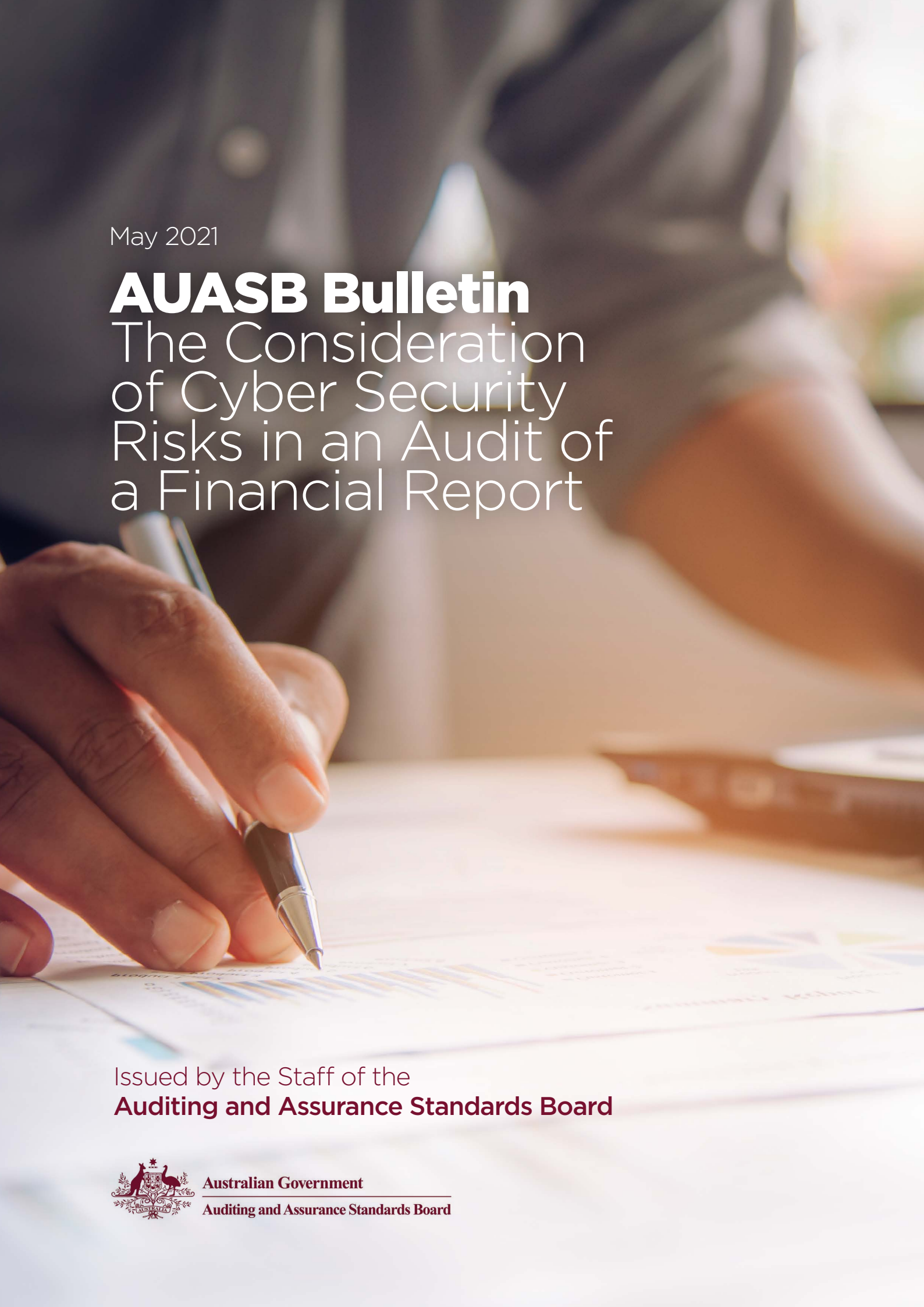

May 2021

AUASB Bulletin

The Consideration of Cyber Security Risks in an Audit of a Financial Report

Issued by the Staff of the
Auditing and Assurance Standards Board

Australian Government
Auditing and Assurance Standards Board

About the AUASB

The Auditing and Assurance Standards Board (AUASB) is an independent, non-corporate Commonwealth entity of the Australian Government, responsible for developing, issuing and maintaining auditing and assurance standards.

Sound public interest-oriented auditing and assurance standards are necessary to reinforce the credibility of the auditing and assurance processes for those who use financial and other information. The AUASB standards are legally enforceable for audits or reviews of financial reports required under the *Corporations Act 2001.* For more information about the AUASB see the AUASB Website.

Disclaimer

This publication has been prepared by the Staff of the Office of the Auditing and Assurance Standards Board.

The views expressed in this publication are those of the author(s) and those views do not necessarily coincide with the views of the Auditing and Assurance Standards Board. Any errors or omissions remain the responsibility of the principal authors.

Enquiries

Auditing and Assurance Standards Board
PO Box 204
Collins Street West,
Victoria, 8007
Australia

Tel: +61 3 8080 7400

Email: enquiries@auasb.gov.au

Website: www.auasb.gov.au

Copyright

Table of contents

Introduction and Purpose

Cyber security in Australia

Cyber security is becoming an increasingly important consideration for governments, entities, regulators and the public. Cyber security refers to the measures used to protect the confidentiality, integrity and availability of systems and information[1]. Recently, there has been significant growth in the number and severity of cyber attacks, including several high-profile Australian entities which have had their business operations significantly impacted.

Over the last few years, there has been considerable integration of technology into how entities operate, including increased reliance on connection to the internet which has also been fast-tracked in response to COVID-19. Whilst there are enormous opportunities for entities in adopting technology, the increased connectivity and reliance on the internet increases the risk of cyber attacks such as unauthorised access to information systems resulting in loss of proprietary and sensitive information; manipulation and destruction of data, systems, and networks; and even the harming of physical assets.

In Australia, the Australian Cyber Security Centre (ACSC) reported that in the 2019/2020 financial year, they responded to 2,266 cyber security incidents and received 59,806 cybercrime reports which worked out to one report every 10 minutes[2]. Globally, cyber security experts project the total net cost of cybercrime to reach USD $10.5 trillion annually by 2025 (up from USD $3 trillion in 2015[3]), with the most prominent forms of attack being e-mail fraud, phishing, ransomware and e-commerce data interception[4].

Consideration of cyber security and cyber resilience is important for all entities and whilst not all entities will have sophisticated online platforms fundamental to their operations, e-mail fraud is still the most common form of cyber attack and is expected to increase exponentially making cyber security a relevant consideration for any entity that utilises e-mail. Examples of e-mail based cyber attacks include bogus invoice schemes, impersonating key personnel in an organisation to request a funds transfer and phishing attacks to gain access to systems and information.

What is the purpose of this publication?

The purpose of this bulletin is to assist auditors to consider the direct and indirect impact of cyber security on the audit of a financial report performed in accordance with Australian Auditing Standards.

Auditors are required to identify and assess the risks of material misstatement of the financial report, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Depending on the facts and circumstances of an entity, cyber security may contribute to the susceptibility to misstatement of certain amounts and disclosures in an entity's financial report.

[1] Australian Cyber Security Centre Glossary https://www.cyber.gov.au/acsc/view-all-content/glossary

[2] ACSC Annual Cyber Threat Report 2019-20

[3] Globenewswire (https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-TheWorld-10-5-Trillion-Annually-By-2025.html)

[4] Interpol ASEAN Cyberthreat Assessment 2021 (https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia)

The responsibility of management and those charged with governance

Management with oversight from Those Charged with Governance (TCWG), are responsible for preparing the financial report in accordance with the applicable financial reporting framework and designing and implementing internal controls necessary to do this. Recognising and managing risk is a crucial part of the role of management and TCWG. The prominence of cybercrime (both in Australia and globally) means that cyber security is a business risk for many entities to consider and manage. The Australian Securities and Investments Commission (ASIC) has published several resources on cyber resilience including good practice guides and key cyber questions for an organisation's board of directors[5].

