



CONSULTATION DOCUMENT

Effecting Measures towards enhancing the security and integrity of Electronic Communications Networks and Services

Initiative #2 – Revision of the Incident Reporting Mechanism

MCA Reference: MCA/C/23-4803

Publication Date: 6th January 2023

 (+356) 2133 6840  info@mca.org.mt  www.mca.org.mt/


 Valletta Waterfront, Pinto Wharf, Floriana FRN1913, Malta

TABLE OF CONTENTS

1	Introduction.....	1
2	Incident Reporting Process.....	3
2.1	Assessment of the type of incident.....	5
2.2	Assessment of the scale of an Incident.....	7
3	Assessing the Scale of Impact of Subscriber Oriented Incidents.....	10
3.1	Loss of Availability.....	11
3.2	Loss of Integrity, Authentication and Privacy.....	15
3.3	Loss of Services which are Required at Law.....	15
4	Assessment of Scale of a Network Oriented Incident.....	17
5	Incident Reporting and Notification.....	20
5.1	Notification of Incidents to the Authority.....	21
5.2	Reporting and Statistics.....	22
5.3	Simplification of Incident Reporting.....	24
6	Data collection requirements.....	26
7	Applicable timeframes for the implementation and review of the proposed initiative.....	27
8	Incident Reporting template.....	28
8.1	Incident Reporting Template (Level 1).....	28
8.2	Incident Reporting Template (Level 2 or over).....	29
9	Consultation Questions.....	40
10	Invitation to Comments.....	41

1 Introduction

Incident reporting is an essential tool within the cycle of incident management, and it is equally important both for the provider of electronic communications networks and services and for the Malta Communications Authority (hereafter the 'Authority' or 'MCA') when fulfilling its supervisory functions in ensuring the appropriate safeguarding of the security of electronic communications networks and services.

From the point of view of the providers, incident analysis and documentation forms part of the information that feeds into the risk assessment cycle. The analysis phase could be instrumental to uncover security risks the nature of which may fall into any of the following categories:

1. Risks that were contemplated by the risk assessment but the probability of occurrence and the cost of mitigation did not match up with the cost incurred to suffer the incident.
2. Risks that were contemplated during the risk assessment, and while a set of mitigation measures were planned and implemented, it results that further aspects of the risk need to be addressed.
3. Risks that were never contemplated because these were either latent to the risk assessment process or the nature of the environment in which the networks and services operate have changed and are now presenting new challenges.

Incident analysis is an opportunity for electronic communication networks and services providers to evaluate their risk assessment and ensure its continuous appropriateness throughout its lifeline.

From the point of view of the Authority, incident reporting serves various purposes as highlighted below:

1. Given that the Authority shall receive detailed information about the major incidents from all the ECS and ECN providers, it is expected that it shall also be better placed to understand the risks to which the ECN and ECS sector is exposed.
2. Electronic communication services often play a critical role in other services, which are themselves either critical or essential in some form or other to society and to the economy of the country. Therefore, incident reporting is also a means of understanding how the risks to the ECN and ECS will also highlight other important and critical services.
3. Incident reporting is also an effective means of understanding the level of maturity achieved by the individual network and service providers in terms of managing the security risks of their networks and, or services.

While noting the importance of incident management and internal documentation is treated in a separate consultation, this Consultation will focus solely on that aspect of incident management where incidents have to be reported to the Authority. Within this context, this consultation will only seek to:

1. **Identify which incidents are reportable to the Authority.** One of the main aims of the Authority is to collect information about those incidents, which, when addressed properly, will result in a considerable improvement in network security. Instead of collecting detailed information about each incident, the Authority is proposing an approach whereby incidents that cause significant impact on the networks, services and their subscribers stand a good chance of bearing the most valuable information to the whole sector. Therefore, one of the key processes proposed in this paper is to identify the scale and severity of incidents.
2. **Establish a tool that facilitates the assessment of the impact of a security incident.** The proposed method aims at achieving a level of harmonisation across the different networks and service providers as well as across the different networks and services on offer.
3. **Determine the information that should reach the Authority.** The proposal will establish both the expected details to be conveyed to the Authority as well as the urgency to be applied when reporting the incident.

The Authority notes that given the overlap between the existing guidelines on incident reporting and the proposed decision on incident reporting, the decision will also repeal the current guidelines.

2 Incident Reporting Process

Regulations 28 to 30 of SL 399.48 require that providers of electronic communication networks and services are required to ensure that the electronic communications networks and services can withstand within reason those actions that attempt to compromise the **availability**, **authenticity**, **integrity** and **confidentiality** of the networks or services. These regulations also requires that networks and services shall be so designed not only to ensure their own security but also to extend the protection towards (a) other related services that they offer or that are accessible through them; and (b) any data that is stored, transmitted or processed by the network and service.

Any event that leads to a breach of any of these security properties, whether in full or in part, is deemed a security incident. Experiencing security incidents is part of the life cycle of a network. However, the scale of impact of a security incident will vary depending on a multitude of factors, including the environment and events leading up to the incident, the type of action causing the incident, the level of technical, administrative and operational preparedness of the network to withstand the attack and contain the effects of the incident.

Figure 1 below outlines a general process around which the proposals in this paper are built. The process consists of two main building blocks where the provider is required to carry out an (a) assessment of the type of incident and (b) evaluate the severity of the incident.

The following sections will discuss these processes in detail.

