THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
High Commission for National Protection

Governmental CERT

Incident Categories (Public)

Version 6.0 - 2024-09-20 (Final)

Procedure (PRO 303)

TLP: **TLP:CLEAR**

Contents

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

1 Introduction

1.1 Overview

After receiving an incident report, it's crucial to handle it rapidly and efficiently to assist the constituent in resolving the incident. The categorisation of incidents helps GOVCERT.LU to plan appropriate actions and sets a clear reporting time frame to the constituent.

The categorisation of incidents also helps to identify standard incident response procedures related to the type of incident.

1.2 Purpose

The aim of this procedure is to define:

- the incident categories used by GOVCERT.LU
- how a category is allocated to an incident
- the reporting time frame for constituents for each type of incident

1.3 Scope

This procedure concerns the GOVCERT.LU ticketing tool, its members and its constituents.

1.4 References

1. *PRS401 - Incident Management Process*
2. *Reference Incident Classification Taxonomy, Task Force Status and Way Forward*. URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

1.5 Abbreviations

Abbreviation	Definition
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
ENISA	European Network and Information Security Agency
ICMP	Internet Control Message Protocol
IoC	Indicator of Compromise
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
VNC	Virtual Network Computing
WPAD	Web Proxy Auto-Discovery Protocol

Table 1: Abbreviations

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

2 Definitions

2.1 Event

An event is an occurrence or change of a particular set of circumstances:

NOTE 1: An event can be one or more occurrences, and can have several causes.

NOTE 2: An event can consist of something not happening.

NOTE 3: An event can sometimes be referred to as an “incident” or “accident”.

2.2 Information security event

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

2.3 Information security incident (or incident)

An information security incident (or incident) is a single or a series of unwanted or unexpected information security events (section 2.2) that have a significant probability of compromising business operations and threatening information security[1].

2.4 Critical system

A critical system is a system, an application, data or other resource that is essential to the survival of an organisation. When a critical system fails or is interrupted, core operations are significantly impacted.

2.5 Non critical system

A non critical system is a system, an application, data or other resource which does not have strong impacts to the regular business operation of a constituent if compromised.

[1] where *information security* means preservation of confidentiality, integrity and availability of information

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

3 Incident categories

Each category in table 2 is enumerated with an identifying number, a name, a description and a *reporting time frame*. The latter is the time frame within which the impacted constituent should report the incident. The incident *reporting time frames* defined in Table 2 are recommended by GOVCERT.LU to ensure efficient and appropriate handling of an incident. The *reporting time frames* are defined according to the importance of the targeted system(s).

Below is a high level set of concepts and descriptions to categorise information security incidents:

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

CAT	Name & description	Reporting time frame after discovery	
		Critical system	Non critical system
1	**Information Content Security** Unauthorised access to information, modification of information or loss of data: - by abusing stolen login credentials for a system or application - intercepting traffic - gaining access to physical documents - a ransomware encrypting data - loss of data caused by hard disk failure or physical theft	Within 1 hour.	Within 4 hours.
2	**Intrusions** Compromise of a system or an application where the attacker: - gained administrative privileges - used an unprivileged (user/service) account - exploited (un-)known software vulnerabilities, e.g. SQL injection Physical intrusion, e.g. into corporate building or data-centre.	Within 1 hour.	Within 1 hour.
3	**Malicious Code** System infected with malware, e.g. PC, smartphone or server infected with a rootkit or which contacted a command-and-control (C2) server. URI used for malware distribution or malware configuration, e.g. a URL included in fake invoice or web-injects for a banking trojan.	Within 1 hour.	Within 4 hours.
4	**Availability** Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down, SYN-Floods or UDP-based reflection attacks. Physical sabotage or outage, e.g cutting wires or malicious arson or caused by air condition failure or natural disaster.	Within 2 hours if the attack is still ongoing and the organisation is unable to successfully mitigate activity.	Within 4 hours if the attack is still ongoing and the organisation is unable to successfully mitigate activity.
5	**Fraud** - Using resources for unauthorised purposes including profit-making ventures. - Offering or installing copies of unlicensed commercial software or other copyright protected materials (Warez). - Impersonation of the identity of another entity in order to benefit from it. - Masquerading as another entity in order to persuade the user to reveal private credentials (phishing).	Within 4 hours.	Within 1 day.
6	**Abusive Content** - SPAM, IoCs referring to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc. - Discrimination of somebody - Child sexual exploitation, sexual content, glorification of violence, etc.	Within 4 hours.	Within 1 day.

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

CAT	Name & description	Reporting time frame after discovery	
		Critical system	Non critical system
7	**Information Gathering** - Attacks that send requests to a system to discover weaknesses. e.g. fingerd, DNS querying, ICMP, SMTP, port scanning. - Observing and recording of network traffic (wiretapping). - Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).	Within 1 hour.	Within 2 weeks.
8	**Intrusion Attempts** - An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.) - Multiple login attempts (Guessing / cracking of passwords, brute force). - An attack using an unknown exploit.	Within 1 hour.	Within 2 weeks.
9	**Vulnerable** - Publicly accessible services offering weak crypto (e.g. web servers susceptible to POODLE/FREAK attacks). - Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks (e.g. open DNS resolvers). - Potentially unwanted publicly accessible services (e.g. Telnet, RDP or VNC). - Publicly accessible services potentially disclosing sensitive information (e.g. SNMP or Redis). - A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (e.g. WPAD, outdated operating system version, etc.).	Within 6 hours.	Within 1 week.
10	**Other** All incidents which do not fit in one of the given categories should be put into this class or the incident is not categorised.	Within 6 hours.	Within 1 day.
11	**Test** Meant for testing.	Not applicable.	Not applicable.