For business risks like cyber security, there can be direct as well as indirect implications for the financial report. Whilst cyber security is a risk for any entity that uses the internet, not all entities will be significantly impacted by a cyber security event[6].

For entities whose operations could be significantly impacted, it is important for management and TCWG to consider the risks related to cyber security and when a cyber security event may occur, whether is it quantitatively or qualitatively material and the implications for the financial report. In considering the impact of cyber events, management and TCWG may consider AASB Practice Statement 2 *Making Materiality Judgements* which provides entities with guidance on making materiality judgements when preparing general purpose financial statements.

Where a cyber event has occurred, some examples of direct and indirect impacts on the financial report include:

- Recognition of provisions or disclosure of contingent liabilities as a result of a data breach. This may be the result of fines or penalties from a regulator as well as the possibility of legal action from impacted parties where sensitive data has been lost. Recognition or disclosure may be further complicated by the dwell time[7] of a breach which may remain undetected across reporting periods.
- Change in fair value of assets as a result of a cyber event, for example where a particular industry is being targeted there may be a hesitancy to transact with those entities.
- Impairment of assets due to decreased operating cashflows as a result of a cyber attack. For example, where an attack has shut down operations for a significant period of time or where an attack has significantly damaged the entity's brand.
- Overall implications for the entity's ability to continue as going concern from the matters identified above.

[5] https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/

[6] Cyber security event – 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.

[7] Dwell time refers to the length of time a cyber attacker has access to an environment before they are discovered and removed.

The auditor's responsibility

The auditor's overall objective is to obtain reasonable assurance that the financial report is free from material misstatement. This is done through:

- Identifying and assessing risks of material misstatement, whether due to fraud or error, based on an understanding of the entity and its environment (in accordance with ASA 315 *Identifying and Assessing Risks of Material Misstatement through Understanding the Entity and Its Environment (ASA 315)*); and
- Designing and implementing responses to the assessed risks (in accordance with ASA 330 T*he Auditor's Responses to Assessed Risks*).

As outlined above, cyber security is a risk for any entity that uses the internet but whether this risk is likely to result in a risk of material misstatement for the financial report is an entity-by-entity consideration.

The auditor's responsibility in relation to cyber security, like other risks, is to firstly consider the risk of material misstatement to the financial report as part of risk assessment procedures and respond appropriately where a risk of material misstatement is identified. Management and TCWG remain responsible for having a risk assessment process in place to identify risks such as cyber security and to implement and monitor internal controls to respond to those risks.

Cyber security and risk assessment

Whether or not a cyber attack or cyber event has occurred, the auditor as part of their risk assessment procedures should consider the implications of cyber security on the financial report and remain alert throughout the conduct of the audit to cyber events and their potential impact on the initial risk assessment performed.

ASA 315 requires the auditor to obtain an understanding of the entity and its environment, and internal controls relevant to the audit, and through this, identify and assess risks of material misstatement. This includes understanding the entity's use of Information Technology (IT) and identifying risks arising from IT.

General IT controls maintain the integrity and security of information and are relevant when considering cyber security. Depending on the specific circumstances of the entity, the auditor may already consider cyber security as part of their work around general IT controls.

Strong general IT controls provide a good first line of defence for cyber security, however as an organisation's operational and financial systems become more integrated, operational systems may also provide a point of access for attackers which may not be considered as part of general IT controls. Operational systems which do not impact on the financial report are outside the scope of an auditor's responsibility, but it may be worthwhile as part of understanding the organisations use of IT to enquire of management what controls are in place for other systems.

ASA 315 has recently been updated and whilst the new version of the standard is not yet effective[8], a key enhancement in the new version has been to include more on the consideration of risks due to IT. ASA 315 now includes extensive new guidance on understanding IT and identifying relevant risks which auditors will find helpful as part of Appendix 5 *Considerations for Understanding Information Technology* and Appendix 6 *Considerations for Understanding General IT Controls*.

[8] ASA 315 *Identifying and Assessing the Risks of Material Misstatement* is operative for financial reporting periods commencing on or after 15 December 2021. Early adoption of the standard is permitted.

Most commonly, cyber attacks manifest as fraud against the organisation so auditors should also refer to ASA 240 *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report*, which expands on how ASA 315 is applied in relation to fraud and is useful for auditors in considering cyber security.

The diagram below illustrates how cyber security may be considered throughout the risk assessment process. **Table 1** of **Appendix 1** provides some context to how cyber security may impact on the audit and the auditor's responsibility related to risk assessment.

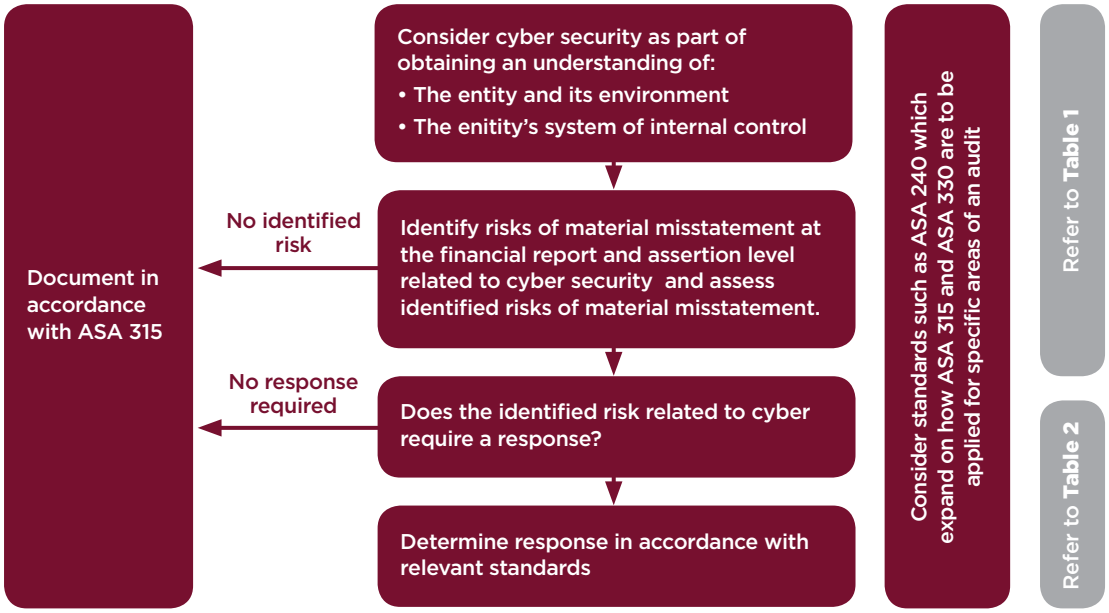

Figure 1 – ASA 315 considerations

Responding to cyber security

For many entities, cyber attacks and cyber events will generally not result in a risk of material misstatement. Where a risk of material misstatement to the financial report has been identified from cyber security as part of risk assessment procedures, the auditor is responsible for designing and implementing responses to those assessed risks.

Depending on the nature of the entity, cyber security risks may have a pervasive impact on the financial report and affect several different elements such as provisions, fair value of assets or going concern. **Table 2** of **Appendix 1** provides a number of examples of how cyber security can impact on the auditor's responsibility.

Where a cyber event has occurred, the auditor's responsibility is to evaluate the impact on the financial report and determine whether the financial report appropriately reflects the impact of the cyber event and presents in all material respects in accordance with the applicable financial reporting framework.