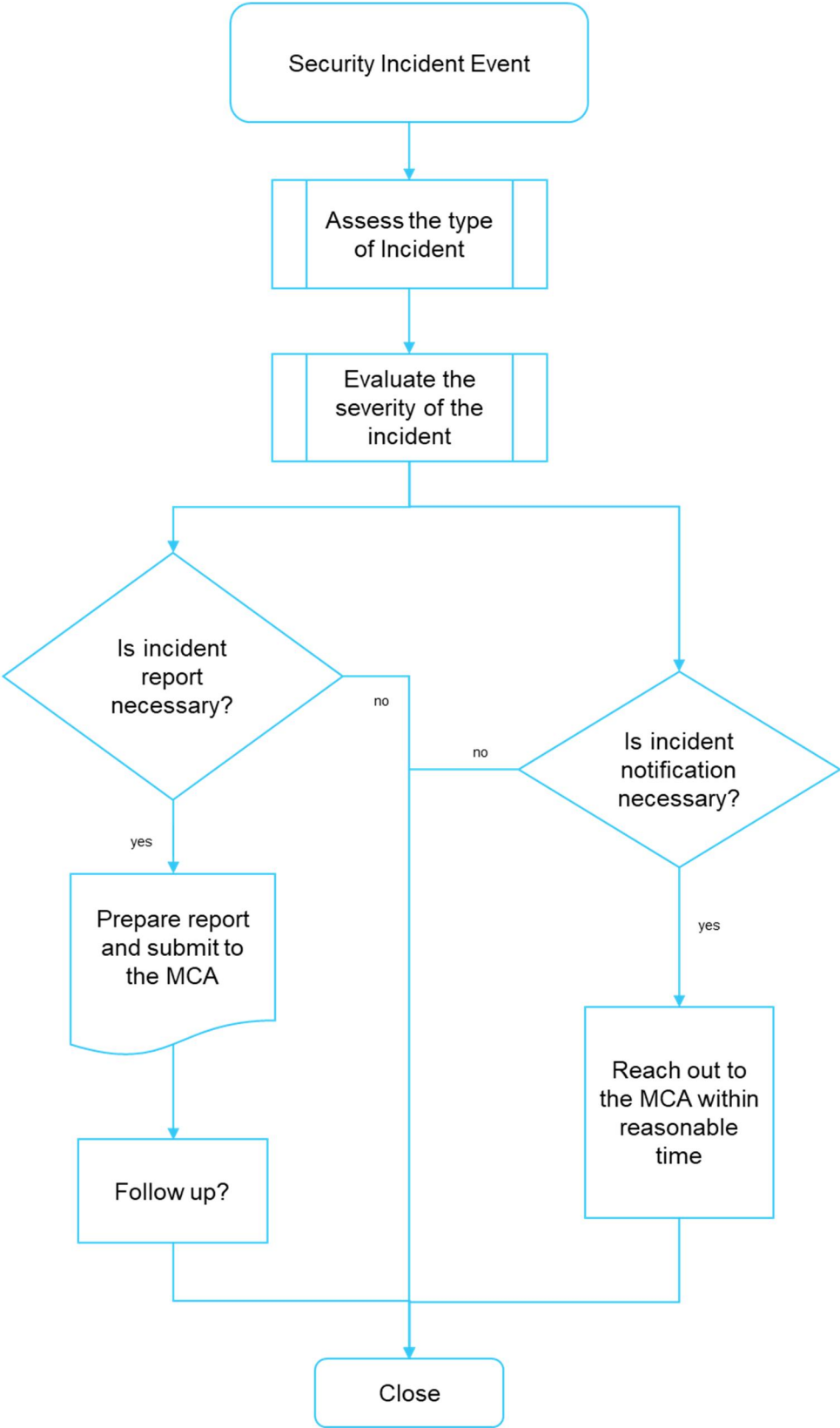


Figure 1 Overview of Incident Reporting Process

2.1 Assessment of the type of incident

Security incidents are events that cause systems to fail by exposing them to conditions that are beyond their design point. Therefore, by nature, the outcome of an incident is theoretically unpredictable. This analysis aims to group, as much as possible, incidents that are similar in nature to extract their commonalities. It is understood that while the nature of some incidents will fit neatly within the assessment proposed, there will remain some scenarios where, due to various reasons, this will not be possible. In such circumstances, a case-by-case evaluation would be necessary.

2.1.1 Subscriber Oriented Incidents

This Consultation paper proposes that incidents that caused tangible disruptions to the subscribers are separated from those that did not result in direct tangible disruptions to the subscribers but rather had an indirect impact on the network, possibly by degrading the level of service offered or by decreasing the level of protection available against security incidents.

The first group of incidents, termed "Subscriber Oriented Incidents", will primarily include incidents where the **availability** of networks and services is impacted. Loss of availability typically gets an immediate response from the subscriber as the service or parts thereof is not available and therefore, the service is not fulfilling the needs of the subscriber. Subscriber Oriented Incidents shall also include those incidents where the network has suffered from loss of **integrity**, **authenticity** and **confidentiality**. Although it is unlikely for the subscriber to be immediately aware of these network issues, these incidents typically expose subscriber data to risks that are of great concern to the subscriber.

Figure 2 summarises all types of incidents that could be grouped under the umbrella of subscriber oriented incidents. Given their nature, this Consultation will place significant importance to discuss them in detail.

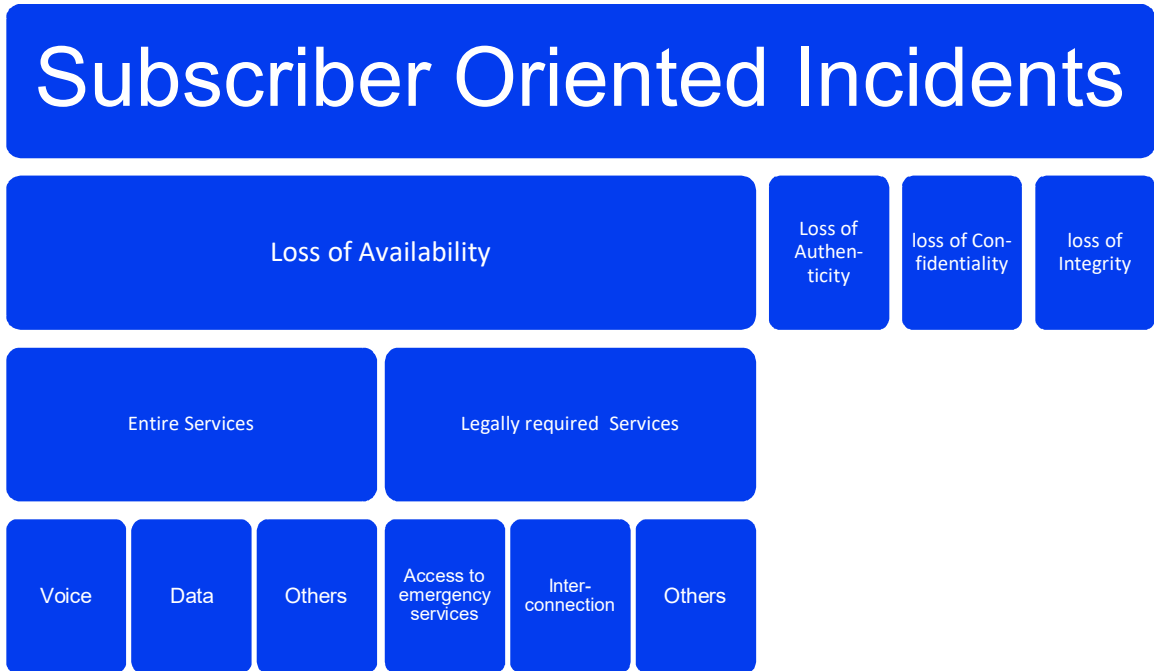


Figure 2 Subscriber Oriented Incidents

2.1.2 Network Oriented Incidents

Security incidents such as the loss of power backups, or the loss of redundancy, are incidents which might not result in a direct impact to the subscriber. Nevertheless, these incidents are still of interest as they may result in a reduction in the quality of service offered or networks which stand in a prolonged state of vulnerability, thus increasing the risk of more catastrophic incidents.

Incidents that cause the network to be in a state where some of its services are partially disrupted e.g. reduced capacity, or where the network itself is brought to a state where planned redundancies are compromised either partially or in full, shall be termed "Network Oriented Incidents". **Error! Reference source not found.** 3 below summarises the idea.

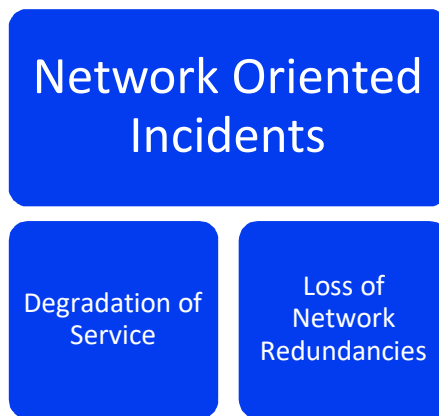


Figure 3 Network Oriented Incidents

Consultation Questions

- IR 1** What are your views on the proposal to classify incidents as Subscriber Oriented Incidents and Network Oriented Incidents?
- IR 2** From your experience, if any, how feasible is it to adopt the proposed incident classification system? Qualify your response.

2.2 Assessment of the scale of an Incident

This section treats at length the type and method of assessment required to determine the scale and impact of an incident and hence later determine the level of reportability of an incident.

The main point of the process is to determine whether an incident is Subscriber Oriented or Network Oriented given that these are then treated differently along the overall process.

By their nature, Subscriber Oriented Incidents are the more severe type, as their impact reaches the subscribers directly and hence merit more detailed attention. Network Oriented Incidents are, at large, a near-miss type of incidents as redundancy or some other mitigating factor would have avoided a full-scale incident. However, an assessment of the incident is still necessary to ensure the consistent performance of the applied measures and thus assure the robustness of the network, especially in those cases where the network will remain compromised for an extended period as a result of potentially lengthy repair procedures that might be necessary to restore the network.

It is worth noting that in the rare eventuality that multiple failures coincide, a preliminary assessment shall be required to establish whether these incidents are related and therefore treated as a chain of cause and effect events, or whether these are completely separate events which merit an independent assessment.

This section has four components. The main sections present the procedure proposed to assess the severity of both the subscriber and network-oriented incidents. Two other sections serve as building blocks to the procedure sections that are presented. In the first section, a method and the necessary considerations for estimating the subscriber base are presented. The second part introduces a standard scale on how different incidents of different magnitudes will be colour-coded.

2.2.1 Color-Coding the severity of Incidents

One of the key processes presented in this paper is to classify the incidents according to their severity. Table 1 below shows a set of four severity levels, starting from incidents with insignificant impact (green) to incidents with severe implications (red). From an administrative perspective, the classification serves the following purposes:

- a) Establish the course of action necessary by the network and service provider in terms of incident reporting and notification
- b) Classify incidents for statistical purposes, providing a means to track the progress in terms of which type of incidents are becoming less or more prevalent
- c) Assist the Authority in justifying any further regulatory considerations that might be necessary to address specific issues in the market.

