any) *(Provide descriptions of the components/assets affected by or related to the incident, including serial, license and version numbers where relevant.)*

### 9.1 Information/Data

### 9.2 Hardware

### 9.3 Software

### 9.4 Communications

### 9.5 Documentation

### 9.6 Processes

### 9.7 Other

## 10. ADVERSE BUSINESS IMPACT/EFFECT OF INCIDENT

For each of the following indicate if relevant in the tick box, then against "value" record the level(s) of adverse business impact, covering all parties affected by the incident, on a scale of 1 to 10 using the guidelines for the categories of: Financial Loss/Disruption to Business Operations, Commercial and Economic Interests, Personal Information, Legal and Regulatory Obligations, Management and Business Operations, and Loss of Goodwill. Record the code letters for the applicable guidelines against "Guideline", and if actual costs are known, enter these against "cost".

		VALUE	GUIDELINE(S)	COST
<b>10.1 Breach of Confidentiality</b> (i.e. unauthorized disclosure)	<input type="checkbox"/>			
<b>10.2 Breach of Integrity</b> (i.e. unauthorized modification)	<input type="checkbox"/>			
<b>10.3 Breach of Availability</b> (i.e. unavailability)	<input type="checkbox"/>			
<b>10.4 Breach of Non-Repudiation</b>	<input type="checkbox"/>			
<b>10.5 Destruction</b>	<input type="checkbox"/>			

## 11. TOTAL RECOVERY COSTS FROM INCIDENT

(Where possible, the actual total costs of recovery for the incident as a whole should be shown, against "value" using the 1 to 10 scale and against "cost" in actuals.)

VALUE	GUIDELINES	COST
-------	------------	------

<sup>4</sup> This is for more details of the components/assets affected if available as investigation and analysis proceeds (in the early stages of event and incident analysis normally only 'high level' information will be collected).

# Information Security Incident Report

Page 5 of 6

## 12. INCIDENT RESOLUTION

12.1 Incident Investigation Commenced Date

12.2 Incident Investigator(s) Names(s)

12.3 Incident End Date

12.4 Impact End Date

12.5 Incident Investigation Completion Date

12.6 Reference and Location of Investigation Report

## 13. (IF INCIDENT CAUSED BY PEOPLE) PERSON(S)/PERPETRATOR(S) INVOLVED

(One of)

Person ☐

Legally Established Organization/Institution ☐

Organized Group ☐

Accident ☐

No Perpetrator ☐

*e.g. natural elements, equipment failure, human error*

## 14. DESCRIPTION OF PERPETRATOR

## 15. ACTUAL OR PERCEIVED MOTIVATION

(One of)

Criminal/Financial Gain ☐

Pastime/Hacking ☐

Political/Terrorism ☐

Revenge ☐

Other ☐

*Specify:*

## 16. ACTIONS TAKEN TO RESOLVE INCIDENT

*(e.g. 'no action', 'in-house action', 'internal investigation', 'external' investigation by ...')*

## 17. ACTIONS PLANNED TO RESOLVE INCIDENT

*(e.g. see above examples)*

## 18. ACTIONS OUTSTANDING

*(e.g. investigation is still required by other personnel)*

Information Security Incident Report

19. CONCLUSION

(tick to indicate that the incident is considered Major or Minor, and include a short narrative to justify the conclusion

Major ☐ Minor ☐

(indicate any other conclusions)

20. INTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)

<input type="checkbox"/>	Information Security Manager/ Responsible Official	<input type="checkbox"/>	IRT Manager	<input type="checkbox"/>
<input type="checkbox"/>	Site Manager (state which site)	<input type="checkbox"/>	Information Systems Manager	<input type="checkbox"/>
<input type="checkbox"/>	Report Originator	<input type="checkbox"/>	Report Originator's Manager/ Line User Management Affected	<input type="checkbox"/>
			Other (e.g. Help Desk, Human Resources, Management, Internal Audit,	<input type="checkbox"/>

Specify:

21. EXTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)

<input type="checkbox"/>	Police	<input type="checkbox"/>	Other (e.g. Regulatory Body, External IRT	<input type="checkbox"/>
--------------------------	--------	--------------------------	---	--------------------------

Specify:

21. SIGN-OFFS

ORIGINATOR	REVIEWER	REVIEWER
Digital Signature	Digital Signature	Digital Signature
Name	Name	Name
Role	Role	Role
Date	Date	Date

## B.4.3 Example form for information security vulnerability report

# Information Security Vulnerability Report

1. Date Vulnerability identified

Page 1 of 1

2. Vulnerability Number<sup>5</sup>

### 3. REPORTING PERSON DETAILS

3.1 Name

3.2 Address

3.3 Organization

3.4 Department

3.5 Telephone

3.6 E-mail

### 4. INFORMATION SECURITY VULNERABILITY DESCRIPTION

4.1 Date and Time the Vulnerability Reported

4.2 Description in Narrative Terms of the Perceived Information Security Vulnerability:

- How Vulnerability Noticed
- Characteristics of Vulnerability – Physical, Technical, etc.
- If Technical, what IT/Networking Components/Assets Concerned
- Components/Assets that might be Affected if Vulnerability were to be Exploited
- Potential Adverse Business Impacts if Vulnerability were to be Exploited

### 5. INFORMATION SECURITY VULNERABILITY RESOLUTION

5.1 Has Vulnerability been Confirmed? (tick as appropriate)

YES ☐

NO ☐

5.2 Date and Time of Vulnerability Confirmation

5.3 Name of Person Authorising

5.4 Address

5.5 Organization

5.6 Telephone

5.7 E-mail

5.8 Has Vulnerability been Resolved? (tick as appropriate)

YES ☐

NO ☐

5.9 Description in Narrative Terms of how Information Security Vulnerability has been Resolved, with Date and Name of Person Authorising Resolution

<sup>5</sup> Vulnerability numbers should be allocated by the organization's IRT Manager.



## Bibliography

- [1] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
- [2] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*
- [3] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*
- [4] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*
- [5] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*
- [6] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
- [7] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [8] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*
- [9] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*
- [10] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*
- [11] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways — Threats, design techniques and control issues*
- [12] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*
- [13] ISO/IEC 27041, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of investigation methods*
- [14] ISO/IEC 27042, *Information technology — Security techniques — Guidelines for the analysis & interpretation of digital evidence*
- [15] ISO/IEC 27043, *Information technology — Security techniques — Investigation principles and processes*
- [16] ISO/IEC 27044, *Information technology — Security techniques — Security information and event management (SIEM)*
- [17] ISO/IEC 8601, *Data elements and inter change formats — Information interchange — Representation of dates and times*
- [18] Internet Engineering Task Force (IETF) Site Security Handbook, <http://www.ietf.org/rfc/rfc2196.txt?number=2196>

- [19] Internet Engineering Task Force (IETF) RFC 2350, Expectations for Computer Security Incident Response, <http://www.ietf.org/rfc/rfc2350.txt?number=2350>
- [20] NIST Special Publication 800-61, Computer Security Incident Handling Guide (2004), <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>
- [21] Internet Engineering Task Force (IETF) RFC 3227, Guidelines for evidence collection and archiving
- [22] Internet Engineering Task Force (IETF) RFC 5070, The Incident Object Description Exchange Format (IODEF)