Further information / Conclusion

The AUASB has established an advisory group to assist with monitoring and responding to the impact of technology on audit and assurance. The AUASB plans to release a series of publications on a number of topics including assessing the integrity of data and assurance over cyber security controls.

If you have any comments on this publication or would like to raise an area for consideration by the AUASB, please contact enquiries@auasb.gov.au

Appendix 1

Specific considerations

When performing risk assessment, ASA 315 requires auditors to obtain an understanding of the entity and its environment which includes the entity's business model and the extent to which this integrates the use of IT. The sector in which the entity operates is also a relevant consideration here as certain sectors, such as financial services[9], may have a higher risk due to a history of breaches and the sensitive nature of data that is generally held by the entity.

Understanding the business model and the use of IT helps the auditor to understand the business risks an entity faces. Not all business risks give rise to risks of material misstatement of the financial report, and whilst cyber security poses a risk for most entities, this risk does not always result in a risk of material misstatement of the financial report which requires the auditor to design and implement a response.

The consideration of cyber security as part of risk assessment also includes auditors enquiring as to whether a cyber attack has occurred. If it has, the auditor ordinarily considers the extent to which such a breach had the potential to affect financial reporting. Where financial reporting may be affected, the auditor may decide to understand, and then test the related controls to determine the possible impact or scope of potential misstatements in the financial report. The auditor considers whether the entity has provided adequate disclosures in relation to the incident.

Table 1 – Consideration of cyber security as part of risk assessment

ASA 315 *Identifying and Assessing the Risks of Material Misstatement*	As part of risk assessment, auditors obtain an understanding of the entity and its environment, which includes the IT systems relevant to the preparation of the financial report and risks due to IT. Broadly, as part of ASA 315, auditors are required to obtain an understanding of the entity and its environment, the entity's system of internal controls and the applicable financial reporting framework. In understanding the entity and its environment, auditors may consider the impact of cyber security as part of: • The structure and complexity of the entity's IT environment, including the extent of use of third-party systems or outsourced IT providers. For example, there may be known vulnerabilities in particular software or systems used by the entity or that an outsourced IT provider operates with little or no oversight from management and those charged with governance. Appendix 5 of ASA 315 includes enhanced guidance on where there may be a heightened risk related to cyber security, for example: o When there are web-based transactions or transactions involving external interfaces. o Considering risks related to unauthorised access by internal or external parties to the IT environment and data, and how to respond if information about a security breach has been identified.

[9] Australian Financial Review – Cyber attacks 'the biggest risk in banking'.

ASA 315 *Identifying and Assessing the Risks of Material Misstatement* *(continued)*	This includes consideration of third parties which may have vulnerabilities in their IT environment which provide an access point to the entity's IT environment. o IT staff gaining access privileges beyond those necessary. o Use of legacy technology which are no longer supported by vendors can provide a vulnerability for an entity's systems. • Industry factors such as particular industries being targeted. Whilst all sectors are likely to be exposed to cyber security risks, there are some sectors that have a higher inherent risk due to the nature of their operations and history of attacks. For example, during 2020, health care and transport organisations were targeted by attackers. ASA 315 also requires auditors to obtain an understanding of management's risk assessment process. Auditors, as part of this, consider how management have considered and assessed the risk due to cyber security.
ASA 330 *The Auditor's Responses to Assessed Risks*	ASA 330 requires the auditor to design and perform further audit procedures in response to the assessed risks of material misstatement. If cyber security risks form part of an assessment of a risk of material misstatement, the auditor's procedures are required to be responsive to these risks and obtain more persuasive audit evidence the higher the assessment of risk. Poor cyber security controls or known cyber security incidents may have an impact on: • The ability for the auditor to rely on controls if they are heavily IT based. • The integrity of data to be used in a particular response. The auditor should be aware of instances where procedures usually performed may no longer be able to be undertaken. Additionally, during the audit, the auditor may identify or become aware of cyber security incidents and may need to adjust the determined risk of material misstatement and response to take this into account. (See ASA 500 *Audit Evidence* regarding reliability of evidence.)