Table 2: Information security incident categories

The categories and attacks are based on the categories proposed by European Network and Information Security Agency (ENISA) in *Reference Incident Classification Taxonomy, Task Force Status and Way Forward*[2].

3.1 Category allocation

Table 2 describes all the categories of incidents. A category is allocated to an incident by the constituent and GOVCERT.LU according to the following flow chart:

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

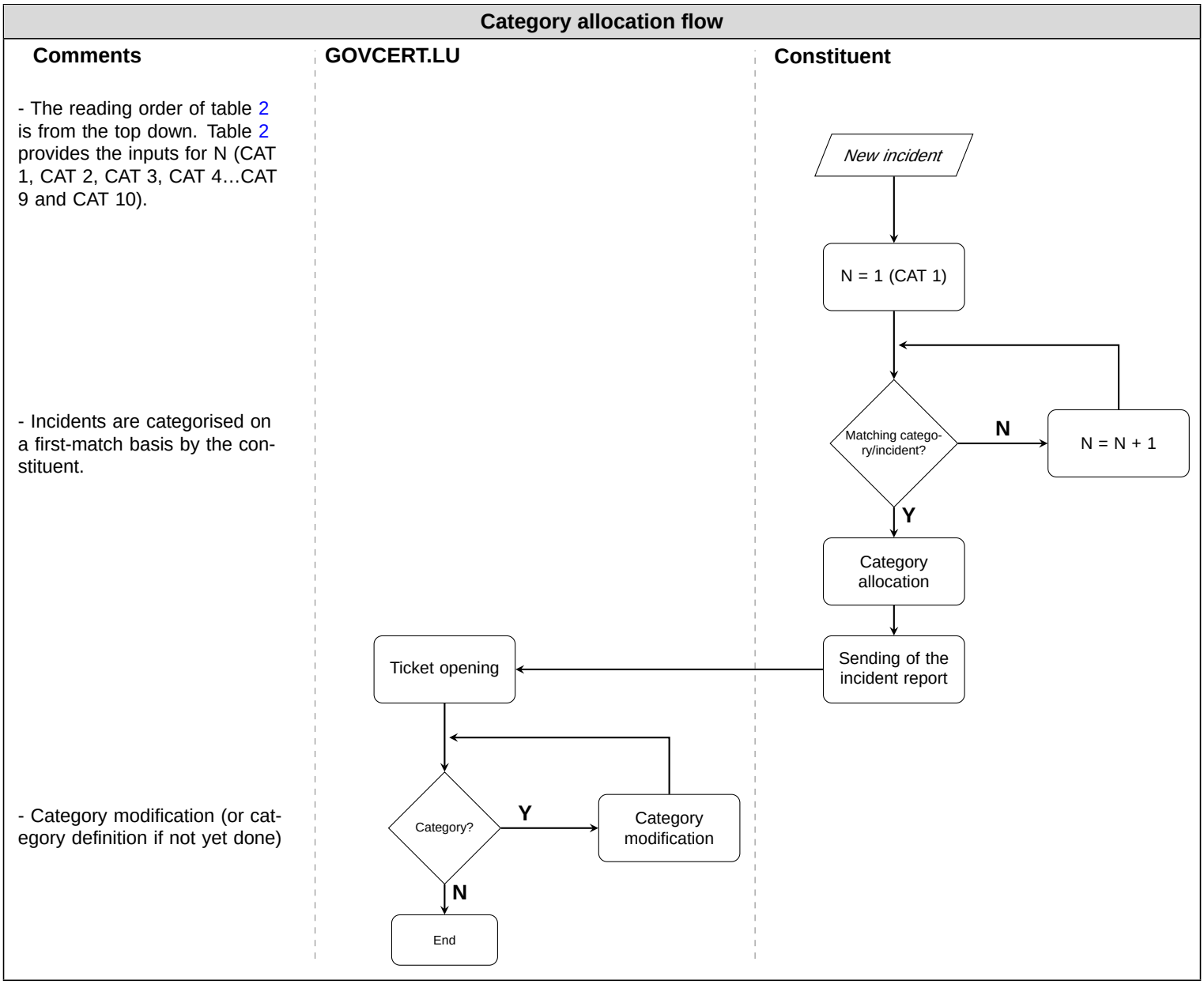

Figure 1: Category allocation flow

During the *identification phase*[2] GOVCERT.LU defines the category that fits best such as described in figure 1. In summary, the reading order of table 2 is top to bottom and the first category which matches with the incident is chosen (i.e. first match basis).

[2] See *PRS401 - Incident Management Process*

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu