Australian Government
Auditing and Assurance Standards Board

Information Sheet

Cyber security in a financial report audit

Issued: November 2026

Introduction

Cyber security incidents may have implications for the preparation and audit of a financial report. This webpage provides support for auditors on:

(i) How an auditor may become aware of a cyber security incident; and

(ii) How an auditor may respond to a cyber security incident.

Background

Entities increasingly rely on technology, digital systems and electronic information in conducting their operations and preparing financial reports. Auditors should evaluate the potential for cyber security incidents to have a **material** effect on amounts or disclosures in the financial report, and systems and controls relevant to the preparation of the financial report.

Examples of cyber security incidents may include:

(a) unauthorised access to systems, networks or data;

(b) ransomware, malware, phishing or other cyber-attacks;

(c) disruption to information technology systems or business operations (e.g. denial of service); and

(d) loss or manipulation of data.

Cyber security matters may affect the auditor's assessment of, and responses to, risks of material misstatement. Whether or not a cyber incident has occurred, auditors would broadly consider cyber security risks as part of their risk assessment and remain alert throughout the conduct of the audit to cyber incidents.

Examples of the factors that may affect the potential impact of an incident and the auditor's risk assessment may include:

(a) The nature of the information held by the entity;

(b) Dependency on IT systems for sales of goods and services;

(c) The potential reputational or financial impact of a loss of confidential client or other data, which could lead to impairment of goodwill or a liability for compensation claims, extortion, etc;

(d) Possible fines or other penalties for a loss of data, breach of contracts or a failure to report; and

(e) Effects on supply chains or from incidents in supply chains.

How an auditor may become aware of a cyber security incident

Depending on the nature and circumstances of the entity, an auditor may become aware of a cyber security incident through a variety of sources, including:

(a) inquiries of management and those charged with governance;

(b) discussions with personnel responsible for information technology and cyber security;

(c) unusual transactions and system disruptions identified during the audit;

(d) through substantive procedures, tests of controls and when control deficiencies are identified;

(e) reports provided by internal audit, risk management or compliance functions;

(f) board or committee papers and minutes;

(g) communications from regulators, customers, suppliers, insurers and legal advisors;

(h) media reports and other publicly available information.

Cyber security risks may be significant where, for example, an entity has a complex IT environment, is heavily dependent on web-based transactions, allows remote access to sensitive information, is dependent on IT services for sales transactions, or does not have a strong IT control environment. The auditor may perform audit procedures to identify, assess and respond to a risk of material misstatement due to cyber security as part of the auditor's risk assessment and response.

Auditors exercise professional judgement and apply professional scepticism when planning and performing an audit. This includes being alert to circumstances that may indicate that the financial report could be materially misstated and evaluating the reliability and sufficiency of audit evidence obtained, particularly where a cyber security incident has occurred that may:

(a) Give rise to a liability for compensation for loss of third-party personal information or financial penalties;

(b) Affect the reputation of the entity and the value of purchased goodwill or other assets;

(c) Affect revenue as a result of a denial of service attack; or

(d) Affect the integrity, completeness or availability of information used in the preparation of the financial report.

The auditor may also consider cyber security matters when agreeing the terms of the engagement and when obtaining written representations from management and, where appropriate, those charged with governance regarding known cyber security incidents that may affect the financial report.

How an auditor may respond to a cyber security incident

Where the auditor becomes aware of a cyber security incident, the nature and extent of the auditor's response will depend on the circumstances of the engagement and the potential effect of the incident on the financial report. The auditor's response may include:

(a) obtaining an understanding of the nature, timing and extent of the incident;

(b) making inquiries of management, those charged with governance and relevant personnel responsible for information technology, information security or cyber security;

(c) evaluating whether the incident may affect risks of material misstatement at the financial report or assertion level;

(d) assessing the impact of the incident on information systems, data integrity and internal controls relevant to financial reporting;

(e) considering whether additional audit procedures are necessary to obtain sufficient appropriate audit evidence;

(f) evaluating whether the incident has affected recognised amounts, estimates, judgements or disclosures in the financial report;

(g) considering the need for the involvement of auditor's experts or information technology specialists;

(h) communicating relevant matters to management and those charged with governance.

Cyber security incidents may also result in actual or potential non-compliance with laws and regulations and may have implications for the auditor's report.

The auditor's response will be influenced by factors such as the nature of the incident, the significance of affected systems or data, the effectiveness of management's response, and the potential impact on the financial report.

The auditor may consider whether an incident could be material to the financial report.

Materiality is not limited to the financial impact of the incident and may also involve qualitative considerations, including the nature of the incident, the sensitivity or volume of information affected, legal or regulatory implications, disruption to operations, reputational impacts, and whether additional disclosures may be necessary to enable users to understand the effect of the incident on the entity.

Cyber security incidents may have direct and indirect implications for the financial report. Depending on the nature and circumstances of the incident, implications may include:

(a) impairment of assets, changes in accounting estimates, provisions, contingent liabilities or going concern considerations;

(b) fraudulent transactions, theft of cash, or misappropriation of assets resulting from unauthorised access to systems;

(c) regulatory penalties, compensation claims, litigation costs or other legal obligations arising from a data breach or cyber-attack;

(d) disruption to operations resulting in lost revenue, increased costs, inventory write-downs or asset impairment;

(e) loss or manipulation of financial data, affecting the completeness, accuracy and reliability of information used to prepare the financial report;

(f) additional disclosures, including disclosures relating to matters that may be quantitatively immaterial but may be qualitatively material due to the nature of the incident; and

(g) subsequent events disclosures.

Cyber Security Disclosures in the Directors' Report

For the directors' report (including the Operating and Financial Review), the auditor complies with ASA 720 *The Auditor's Responsibilities Relation to Other Information* and considers:

(a) whether there is a material inconsistency between the directors' report and the financial report;

(b) whether there is a material inconsistency between the directors' report and the auditor's knowledge obtained during the audit; and

(c) whether a cyber security matter identified during the audit should be disclosed in, or may be relevant to information disclosed in, the directors' report.

Depending on the circumstances, disclosures in the directors' report may include:

(a) a significant cyber security incident, data breach or cyber-attack;

(b) disruption to critical systems or business operations;

(c) material financial, operational, legal or regulatory consequences arising from a cyber security incident;

(d) cyber security risks relevant to the entity's future operations or prospects; and

(e) cyber security governance, oversight or resilience initiatives.

Further information

The Australian Institute of Company Directors (AICD) and Cyber Security Cooperative Research Centre joint publication *Cyber Security Governance Principles* may assist auditors in understanding some cyber security related matters.

Important note

The material in this Information Sheet is intended to assist auditors. This webpage is not an authoritative publication of the AUASB and auditors should use their own professional judgement when conducting an assurance engagement. This webpage does not establish new principles or amend existing AUASB standards. It is not intended to be a substitute for compliance with relevant AUASB standards.

© 2026 Auditing and Assurance Standards Board (AUASB). The text, graphics and layout of this Information Sheet are protected by Australian copyright law and the comparable law of other countries. Reproduction in unaltered form (retaining this notice) is permitted for personal and non-commercial use, acknowledging the AUASB as the source. Otherwise, no part of this webpage may be reproduced, stored or transmitted in any form or by any means without the prior written permission of the AUASB. Requests and enquiries concerning reproduction and rights for commercial purposes should be addressed to the 'Auditing and Assurance Standards Board, PO Box 204, Collins Street West, Melbourne, Victoria 8007' or sent to enquiries@auasb.gov.au.