Table 2 – Consideration of the impact of identified risks of material misstatement related to cyber security risks on the audit

ASA 240 *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report*	The primary responsibility for the prevention and detection of fraud rests with management and TCWG. The entity is responsible, even where IT functions are outsourced, for having a process to identify and respond to the risks of fraud, which includes risks of fraud as a result of cyber attacks. Examples of types of cyber attacks and fraud include: • E-mail fraud such as bogus invoice schemes or impersonating key personnel in an entity and requesting a funds transfer. • Phishing schemes such as an attacker using an authentic-looking e-mail from an entity (such as a supplier) to trick the recipient into clicking a link in the email which provides access to the entity's systems. Once the system is accessed, a number of different actions can be taken by the attacker. • Ransomware which is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. Not all examples will be applicable to each audit and it is the responsibility of the auditor to determine the procedures that are to be undertaken to identify and respond to risks of material misstatement arising from fraud. As part of this process auditors could: • Make enquiries of management including IT personnel on: o Whether the entity has been subjected to any attacks. Generally, attacks are not isolated so if the entity has been subjected to a phishing attack there is a risk that not all instances have been detected by the entity. o The nature of data held by the entity, the sensitivity of the data and the location of that data (whether held by the entity or a third party). • Assess whether the engagement team has the knowledge and skill and consider whether an auditor's expert should be used. The auditing standards do not specifically require the use of experts however individuals with specialized skills and knowledge, such as forensic and IT experts, may better respond to assessed risks. Auditors should also be aware of any non-compliance with law or regulation (NOCLAR) where fraud is detected as part of the audit, particularly where it involves a breach of data privacy or other legislation. See the below section on ASA 250 *Consideration of Laws and Regulations in an Audit of a Financial Report.*

ASA 250 *Consideration of Laws and Regulations in an Audit of a Financial Report*	In meeting the requirements of ASA 250, an auditor may for example consider: • Where a data breach has occurred, requirements of the *Privacy Act 1988* including the Notifiable Data Breaches Scheme requiring entities to provide notice to the Office of the Australian Information Commissioner (OAIC) and affected individuals. • Requirements under the *Corporations Act 2001* may be relevant. In 2020, ASIC commenced proceedings against an AFSL holder for failing to have adequate cyber security systems[10]. • Data protection legislation in other jurisdictions where the entity operates such as the UK General Data Protection Regulation (UK GDPR).
ASA 260 *Communication with Those Charged with Governance* and *ASA 265 Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*	The auditing standards require auditors to provide TCWG with timely observations arising from the audit that are significant and relevant to their responsibility to oversee the financial reporting process. Particularly, ASA 265 requires the auditor to communicate deficiencies in internal controls that the auditor has identified during the audit. Auditors may consider including matters related to cyber security as part of this communication, for example: • Significant difficulties encountered during the audit as a result of cyber security such as being unable to perform proposed responses to risks of material misstatement due to difficulty determining the reliability of data to be used due to poor cyber security. • Deficiencies in controls as a result of cyber security. The Australian Cyber Security Centre, which is part of the Australian Signals Directorate, has published the Essential Eight which is a prioritised list of mitigation strategies to assist entities in protecting their systems against cyber security attacks (a more detailed list of mitigation strategies is also provided). Auditors may consider using this guidance, or other frameworks such as NIST, when communicating with TCWG regarding difficulties encountered or deficiencies in internal controls.
ASA 210 *Agreeing the Terms of Audit Engagements* and ASA 580 *Written Representations*	Management and TCWG are responsible for assessing cyber security risks and implementing appropriate controls to respond to those risks. To communicate and reinforce this responsibility, an auditor may consider including cyber security as part of the terms of engagement and written representation requested from management and TCWG.

