TS 00075.1:1.0

Standard

Cyber Security Incident Management

Part 1: Overview and Principles

Issue date: 22 July 2024

Effective date: 22 July 2024

Disclaimer

This document has been prepared by Transport for NSW (TfNSW) specifically for its own use and is also available for use by NSW public transport agencies for transport assets.

Any third parties considering use of this document should obtain their own independent professional advice about the appropriateness of using this document and the accuracy of its contents. TfNSW disclaims all responsibility and liability arising whether directly or indirectly out of or in connection with the contents or use of this document.

TfNSW makes no warranty or representation in relation to the accuracy, currency or adequacy of this document or that the document is fit for purpose.

The inclusion of any third party material in this document, does not represent an endorsement by TfNSW of any third party product or service.

For queries regarding this document, please email Transport for NSW Asset Management Branch at standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

Document information

Owner:	Director Telecom Engineering Asset Management Safety, Environment and Regulation
Mode:	Multimodal
Discipline:	Security

Document history

Revision	Effective date	Summary of changes
1.0	22/07/2024	First issue

Preface

This document is a first issue.

This document sets requirements to ensure that arrangements for centralised management and reporting are clear and consistent and that cyber security incident information is protected in accordance with regulatory obligations.

This document is the first in a series that outlines a structured approach for the management of cyber security incidents. This document provides an overview of the series and sets out common principles and models that are further developed in the other parts.

The series includes the following documents:

- TS 00075.1 *Cyber Security Incident Management – Part 1: Overview and Principles*
- TS 00075.2 *Cyber Security Incident Management – Part 2: Compliance and Reporting*

The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards.

Table of contents

1 Scope

This document sets requirements for a structured approach for the management of cyber security incidents. This document is the first in a series related to cyber security incident management.

This document does not cover coordination arrangements for crisis or emergency management.

This document provides an overview of the series and sets out common principles and models that are further developed in the other parts:

- high level roles and relationships
- concepts and principles
- incident management process and phases.

This standard is based on ISO/IEC 27035 (all parts).

2 Application

This document applies to new and altered assets and may require alterations to existing asset-related processes.

This document applies to asset custodians, asset stewards, delivery partners and service providers who are accountable or responsible for technology systems.

3 Referenced documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

International standards

ISO/IEC 27035 (all parts) *Information technology – Information security incident management*

ISO/IEC 27035-1 *Information technology – Information security incident management – Part 1: Principles and process*

ISO/IEC 27035-2 *Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*

Other referenced documents

Australian Signals Directorate, *Cyber Incident Management Arrangements for Australian Governments*

Premier's Department, *NSW Cyber Security Incident Emergency Sub Plan – A Sub Plan of the State Emergency Management Plan*

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document.

asset steward the party given the responsibility by a custodian to oversee part of the life cycle process for an asset

IMT incident management team; team consisting of appropriately skilled and trusted members of an organization responsible for leading all information security incident management activities, in coordination with other parties both internal and external, throughout the incident lifecycle (Source: ISO/IEC 27035-1 ed. 2.0 Copyright © 2023 IEC Geneva, Switzerland. www.iec.ch)

information security event occurrence indicating a possible breach of information security or failure of controls (Source: ISO/IEC 27035-1 ed. 2.0 Copyright © 2023 IEC Geneva, Switzerland. www.iec.ch)

information security incident related and identified information security events that can harm an organization's assets or compromise its operations (Source: ISO/IEC 27035-1 ed. 2.0 Copyright © 2023 IEC Geneva, Switzerland. www.iec.ch)

IRT incident response team; team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way (Source: ISO/IEC 27035-1 ed. 2.0 Copyright © 2023 IEC Geneva, Switzerland. www.iec.ch)

NCSA National Cyber Security Arrangements

operational technology technology-based assets and services directly involved in the context of TfNSW's operations that can affect or influence safety, security, reliability, operational efficiency, service quality and regulatory compliance

security event occurrence in a system that is relevant to the security of the system (Source: IEC TS 62443-1-1 ed. 1.0 Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

security incident adverse event in a system or network, or the threat of the occurrence of such an event (Source: IEC TS 62443-1-1 ed. 1.0 Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

TfNSW Transport for NSW

5 High level roles and relationships

The asset steward shall define the roles, responsibilities and decision-making authority for each phase of the cyber security incident management process as defined in Section 6.3 and related activities within their organisation.

5.1 Incident management and response teams

An IMT shall be established by the asset steward to manage the end to end of incident management in alignment with recommendations and guidance in ISO/IEC 27035-2.

The asset steward shall address the requirements for establishing and terminating IRTs to respond to specific incidents which have different scopes and expertise depending on the incident.

The types of IRTs, their structures, roles and responsibilities shall align with the recommendations and guidance in ISO/IEC 27035-2.

5.2 Relationships with internal and external organisations

Asset stewards shall establish relationships with other parts of the organisation and with external interested parties such as regulators, public sector agencies, and other affected parties in alignment with ISO/IEC 27035.2.