The details on how an incident is classified are presented later in this consultation paper. This process will involve various factors as applicable to the different types of incidents





Level	Severity	Colour code
Level 0	Incidents of insignificant impact	
Level 1	Low impact incidents	
Level 2	Moderate impact incidents	
Level 3	Severe impact incidents	

Table 1 Classification of security incidents by severity

2.2.2 Estimate of the Subscriber Base

The number of subscribers impacted during an incident is one of the key metrics in measuring the scale of the incident. The market share captured by the different ECN and ECS varies,

resulting in significant disparities in the size and proportion of the networks and services. Therefore, normalisation of impacted subscribers against the subscriber base of the network and or service provider is necessary. This section provides details on how the subscriber base for each network and service provider is estimated to ensure uniformity across the market.

The subscriber base denotes the total number of subscribers that are serviced through a given ECS and ECN. The following considerations shall be taken into account when establishing the metric:

1. In estimating the subscriber base, the provider needs to take note of those subscribers that are serviced both through its own retail arm of its services and, where applicable, through the wholesale arm.
2. Providers offering multiple networks and services shall consider each network and service individually and therefore count the subscribers individually. These services are typically unrelated and not substitutable in function. For example, a single subscriber having voice telephony and fixed broadband service shall be counted as two subscribers – one for each service.
3. In the case of mobile networks, voice telephony, mobile broadband, and text messaging are services that are considered separately. A simcard that has access to any of the services shall count as a single subscriber for every service available. This count shall be equally applied when estimating the market share of the services, and when estimating the number of subscribers impacted during a service outage. Specifically to mobile access, it is common, though not mandatory, for similar services to be offered simultaneously over multiple networks. For example, voice service may be offered over GSM and 3G networks and the user equipment is seamlessly handed over across the networks; similarities also exist for the other services. In such circumstances, access to the same type of service but through multiple seamlessly connected networks will still be considered as a single service offered to a single subscriber. The advantage of having multiple networks servicing the same service shall be reflected in the resilience level provided to the subscriber.

3 Assessing the Scale of Impact of Subscriber Oriented Incidents

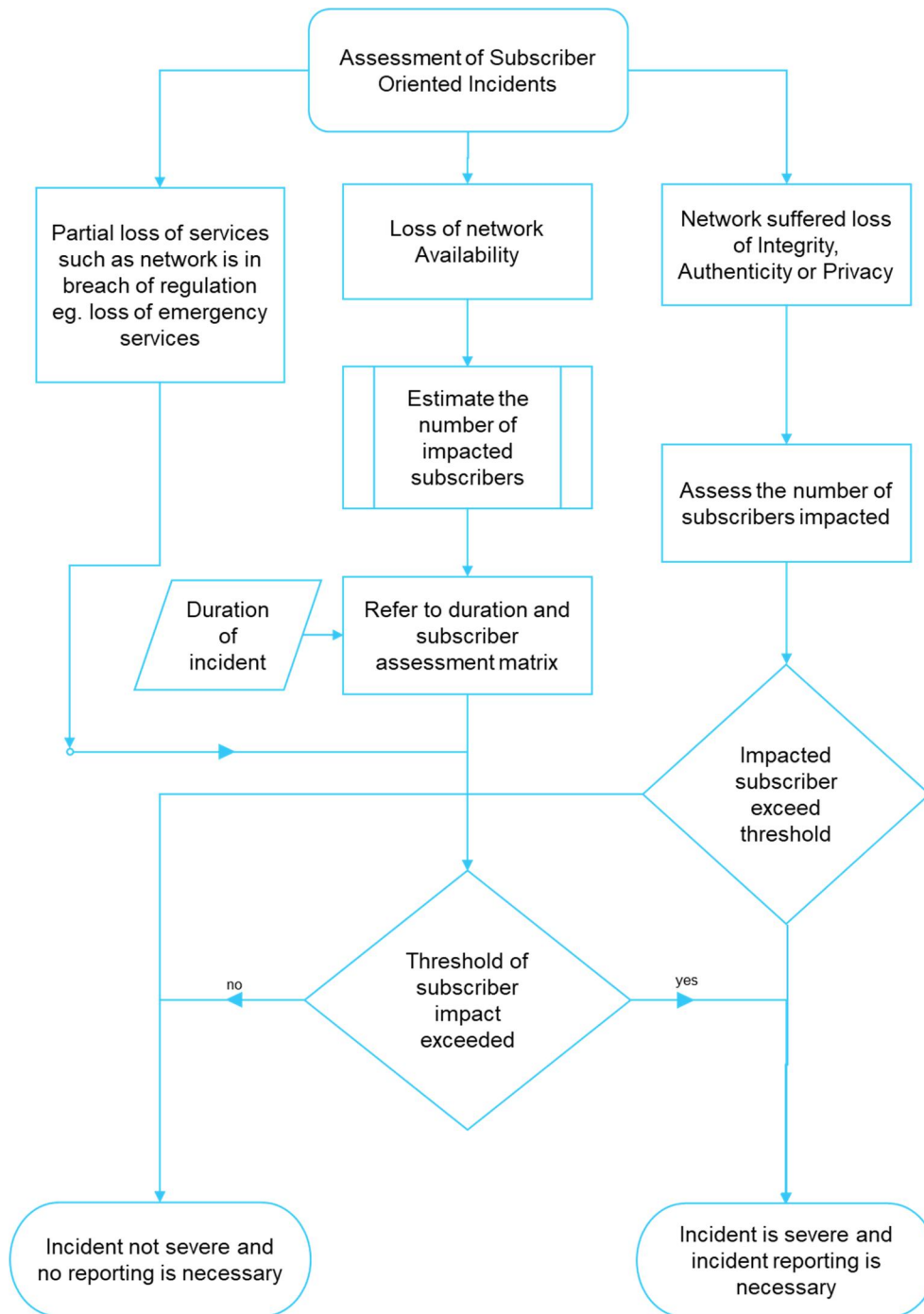


Figure 4 Process for assessing the Subscriber Oriented Incidents

The main goal in assessing the impact of Subscriber Oriented Incidents is to apply a metric that quantifies the number of subscribers impacted. In those cases where the temporal nature of the incident reflects on the impact suffered by the subscriber, then the duration of the incident is also factored in.

The treatment and assessment of Subscriber Oriented Incidents are grouped as follows:

- a) **Loss of Availability of Network and/or Service.** This is applicable for those incidents that result in loss of availability either in whole or part of an electronic communications network and/or services that are available to the subscribers.
- b) **Loss of Integrity, Authenticity and Privacy** are three types of incidents that generally occur within the core network rather than the access network. They are distinct incidents by nature, but a common approach for the assessment of incident severity is presented. The time factor does not come into play as the harm suffered by the subscriber and its data cannot be reversed when the network recovers from the incident. Therefore, identifying the area of origination of the incident and the subscribers impacted are at the core of the assessment required.
- c) **Loss of services that are mandatory at law:** Some electronic communication networks and services are required by law to provide specific services. Incidents that render these mandated services inoperable or unavailable are treated within this group.

The three sections below will detail the applicable procedures for each group.

3.1 Loss of Availability

The scale of impact of the loss of availability is measured using a combination of the number of subscribers impacted and the duration of the incident as the metric defining severity of the impact of the incident. The main idea of this combination is that a few subscribers suffering from loss of service for a long time should have the same significance as a larger group of subscribers impacted for a shorter period of time. Estimating the number of subscribers impacted during an incident may be a somewhat complex task when subscriber mobility is a key network feature. This is treated in detail in the following sub-sections.

Owing to the different sizes of the providers, in terms of market shares, normalising the number of impacted subscribers by the number of subscribers of the provider is necessary. This approach is also similar to that presented by ENISA in its Guidelines on Incident Reporting.

The assessment relevant to fixed networks and mobile networks is very similar. However, the rationale supporting the process differs in both cases and merits separate treatment.

3.1.1 Fixed networks and services

In fixed networks and services, the relationship between the subscribers and the assets involved in delivering the service is static. As the term implies, the subscribers are fixed in location, and therefore mobility plays no role in transferring the subscriber from one asset group to the next, as will be the case for mobile services. This simplifies the task of establishing the number of subscribers impacted during a given incident, as this remains fixed for the whole duration of the incident. Any fluctuations in the number of affected subscribers will only be due to a progressive restoration of the network and service.

On this basis, the Authority proposes that the number of subscribers affected during an incident shall include all those subscribers that are directly associated with the compromised assets, irrespective of whether the subscribers were making actual use of the service or not at the onset of the incident.

3.1.2 Mobile Access Networks and Services

The mobility of subscribers is the key feature of mobile networks. It is also the main attribute of mobile networks that renders the calculation of subscribers impacted during an incident a rather challenging task. Mobility has rather complex implications since subscribers may be on the move, thus detaching from parts of the network and attaching to others. Therefore, unlike fixed networks, a single network asset cannot be associated with a subscriber or a group thereof. In addition, when a network suffers from a partial loss of service, subscribers may move in and out of the affected area, and hence the duration of the incident relative to them may vary.

Mobile networks have different forms of redundancy that help to soften the impact of an incident. At the access layer, a network may have multiple cells covering the same geographic area. This may or may not be a desired or planned feature of the network but an outcome due to other network planning considerations. Therefore, the outcome of this overlap, while it is beneficial to the subscriber in some way or other, is neither consistent nor predictable.

Another form of network redundancy is derived from multiple networks that offer similar services but which are also geographically overlapping. This offers a level of redundancy offered to the subscriber, but the type of quality of the service may differ. For example, both 3G and 4G networks are capable of offering high-speed data services; however, the quality of service differs and therefore, within the context of identifying the impact of a security incident on the subscriber, this level of redundancy may be of a hindrance.

The above considerations clearly show that estimating the number of subscribers impacted during an incident within a mobile network is not trivial, and attempting to achieve highly accurate estimates will quickly become a mammoth task. This is not the purpose of this exercise.

In an attempt to resolve this complexity, the Authority had initially considered the following two methods suitable to trace the number of subscribers:

- a) Mobile network providers may apply mathematical models to estimate the coverage area of a cell and its impact on the network when this is compromised. However, apart from the complexity involved due to the use of sophisticated mobile coverage and prediction tools, there exists a significant risk where mobile service providers will not use the same software models and calibrations, hence rendering the outcomes incomparable.
- b) Mobile network providers may use KPI measurements to track the performance of various network elements, and the loss of service and impact to subscribers could be estimated through rigorous and complex analysis. While this method could provide accurate information, it is inherently complex and requires extensive data gathering and processing from the service provider's side. Moreover, the data collection and processing involved relies on base KPIs that may vary from one supplier to another. This will cause harmonisation issues that lead to results that are not comparable and replicable across the different providers.

Given that none of the above methods can provide an adequate solution that balances the accuracy of the result and the complexity of the process to obtain the result while ensuring comparability across different providers, the Authority is therefore proposing the a simplified approach to estimate the number of impacted subscribers. Whenever mobility issues complicate the process of identifying the impacted subscribers, the impact of the incident is traced down to the network cells, and all the subscribers that were logged onto the cells at the onset of the incident are considered to be all impacted subscribers. This approach hinges on the idea that a network cell is the smallest element in the access network and assumes that when the cell is impacted, all the subscribers logged on to it are affected.

The Authority concedes that this method might not provide the most accurate estimate of the impacted subscribers. However, it should be noted that the accuracy of this estimate improves when the root of the incident moves further from the access network and closer to the core network. In doing so, the associated network elements tend to control physically larger geographical areas of the network, therefore limiting the logical border between the incident impacted area of the network and the remaining one. This in turn reduces the effect of user mobility. This is further combined with the fact that when incidents impact any such network element, an increase in the number of affected subscribers is expected, and therefore the inaccuracies due to subscriber mobility become diluted.

Having established a method of estimating the impact on the subscriber during an incident causing loss of service, Figure 5 below presents the relationship between the impacted subscribers, time and the severity of the incident where, the duration of an incident equates to the time taken for the provider to restore the service to all customers fully

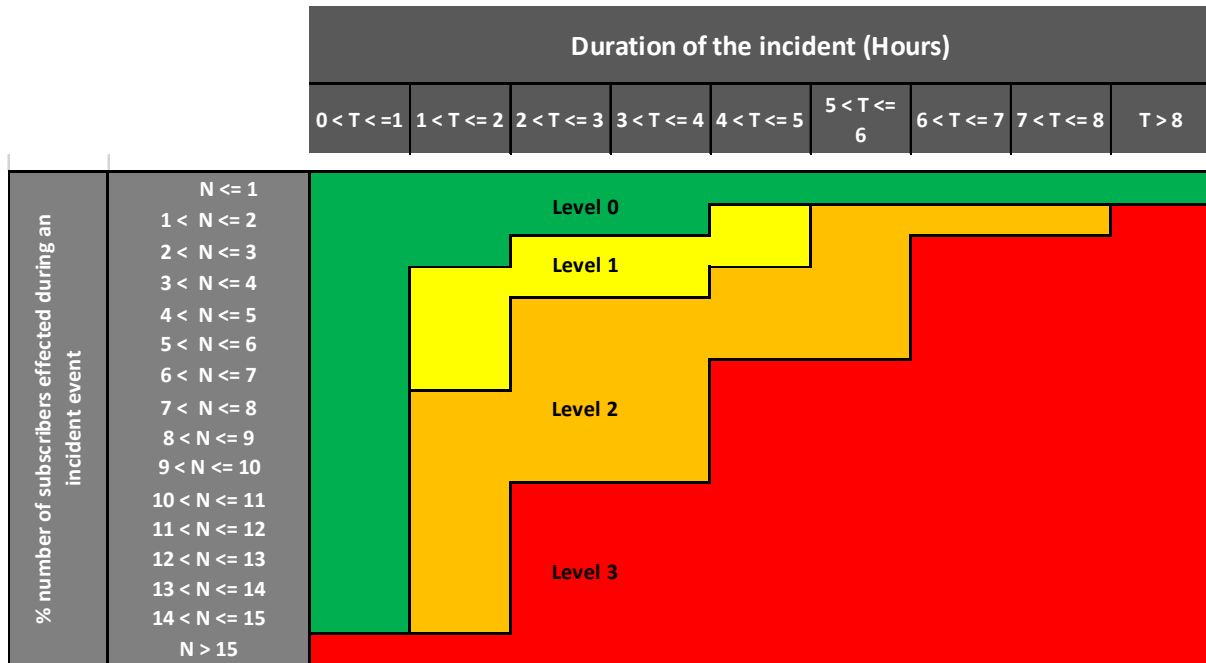


Figure 5 Incident reporting thresholds for fixed and mobile electronic communication networks and/or services and core networks for loss of availability

A security incident is defined as Level 0 if any of the following conditions is true: ■

- It has an impact on up to 1 % of the subscribers, irrespective of the duration of the incident.
- It lasts for up to 4 hours and impacts 2% of the subscribers or less
- It lasts for up to 2 hours and impacts 3% of the subscribers or less
- It lasts for less than 1 hour has an impact on 15% of the subscribers or less

An incident is defined as Level 1 if any of the following conditions is true: ■

- It lasts for more than an hour but less than or equal to 2 hours and impacts more than 3% but less than or equal to 7% of the subscribers
- It lasts for more than 2 hours but less than or equal to 4 hours and impacts more than 2% but less than or equal to 4% of the subscribers
- It lasts for more than 4 hours but less than or equal to 5 hours and impacts more than 1% but less than or equal to 3% of the subscribers

An incident is defined as Level 2 if any of the following conditions is true ■

- It lasts for more than an hour but less than or equal to 2 hours and impacts more than 7% but less than or equal 15% of the subscribers

- It lasts for more than 2 hours but less than or equal to 4 hours and impacts more than 4% but less than or equal to 10% of the subscribers
- It lasts for more than 4 hours but less than or equal to 5 hours and impacts more than 3% but less than or equal to 6% of the subscribers
- It lasts for more than 5 hours but less than or equal to 6 hours and impacts more than 1% but less than or equal to 6% of the subscribers
- It lasts for more than 6 hours but less than or equal to 8 hours and impacts more than 1% but less than or equal to 2% of the subscribers

An incident is defined as Level 3 if any of the following conditions is true



- It impacts more than 15% of the subscribers irrespective of the duration of the incident
- It lasts for more than 2 hours and impacts more than 10% of the subscribers
- It lasts for more than 4 hours and impacts more than 6% of the subscribers
- It lasts for more than 6 hours and impacts more than 2% of the subscribers
- It lasts for more than 8 hours and impacts more than 1% of the subscribers

3.2 Loss of Integrity, Authentication and Privacy

Security incidents that lead to the loss of either integrity, authenticity or confidentiality may well be separate incidents in their own right. The proposed assessment for incident severity shall be the same for all types of incidents. An incident shall be classified as severe (Level 3) when the number of impacted subscribers reaches a threshold of 1% of the subscriber base. The duration of the incident is not taken into account since the harm done to the subscriber is not a function of time.

The Authority notes that since these types of losses were introduced for the first time in the EECC, no prior information is available concerning their prevalence. Therefore, while the threshold proposed is in line with the guidelines published by ENISA, the Authority will be reviewing this threshold when sufficient data is collected.

3.3 Loss of Services which are Required at Law

The General Authorisation granted to providers of electronic communication networks and, or services may mandate the provision of some specific services to be included with those offered by the provider. For example, providers of voice services are required to provide connectivity to emergency services. Similarly, the interconnectivity between networks and the provision of legal intercept interfaces is also mandated at law. Some security incidents may result in having the provision of these services suspended. Therefore, for the duration of the incident, the network is not providing the full set of services required of it while also being in a state of legal irregularity, albeit temporarily.

In these circumstances, incidents that lead to the loss of service such that obligations of the General Authorisation and when other legal obligations are not met, the incident is immediately considered a Level 3 (Red) on the incident severity scale. While the duration of the incident is not taken into account to establish the severity of the incident, providers will still be required to include the duration of the incident as part of their report

Consultation Questions

IR 3	What are your views on the proposed process to analyse and classify subscriber-oriented Incidents?
IR 4	What are your views on the thresholds applicable to subscriber-oriented incidents as indicated in Figure 5
IR 5	What are your views on the proposed estimation method relevant to mobile broadband subscribers?

4 Assessment of Scale of a Network-Oriented Incident

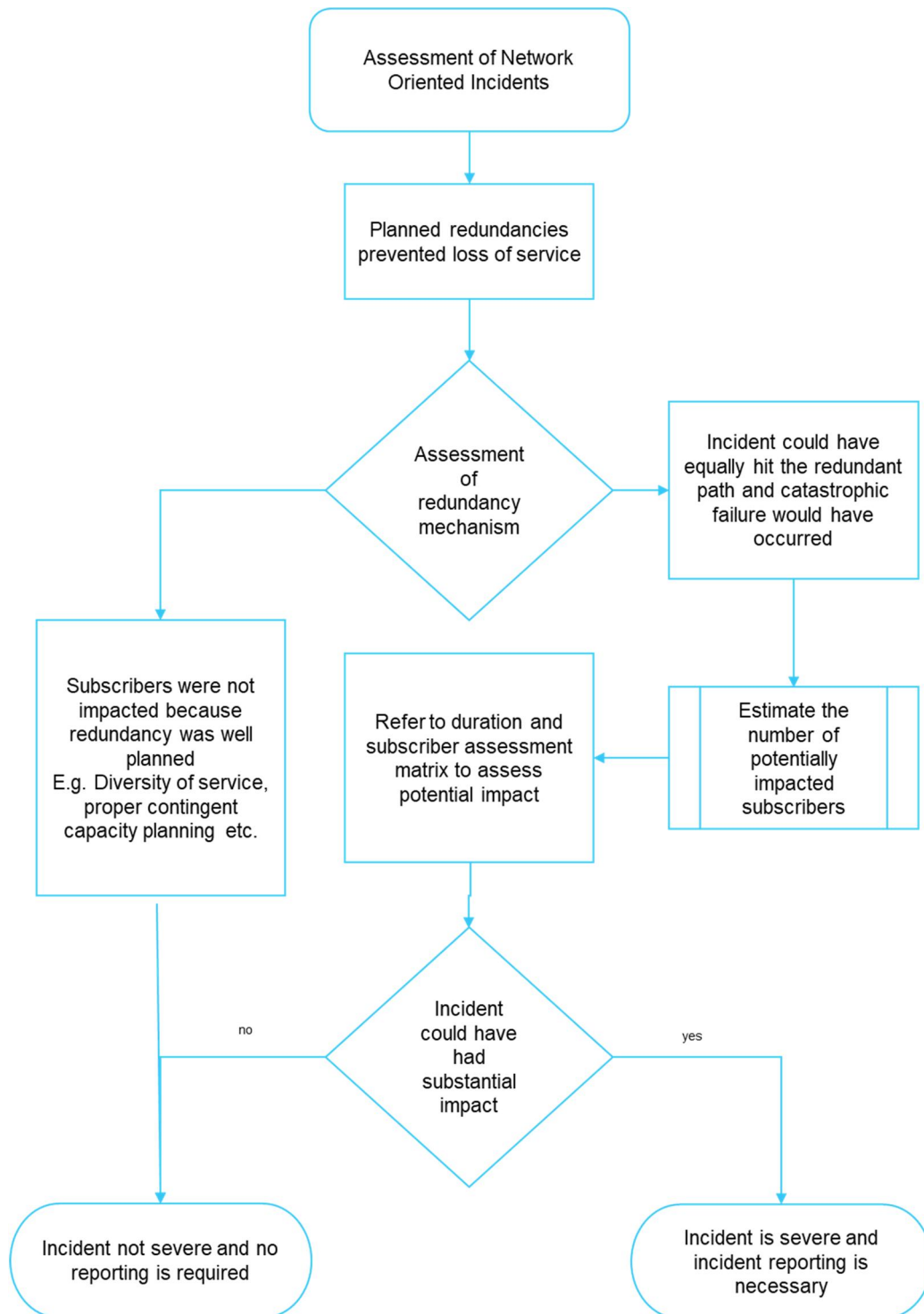


Figure 6 Process for assessing Network Oriented Incidents

The nature of Network Oriented Incidents does not present tangible disruptive issues to subscribers. Therefore, using the number of impacted subscribers would not be the right metric to measure the incident. Nevertheless, interest in collecting data about Network Oriented Incidents remains to understand the type of mitigation measures that are deployed and their effectiveness, or lack thereof to respond to certain incidents. The proposed analysis aims to obtain information on the mitigation measure's performance in repeat scenarios.

Figure 6 above shows a high-level process of the analysis where the assessment is split into two phases. In the first part of the assessment, the elements that have prevented the incident from producing catastrophic results are identified. The second step is to assess whether their effectiveness was the result of the correct planning and execution of the mitigation or whether it just happened to be effective.

For illustration purposes, we present a scenario where network losses were prevented due to network redundancies through the deployment of diverse network routes. The network redundancy proved adequate because the incident impacted one of the network paths, but it was impossible to reach the redundant path. Alternatively, the incident could have reached both paths simultaneously, but *it just happened* that one of the network paths was spared.

It is clear that in the first example, the redundancy was well planned to cater for the incident scenario, while in the second, not so much. Under these circumstances, the level of severity in the first example is labelled at Level 0. In the second scenario, it is evident that the redundancy offered protection, but it wasn't necessarily planned to cater for the scenario presented in the incident, and therefore there is no predictability in repeat circumstances. In this case, the second phase of the assessment is necessary. In this part of the assessment, the provider is required to run a scenario where the surviving redundancy would have also failed and estimates the number of potentially impacted subscribers. The duration of this incident and the number of potentially impacted subscribers are used to estimate the severity of the incident.

Figure 7 below presents the relationship between the number of potentially impacted subscribers, time, and the scale of the incident, which is applicable in Network Oriented Incidents.

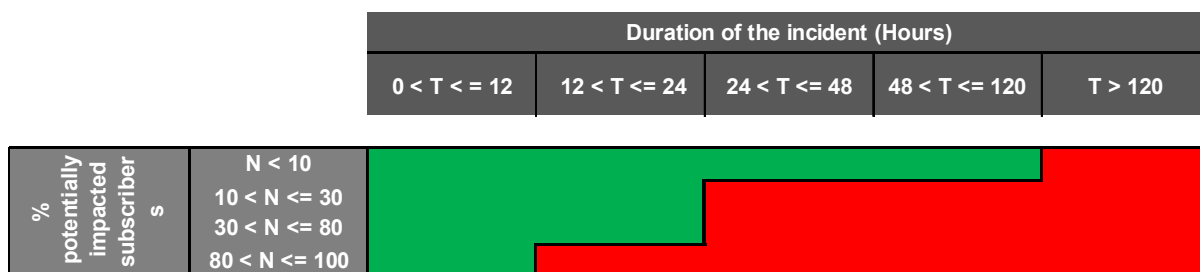




Figure 7 Incident reporting thresholds for Network Oriented Incidents

A Network Oriented Incident is defined as Level 0 if: 

- It lasts for up to 12 hours
- It lasts for up to 24 hours, and the potential impact on subscribers is less than or equal to 80%
- It lasts for up to 120 hours, and the potential impact on subscribers is less than or equal to 10%

A Network Oriented Incident is defined as Level 3 if 

- It lasts for more than 12 hours and has a potential impact on more than 80% of subscribers
- It lasts for more than 24 hours and has a potential impact on more than 10% of subscribers
- It lasts for more than 120 hours

Consultation Questions	
IR 6	What are your views on the proposed process to analyse and classify Network-oriented Incidents?
IR 7	What are your views on the thresholds applicable to network-oriented incidents as indicated in Figure 7

5 Incident Reporting and Notification

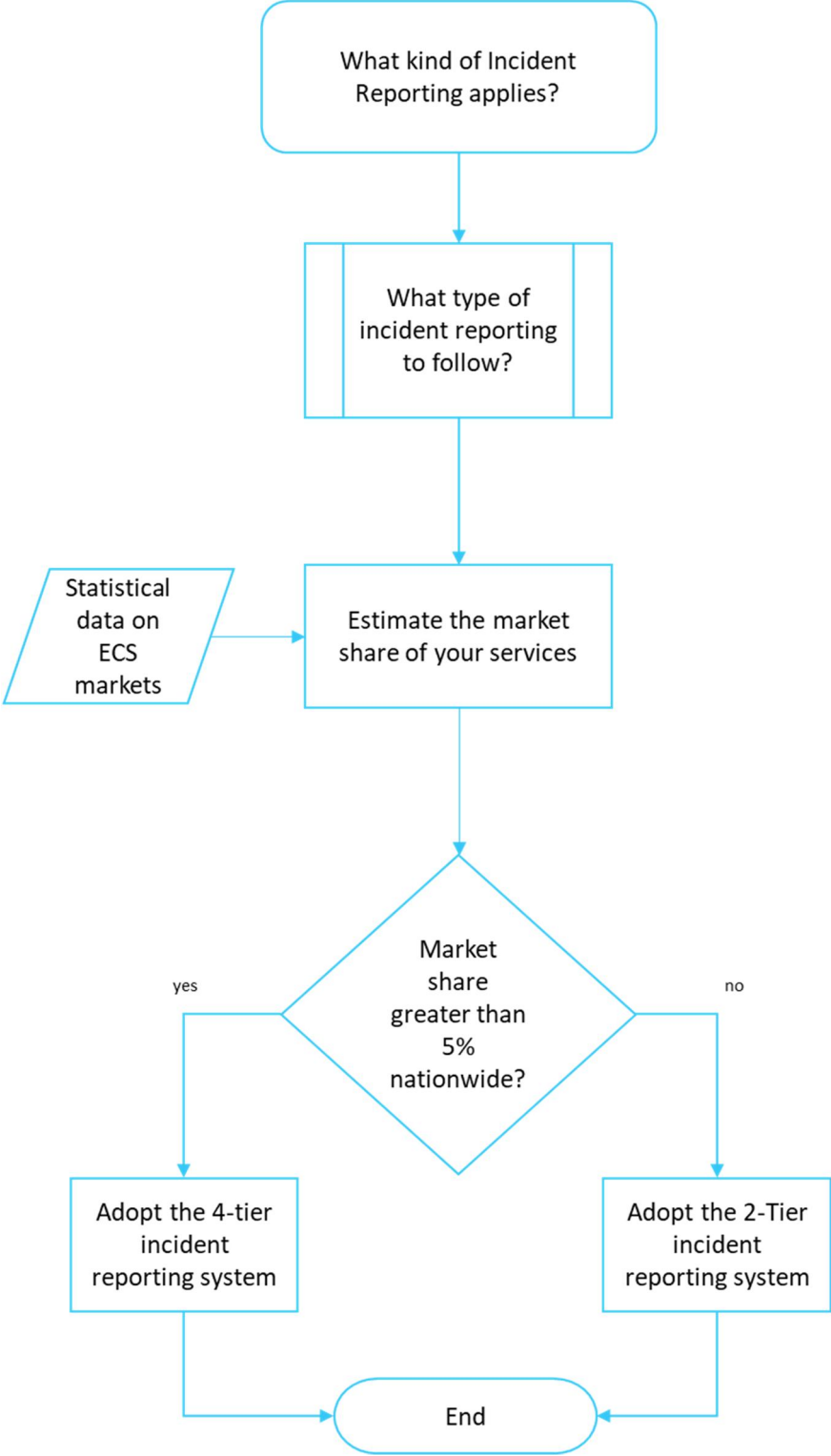


Figure 8 Process suitable to identify the applicable incident reporting

Incident reporting and notification are two processes that require the provider to inform the Authority of a security incident at the point of onset, the point of resolution and the point of understanding and resolution the incident. The severity of the incident will guide on what kind of notification and reporting is appropriate.

Incident notification aims at providing the Authority with basic knowledge of the incident allowing the Authority to issue any relevant instructions to the providers or advise interested stakeholders of the incident and advise on any possible mitigation necessary to limit the impact of the incident. Therefore providers who suffer incidents of a certain magnitude shall be required to notify the Authority of such incidents within a short time frame – even if the details of the cause and extent of the same incident are not yet known.

Incident reporting happens at a later stage after the incident is either resolved or is under control, and similarly, the network and service are either restored or stabilised. The provider, having analysed the details of the circumstances related to the incident is required to provide detailed account of the events leading up to the incident, those actions taken to resolve it and any mitigation measures to prevent repetition of the incident.


5.1 Notification of Incidents to the Authority

ECSN providers are obliged, depending on the severity of the incident, to establish contact with the Authority to notify it at the earliest possible when the incident is discovered and when it is resolved. The notification procedure is intended to (i) provide the Authority with basic information about the occurrence of an incident, and (ii) update the Authority in real-time so as to enable the Authority to deal with any respective queries appropriately and issue any related public announcements, particularly those relevant to the general .

The Authority also proposes that the proper procedure for incident notification is to send an email to a designated address providing

- a) Contact point within the provider with whom the Authority may liaise for obtaining information.
- b) Estimated downtime – if available

The Authority is proposing the following timelines for notification depending on the severity of the incident as follows:-

Incident Level	Notification Required	Notification at start of the incident	Notification at or after the resolution of the incident
Level 0 	No	n/a	n/a




Level 1		No	n/a	n/a
Level 2		Yes	Not required	Within three working days from the resolution of the incident
Level 3		Yes	Yes – Immediately after the provider discovers the incident and is aware of its scale	Yes – Within one hour from the resolution of the incident

Table 2 Incident notification requirements based on the severity of the incident

Consultation Questions

IR 8 What are your views on the requirements of incident notification?

5.2 Reporting and Statistics

Following a severe incident, the impacted stakeholders are required to assess the circumstances, action taken and/or lack thereof, leading to the incident and documenting these findings in the form of a report. The template used to structure the report is presented in a later section of this consultation paper.

The Authority is proposing that an incident report be submitted by the provider suffering the incident according to the scale of the incident as listed in Table 3.

Level 0

- Incidents classified as Level 0 are not required to be analysed and documented




<p>Level 1</p>	
<ul style="list-style-type: none"> • Incidents classified as Level 1 are not required to be accompanied by a detailed incident report. • Nevertheless, providers shall be required to analyse the root cause of these incidents. • Once every quarter, the provider shall report the number of incidents experienced under the heading of each root cause category. 	
<p>Level 2</p>	
<ul style="list-style-type: none"> • Incidents classified as level 2 are required to be followed by a detailed incident report in line with the template provided in this paper. • Providers are expected to provide a copy of the incident report to the Authority within six weeks from the resolution of the incident. 	
<p>Level 3</p>	
<ul style="list-style-type: none"> • Incidents classified as level 2 are required to be followed by a detailed incident report in line with the template provided in this paper. • Providers are expected to provide a copy of the incident report to the Authority within three weeks from the resolution of the incident. • The Authority may request follow up actions and/or reports as necessary 	

Table 3 Incident reporting requirements based on incident severity

All incident reports are to be submitted to the Authority through the designated electronic channels as identified by the Authority¹.

The Authority will take serious note of any failure to submit incident reporting on time. It shall take the appropriate regulatory measures in accordance with its powers under Cap 418 which may include the imposition of sanctions vis-à-vis the non-compliant provider.

¹ The current incident notification channel designated by the Authority in the electronic mailbox incidentreporting@mca.org.mt

Consultation Questions

IR 9	What are your views on the proposed requirements of incident reporting?
-------------	---

5.3 Simplification of Incident Reporting

In view of the incident reporting framework being applicable to all electronic communication networks and service providers, a simplified incident classification system is proposed intended to be used by the smaller providers. The simplified incident classification system will make use of two categories where Levels 0, 1 and 2 are merged together into Level 0 while Level 3 classification will remain common between the two schemes. This simplification will reduce the administrative burden when the incident only impacts a small percentage of the national subscriber base.

Table 4 below depicts the correlation between the compound 4 level and simplified 2-level incident classification system

Classification Category – 4-level system	Classification Category – 2-level system
Level 0 – Insignificant ●	Level 0 – Insignificant/ Low/ Medium Impact ●
Level 1 – Low Impact ●	
Level 2 – Medium Impact ●	
Level 3 – Severe Impact ●	Level 3 – Severe Impact ●

Table 4 Mapping between the 4-level and 2-level systems

All service and network providers shall, by default, be required to use the 4-level incident classification system unless the number of subscribers of a specific service at the beginning of a calendar year is equivalent to or less than the 5% of the national subscribers, in which case the 2-level incident classification system may be used.

In the case of a provider offering multiple services, the 2-level incident classification system may only be used for those services which reach the criteria stated in (a) above.

Consultation Questions

IR 10

What are your views on the proposed simplification of incident reporting?

6 Data collection requirements

Information pertaining to the number of subscribers for the respective fixed services, the number of active mobile cells are necessary for calculating the severity of an incident is required to support the computation of metrics related to the subscriber base. The Authority remarks that such information is already in its possession through existing data collection processes.

The Authority proposes that in an effort to avoid time-consuming and repetitive data collection processes by the providers, the Authority shall make reference to existing data in its possession, provided that:

- (i) the ECS and ECN providers consent that the Authority makes use of existing data for the scope of incident reporting;
- (ii) the format and meaning of this data is compatible with the requirement of incident reporting; and
- (iii) the Authority shall reserve the right to request the latest available data with regard to incident reporting,

In the eventuality that any of the above criteria is not met, then the Authority would make fresh data requests as necessary.

7 Applicable timeframes for the implementation and review of the proposed initiative

The Authority is cognisant that the proposed framework involves more stringent reporting thresholds and new concepts especially those related to the network-oriented incidents. Taking this into account, the MCA is proposing that in the case of existing providers of electronic communications networks and services, these proposals shall come into force after six (6) months from the publication of the final decision subsequent to this consultation.

In the case of new entrants to the electronic communications networks and services into the market, the proposals shall be in force immediately when they start operating their networks. By virtue of proportionality, new entrants typically have initially smaller networks and therefore are likely to initially adopt the simplified version of incident reporting thus allowing them more time before being subject to the full extent of the framework.

At the end of the transition period, the current guidelines on incident reporting shall be considered repealed.

The Authority has endeavoured to ensure that the reporting efforts arising from the newly proposed thresholds are reasonable in view of the providers' operational capacities. The operation of these thresholds will also provide information about the quality of the incidents reported and their quantity. Therefore, the Authority notes that the proposed thresholds may need to be revisited until the volume of incidents reported is manageable.

Consultation Questions

IR 11	What are your views on the implementation timelines?
--------------	--

8 Incident Reporting template

This section includes the incident reporting templates to be used by providers to cover all the incidents. Different templates are applicable according to the severity of the incident

8.1 Incident Reporting Template (Level 1)

This template is to be submitted every quarter and is suitable to collect aggregate information about those incidents classified as Level 1

Incident Reporting Template for Level 1 incidents			
1	Date of Report		
2	Reporting Operator		
3	Contact Person		
4	Reference Number		
5	Reporting Period	1 st January - 31 st March	<input type="checkbox"/>
		1 st April - 30 th June	<input type="checkbox"/>
		1 st July - 30 th September	<input type="checkbox"/>
		1 st October - 31 st December	<input type="checkbox"/>
6	Number of Incidents for each root cause	System Failure	
		Human Errors	
		Malicious Actions	
		Natural Phenomena	
		Third-party failures	

Notes on the fields	
1	The provider is to write down the date of the report
2	The provider is to include
3	Details of a contact person with whom the Authority may follow up on the report if necessary
4	The provider is to generate a unique reference number for each report produced. The format OPR-xxxx-yy is suggested
5	The provider is to indicate the reporting period which covers the report
6	<p>The provider shall report the number of incidents incurred during the reporting period grouped by the root cause.</p> <p>The tick-mark "Third-party failures" should be used in conjunction with one other root cause indicator.</p>

This template is to be submitted for each incident and is suitable to report those incidents that are more severe than Level 2.

8.2 Incident Reporting Template (Level 2 or over)

General Information

1	Date of Report				
	Reporting Operator				
2	Reference Number				
3	Start of incident	Date		Time	
	Resolution of incident	Date		Time	

Notification of incident to the MCA (Start)	Date		Time	
Notification of incident to the MCA (End)	Date		Time	

Cause Analysis

4	Root Cause	System Failures	<input type="checkbox"/>
		Human errors	<input type="checkbox"/>
		Malicious actions	<input type="checkbox"/>
		Natural Phenomena	<input type="checkbox"/>
		Third-party failures	<input type="checkbox"/>
5	Initial Cause	Arson	<input type="checkbox"/>
		Cable cut	<input type="checkbox"/>
		Cable theft	<input type="checkbox"/>
		Cooling outage	<input type="checkbox"/>
		Denial of Service attack	<input type="checkbox"/>
		Earth Quake	<input type="checkbox"/>
		Electromagnetic interference	<input type="checkbox"/>
		Faulty hardware change/update	<input type="checkbox"/>
		Faulty software change/update	<input type="checkbox"/>
		Fire	<input type="checkbox"/>

		Flood	<input type="checkbox"/>
		Fuel exhaustion	<input type="checkbox"/>
		Hardware failure	<input type="checkbox"/>
		Hardware theft	<input type="checkbox"/>
		Heavy snow/ice	<input type="checkbox"/>
		Heavy wind	<input type="checkbox"/>
		Malware and viruses	<input type="checkbox"/>
		Network traffic hijack	<input type="checkbox"/>
		No Information	<input type="checkbox"/>
		None/Not applicable	<input type="checkbox"/>
		Overload	<input type="checkbox"/>
		Policy/procedure Flaw	<input type="checkbox"/>
		Power cut	<input type="checkbox"/>
		Power surges	<input type="checkbox"/>
		Security Shutdown	<input type="checkbox"/>
		Software bug	<input type="checkbox"/>
		Wildfire	<input type="checkbox"/>
		Other	<input type="checkbox"/>
6	Subsequent Cause		<input type="checkbox"/>
		Arson	<input type="checkbox"/>
		Cable cut	<input type="checkbox"/>

			<input type="checkbox"/>
		Cable theft	<input type="checkbox"/>
		Cooling outage	<input type="checkbox"/>
		Denial of Service attack	<input type="checkbox"/>
		Earth Quake	<input type="checkbox"/>
		Electromagnetic interference	<input type="checkbox"/>
		Faulty hardware change/update	<input type="checkbox"/>
		Faulty software change/update	<input type="checkbox"/>
		Fire	<input type="checkbox"/>
		Flood	<input type="checkbox"/>
		Fuel exhaustion	<input type="checkbox"/>
		Hardware failure	<input type="checkbox"/>
		Hardware theft	<input type="checkbox"/>
		Heavy snow/ice	<input type="checkbox"/>
		Heavy wind	<input type="checkbox"/>
		Malware and viruses	<input type="checkbox"/>
		Network traffic hijack	<input type="checkbox"/>
		No Information	<input type="checkbox"/>
		None/Not applicable	<input type="checkbox"/>
		Overload	<input type="checkbox"/>
		Policy/procedure Flaw	<input type="checkbox"/>

		<input type="checkbox"/> Power cut <input type="checkbox"/> Power surges <input type="checkbox"/> Security Shutdown <input type="checkbox"/> Software bug <input type="checkbox"/> Wildfire <input type="checkbox"/> Other (Specify with details)
7	Assets affected by initial cause	<input type="checkbox"/> Addressing servers <input type="checkbox"/> Backup power supplies <input type="checkbox"/> Billing and mediation systems <input type="checkbox"/> Building and physical security systems <input type="checkbox"/> Cooling systems <input type="checkbox"/> Intelligent network devices <input type="checkbox"/> Interconnection points <input type="checkbox"/> Logical security systems <input type="checkbox"/> Mobile base stations and controllers <input type="checkbox"/> Mobile messaging centre <input type="checkbox"/> Mobile switches <input type="checkbox"/> Mobile user and location registers <input type="checkbox"/> No information

		Operational support systems	<input type="checkbox"/>
		Overhead cables	<input type="checkbox"/>
		PSTN switches	<input type="checkbox"/>
		Power supplies	<input type="checkbox"/>
		Street cabinets	<input type="checkbox"/>
		Submarine cables	<input type="checkbox"/>
		Subscriber equipment	<input type="checkbox"/>
		Switches and routers	<input type="checkbox"/>
		Transmission nodes	<input type="checkbox"/>
		Underground cables	<input type="checkbox"/>
		Other (Specify with details)	<input type="checkbox"/>
8	All assets affected during the incident except for those affected by the initial cause	Addressing servers	<input type="checkbox"/>
		Backup power supplies	<input type="checkbox"/>
		Billing and mediation systems	<input type="checkbox"/>
		Building and physical security systems	<input type="checkbox"/>
		Cooling systems	<input type="checkbox"/>
		Intelligent network devices	<input type="checkbox"/>
		Interconnection points	<input type="checkbox"/>
		Logical security systems	<input type="checkbox"/>

		Mobile base stations and controllers	<input type="checkbox"/>
		Mobile messaging centre	<input type="checkbox"/>
		Mobile switches	<input type="checkbox"/>
		Mobile user and location registers	<input type="checkbox"/>
		No information	<input type="checkbox"/>
		Operational support systems	<input type="checkbox"/>
		Overhead cables	<input type="checkbox"/>
		PSTN switches	<input type="checkbox"/>
		Power supplies	<input type="checkbox"/>
		Street cabinets	<input type="checkbox"/>
		Submarine cables	<input type="checkbox"/>
		Subscriber equipment	<input type="checkbox"/>
		Switches and routers	<input type="checkbox"/>
		Transmission nodes	<input type="checkbox"/>
		Underground cables	<input type="checkbox"/>
		Other (Specify with details)	<input type="checkbox"/>

Services Impacted			
9	Fixed Telephony Service	Duration (hours)	

		Number of users	
	Fixed Broadband Internet	Duration (hours)	
		Number of Users	
10	Mobile Telephony	Duration (hours)	
		Number of 2G Cells	
		Number of 3G and 3.5G Cells	
		Number of 4G and 4.5G Cells (LTE)	
		Number of Cells using any other technology (specify technology)	
		Estimated number of subscribers	
		Mobile Internet	Duration (hours)
		Number of 2G Cells	
		Number of 3G and 3.5G Cells	
		Number of 4G and 4.5G Cells (LTE)	
		Number of Cells using any other technology (specify technology)	
		Estimated number of subscribers	
	11	TV Service	Duration (hours)
Number of users			

	Other Service (Please Specify)	Number of users	
		Duration (hours)	

Networks Impacted				
12	Networks	Cable Aerial		
		Cable Terrestrial (underground)		
		Electricity cable Systems		
		Submarine Cable	% capacity lost	
		Satellite		
		Radio (Terrestrial)		
		Fibre Optic cables		
13	Impact on emergency calls	Yes		
		No		
14	Impact on interconnections	Yes		
		No		

Actions

15	Incident Description	
----	----------------------	--

	Describe in detail the dynamics of the incident	
16	Incident response and recovery actions A description of the actions taken after the discovery of the incident	
17	Post-incident actions A description of those actions taken by the provider to reduce the likelihood of the incident occurring again or reduce the impact of the incident	
18	Lessons Learnt A description of any lessons learnt and any measures or procedures to be implemented in the long –term.	
19	Further remarks (if any):	

Notes about the fields

1	The provider is to insert the date when the report was compiled
2	The operator is to generate a report number. Sequential numbers are advised in the format OPR/XXXX-YY, where OPR denote an abbreviation of the operator, XXXX is a sequential number of the report, and YY denotes the year of the report
3	The date and time when the incident started and when this was successfully resolved, together with the relevant notification, are to be listed. In case that notification is not necessary, the use of N/A is acceptable.

4 The root cause of an incident is the initial cause of an incident; in other words, the event or factor that triggered the incident. In the field "root cause category", operators should indicate the root cause of the incident. In its guidance document, ENISA identifies five categories as follows

Human Errors

This category refers to those incidents caused by human errors during the operation of equipment or facilities, the use of tools and the execution of procedures.

System Failures

Operators should use this field for incidents caused by failures of a system, for example, hardware failures, software failures or flaws in manuals, procedures or policies.

Natural Phenomena

This field should be used for incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife and so on.

Malicious Actions

Operators should tick this field for incidents caused by a deliberate act by someone or some organisation.

Third-Party Failure

This category should be used for incidents where the root cause is outside the provider's direct control, for example, when the root cause occurred to a contractor used for outsourcing or at an organisation somewhere along the supply chain. This category may be used standalone when the root cause of the incident is unknown. In all other cases, this category should be used in conjunction with one of the other root cause categories.

9 Consultation Questions

IR 1	What are your views on the proposal to classify incidents as Subscriber Oriented Incidents and Network Oriented Incidents?
IR 2	From your experience, if any, how feasible is it to adopt the proposed incident classification system?
IR 3	What are your views on the proposed process to analyse and classify subscriber-oriented Incidents?
IR 4	What are your views on the thresholds applicable to subscriber-oriented incidents as indicated in Figure 5
IR 5	What are your views on the proposed estimation method relevant to mobile broadband subscribers?
IR 6	What are your views on the proposed process to analyse and classify Network-oriented Incidents?
IR 7	What are your views on the thresholds applicable to network-oriented incidents as indicated in Figure 7
IR 8	What are your views on the requirements of incident notification?
IR 9	What are your views on the proposed requirements of incident reporting?
IR 10	What are your views on the simplification of incident reporting?
IR 11	What are your views on the implementation timelines?

10 Invitation to Comments

Following its obligations under Article 4A of the Malta Communications Authority Act [Cap. 418 of the Laws of Malta], the Authority welcomes written comments and representations from interested parties and stakeholders during the national consultation period, which shall run from the 6th January 2023 till the 3rd March 2023.

The Authority appreciates that respondents may provide confidential information in their feedback to this Consultation document. This information is to be included in a separate annexe and should be clearly marked as **confidential**. Respondents are also requested to state the reasons why the information should be treated as confidential.

For the sake of transparency, the Authority may publish a list of all respondents to this Consultation on its website, within three days following the deadline for responses. The Authority will take the necessary steps to protect the confidentiality of all such material as soon as it is received, in accordance with the Authority's confidentiality guidelines and procedures².

Respondents are, however, encouraged to avoid confidential markings wherever possible.

All responses should be submitted electronically to the Authority on **consultations@mca.org.mt** and addressed to the Chief Executive Officer.

Extensions to the consultation deadline will only be considered in exceptional circumstances and where the Authority deems fit. The MCA reserves the right to grant or refuse any such request at its discretion. Requests for extensions must be made in writing within the first ten (10) working days of the consultation period.

² http://www.mca.org.mt/sites/default/files/articles/confidentialityguidelinesFINAL_0.pdf



MALTA COMMUNICATIONS AUTHORITY

-  (+356) 2133 6840
-  info@mca.org.mt
-  www.mca.org.mt
-  Valletta Waterfront, Pinto Wharf,
Floriana FRN1913, Malta