[10] 20-191MR ASIC commences proceedings against RI Advice Group Pty Ltd for alleged failure to have adequate cyber security systems https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-191mr-asic-commences-proceedings-against-ri-advice-group-pty-ltd-for-alleged-failure-to-have-adequate-cyber-security-systems/

ASA 500 *Audit Evidence*	Auditing standards require the auditor to obtain sufficient appropriate audit evidence to support their opinion. A key element of this is the reliability of audit evidence. Reliability of audit evidence is influenced by its source and its nature, and the circumstances under which it is obtained, including the controls over its preparation and maintenance where relevant. Auditors should consider the implications of cyber security as part of their assessment of reliability of audit evidence and, where there are doubts over the reliability of audit evidence, consider the implications for the audit.
ASA 540 *Auditing Accounting Estimates and Related Disclosures*	ASA 540 requires the auditor to obtain sufficient appropriate audit evidence about whether accounting estimates and related disclosures in the financial report are reasonable in the context of the applicable financial reporting framework. A number of matters raised above as part of ASA 240 will be relevant for the auditor in considering the impact of cyber security on ASA 540. Matters the auditor may consider as part of meeting the responsibilities under ASA 540 may include: • Whether there is any indication that assets, such as Property, Plant and Equipment, intangible assets and goodwill as well as financial assets, may be impaired as a result of a cyber attack. For example: o Intellectual property has been stolen by an attacker. The loss of exclusivity may impact on the recoverable amount of the related asset. o An attack has shut down key infrastructure which is required to be constantly running. The shutdown may result in damage to the equipment which may impact on the recoverable amount of the asset. • Assessing the adequacy of provisions or disclosures of contingent liabilities because of a cyber attack. For example, where a significant data breach has occurred, there may potentially be fines, penalties or legal action from regulators as well as legal action initiated by impacted individuals. The matters raised above may also have implications for going concern assessment which is discussed below as part of ASA 570 *Going Concern.*

ASA 560 ***Subsequent Events***	An auditor is required to obtain sufficient appropriate evidence of events occurring between the end of the financial reporting period and sign off but to also respond appropriately to facts that become known to the auditor after the date of the auditor's report, that, had they been known to the auditor, may have caused the auditor to amend the auditor's report. An important consideration for auditors is that the average time to identify and contain a cyber security breach is approximately 280 days.[11] Auditors should be aware of the possibility that a cyber security breach crosses multiple financial reporting periods and understand what their responsibilities are in accordance with ASA 560.
ASA 570 ***Going Concern***	ASA 570 requires the auditor to obtain sufficient appropriate audit evidence regarding, and conclude on, the appropriateness of management's use of the going concern basis of accounting in the preparation of the financial report and conclude, based on the evidence, whether a material uncertainty exists. A cyber attack may severely impact an entity's business operations and, in extreme circumstances, its ability to continue as a going concern, for example: • Ransomware attacks locking key systems or records impacting the ability of the entity to operate for a period of time. This includes the loss of important records such as accounts receivable ledgers as a result of the ransomware. • Distributed Denial-of-Service (DDoS) attacks on an entity's online infrastructure such as an online store, delivery system, automated warehouse or invoice and payment system. • Brand damage as a result of cyber attacks impacting future operations/cashflows. For example, loss of customers who had their data stolen as part of a data breach.

[11] IBM Cost of a Data Breach Report 2020 (https://www.ibm.com/sg-en/security/data-breach). Data breaches analysed occurred between August 2019 and April 2020.

Terms used

The below terms have been used in this publication. The definitions are taken from the *Australian Cyber Security Centre* Glossary:

- Cybercrime – Crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also includes crimes where computers facilitate an existing offence, such as online fraud or online child sex offences.
- Cyber attack – A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.
- Cyber event – 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.
- Cyber security – Measures used to protect the confidentiality, integrity and availability of systems and information.
- Cyber threat – Any circumstance or event with the potential to harm systems or information.