6 Concepts and principles

6.1 Cyber security events and incidents

Cyber security events are either an information security event or security event.

Cyber security incidents are either an information security incident or security incident.

> Note: The definitions of cyber security events and incidents have been aligned to international standards. Some legislation, regulation, government directives and mandatory policies prescribe alternative definitions which fit with the broad definitions adopted by this standard.

6.2 Classification of cyber security incidents

6.2.1 Alignment of classification schemes

The classification of cyber security incidents differs depending on the frame of reference such as national, state, TfNSW and asset steward.

Figure 1 shows a simplified mapping between national, state and TfNSW classifications defined in the *Cyber Incident Management Arrangements for Australian Governments* and *NSW Cyber Security Incident Emergency Sub Plan – A Sub Plan of the State Emergency Management Plan.* Figure 1 shows that each level of government classifies cyber security incidents using different terminology and thresholds that reflect their respective agency mission and objective. Figure 1 also shows that whilst different terminology and thresholds are defined mappings can be made from one level of government to another.

Note: NCSA levels are defined in *Cyber Incident Management Arrangements for Australian Governments*.

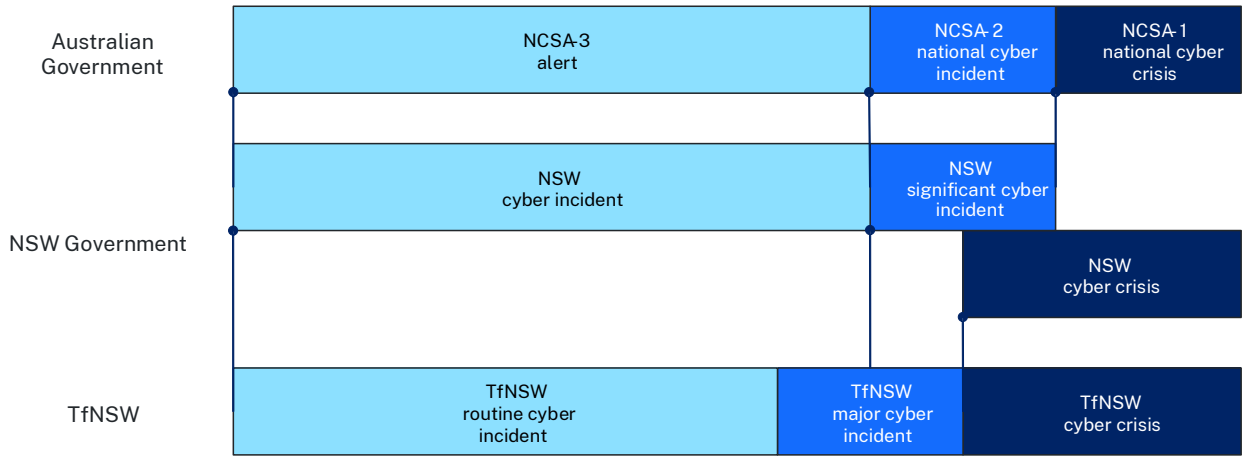

Figure 1 – Classification of cyber security incidents at national, state and TfNSW levels

TfNSW and asset stewards classify cyber security incidents using different terminology and thresholds that reflect their respective agency or organisational missions and objectives.

Figure 2 shows a simplified example between TfNSW and asset stewards – including a Government operating agency A and operating entity B.

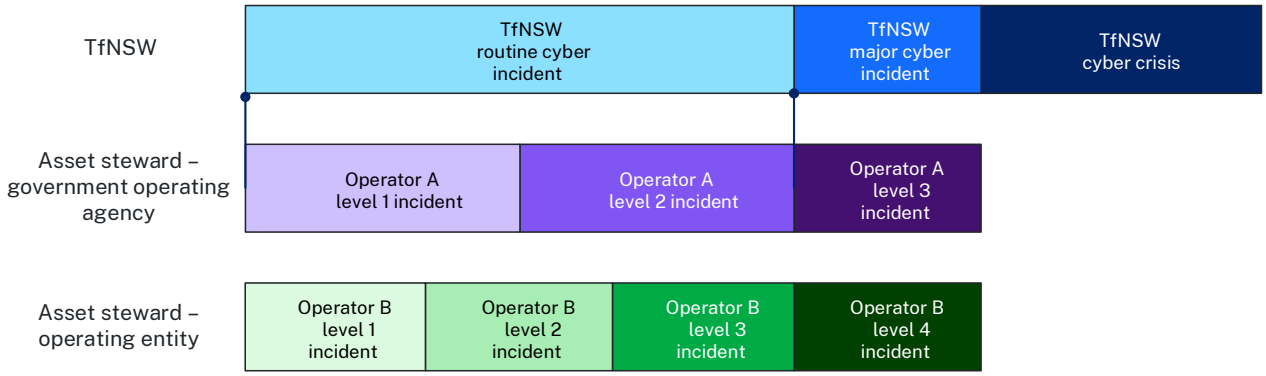

Figure 2 – Classification of cyber security incidents at cluster and operating agency or operating entity levels

Cyber security incidents shall be classified in alignment with the overarching incident management plans and practices of the asset steward.

Asset steward cyber security incident management plans shall include a mapping of the classification criteria to TfNSW incident classification schemes made available from time to time to support notification, reporting, coordination, escalation and de-escalation.

6.2.2 Basis of classification

Cyber security incidents shall be classified based on their immediate impact on information technology and operational technology assets, systems and data shown in Figure 3 as in scope. Figure 3 shows the causal relationship between risk events and the following impacts:

- asset impacts – immediate (less than or equal to 1 day)
- business impacts – immediate (less than or equal to 1 day)
- business impacts – short-term (less than or equal to 14 days)
- business impacts – long-term (greater than 14 days)
- community and society impacts – indirect.

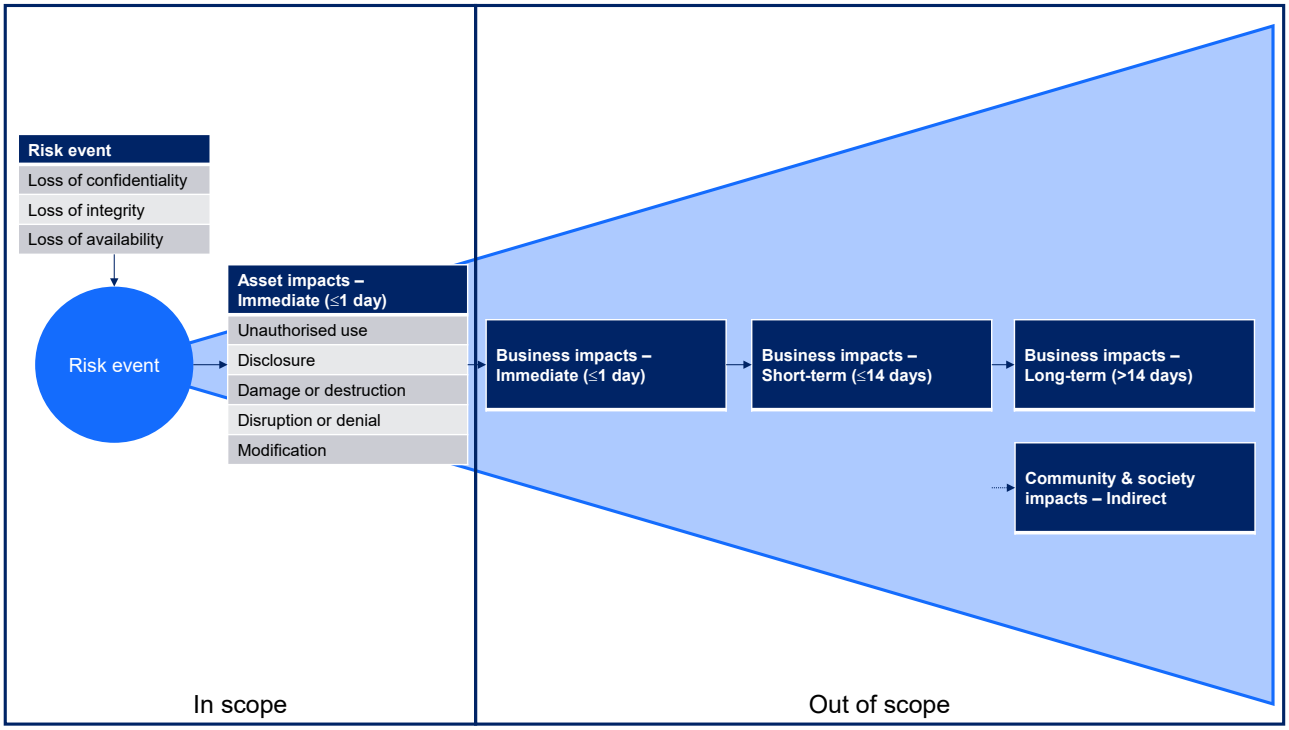

Figure 3 – Causal relationship between risk events and impacts to assets, business, community and society

Note: During the response to an active cyber security incident, it can be challenging to classify cyber security incidents by their potential future impacts to the business, particularly longer-term business impacts. It is more useful to classify cyber security incidents based on the severity of impact on technology assets, systems and data.

A cyber security incident shall be classified based on the severity of impact on technology assets, systems and data as follows:

- unauthorised use
- disclosure

- damage or destruction
- disruption or denial of service
- modification.

A rationale and justification shall support any such classification scheme which demonstrates how the severity of impact to assets aligns with the potential direct impacts to the business over time.

6.3 Incident management process and phases

The cyber security incident management process and phases shall align with ISO/IEC 27035-1.

ISO/IEC 27035-1 describes the cyber security incident management process consisting of five distinct phases as follows:

- plan and prepare
- detection and reporting
- assessment and decision
- responses
- lessons learnt.