



Digital Transformation

11 Cybersecurity

27 February 2023



Version Control

Document:	11 Cybersecurity	Version	1.0
Author:	Roger Jameson, Director Housing Information Solutions	Issue Date	27-Feb-2023
Reviewed by:	John Parkinson, Director Housing Information Solutions Adam West, Head of Business, CHIA NSW Alex Dordevic, Director Leading Practice, CHIA Vic	Review Date	22-Feb-2023

Version History					
Version No	Date	Revised By	Description	Reviewed	Status
0.1	22-Feb-2023		1. First draft for CHIA review	John Parkinson Adam West Alex Dordevic	Reviewed

Distribution

This document is intended for the sole use of the Community Housing Industry Association NSW, the Community Housing Industry Association Victoria and their respective member organisations. It is not be provided to any unrelated third parties without the written permission of Housing Information Solutions.

Copyright © 2023 Housing Information Solutions. All rights reserved.

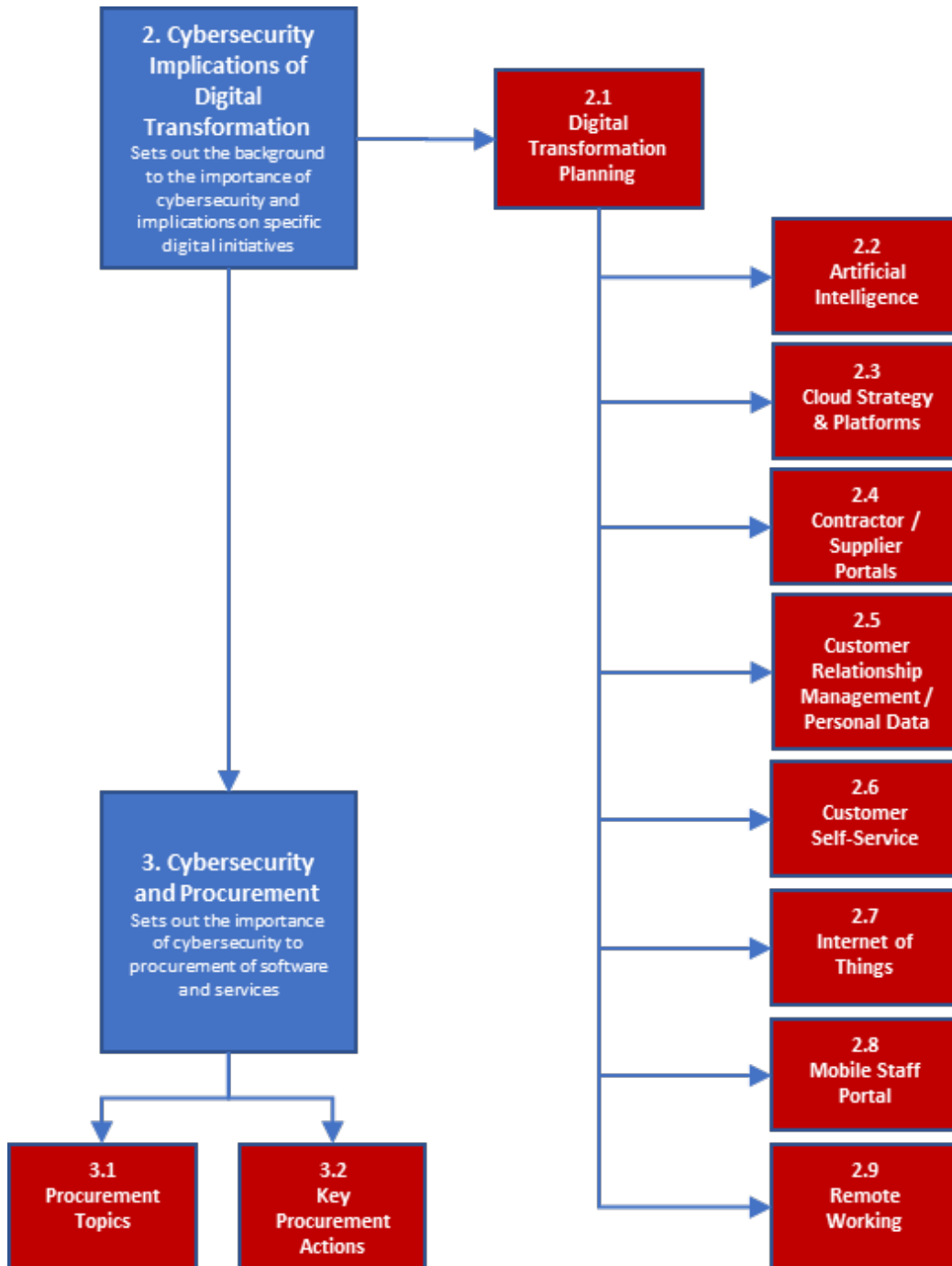
Contents

1.	Introduction	1
2.	Cybersecurity Implications of Digital Transformation	3
2.1	Digital Transformation Planning	6
2.2	Artificial Intelligence	6
2.3	Cloud Strategy & Platforms.....	9
2.4	Contractor / Supplier Portals	10
2.5	Customer Relationship Management / Personal Data	11
2.6	Customer Self-Service	13
2.7	Internet of Things / Smart Asset Management	15
2.8	Mobile Staff Portal	17
2.9	Remote Working.....	19
3.	Cybersecurity and Procurement	21
3.1	Procurement Topics	22
3.1.1	Standards	22
3.1.2	Information Security Management.....	25
3.1.3	Data Retention Policies.....	25
3.1.4	Audit Certificates.....	26
3.1.5	Independent Assessments	26
3.1.6	Security Monitoring	26
3.1.7	Data Storage.....	26
3.1.8	Patch Releases	26
3.1.9	Supplier Cybersecurity Risks & Capabilities	26
3.1.10	Functional Requirements.....	28
3.2	Key Procurement Actions.....	29

1. Introduction

The purpose of this document is to set out the cybersecurity implications that need to be considered when implementing digital transformation initiatives.

It will take you through the following:



During the course of 2022, CHIA NSW engaged consultants Tesserent to prepare an Information Technology and Cyber Risk Assessment framework and associated toolkit, which was published and distributed to CHIA NSW member organisations on 14 July 2022. This guide shows how community housing organisations (CHOs) should best align their IT management to cybersecurity maturity levels.

Taking that into account, this document will **NOT** therefore provide guidance on how CHOs should:

1. Identify, quantify and record the current state of cybersecurity in their respective organisations.
2. Identify suitable and control strategies to improve the overall cybersecurity posture.
3. Analyse the key areas of their business that impact upon the achievement of cybersecurity.
4. Identify key risks to cybersecurity and where those risks are not sufficiently managed.
5. Determine their level of cybersecurity maturity.
6. Self-assess their alignment to the controls defined within the CHIA NSW Cybersecurity Framework which incorporates the recommended and relevant guidance from the Essential 8 Principles of Cybersecurity.
7. Determine mitigation strategies.
8. Develop practical control implementations to:
 - a. Better secure information and information technology systems.
 - b. Reduce the risk of cyber breach and unauthorised data extraction through inadvertent or intentional loss or unrecoverable outage events.

This document should be read in conjunction with the following which are included in the CHIA NSW and CHIA Vic Digital Transformation Toolkit pack:

Document Name	Description
01 Developing an IS IT Strategy.pdf	Provides a stepped-out process for CHOs on how to develop information technology and information systems strategies.
02 IS-IT Strategy Toolkit.xlsx	Aligned to the strategy document, the toolkit provides series of templates to use in defining your strategy.
03 Assessing IT Improvements.pdf	Investigates and researches the available opportunities for IT improvements needed by CHOs and document the findings with recommendations.
04 Digital Readiness Assessment.pdf	Sets out the approach on how to determine the state of a CHO's digital readiness and the results of a survey completed by 29 CHOs in NSW and Victoria
07 Digital Transformation Implementation Guide.pdf	Sets out the steps community housing organisations (CHOs) need to follow in defining and implementing digital transformation initiatives.
08 Digital Transformation Planning Toolkit.xlsx	Provides a toolkit of templates on defining and prioritising digital objectives, defining projects aligned to objectives, assessing risk and defining a digital transformation roadmap.
09 Case Studies.pdf	Sets out a range of case studies across a selection of industries, with each study focussing on the challenge(s) that each organisation has faced, the solutions it implemented and the results that have eventuated

Document Name	Description
10 Digital Channels & Utilisation.pdf	Explores the use of digital and non-digital channels and provides an assessment on the areas of operation where digital transformation could add most value through effective utilisation, taking into account the associated implications that need to be considered.

2. Cybersecurity Implications of Digital Transformation

Digital transformation initiatives will increase the risk of cybersecurity attacks. Why? Simply put, you are expanding the range of technology tools as well as expanding the extent of online access, and therefore you are opening yourself up to greater risk than what you have now.

The importance of cybersecurity in an ever-increasing digital environment should never be underestimated. A single breach could have serious consequences to a CHO's operations and reputation. The number of ransomware attacks are increasing rapidly across many industry sectors. Not only that, such attacks are becoming increasingly sophisticated. CHOs need to be pro-active, assess the cybersecurity risks to their infrastructure and operations and develop mitigation strategies.

To reinforce the importance of cybersecurity and the impact of ransomware attacks, in January 2022, Sophos, (<https://www.sophos.com/en-us>) a British based security software and hardware company specialising in the development and delivery of cybersecurity-as-a-service, commissioned research agency Vanson Bourne (<https://www.vansonbourne.com/>) to conduct an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations (100-5,000 employees) across 31 countries¹. Respondents were asked to respond based on their experiences over the previous year.

The survey found that 66% of businesses globally were hit by ransomware in 2021. The survey also found that Australia was well above this rate with 80% of organisations being hit with ransomware in 2021 (up from 45% in 2020).

The average cost to respond to an attack in Australia was \$1.61million, with almost half of those attacked paying the cybercriminals a ransom.

A 2022 report from mobile security vendor Zimperium² found that a global average of 23% of mobile devices



¹ <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgi9bxgi9/sophos-state-of-ransomware-2022-wp.pdf>

² <https://www.zimperium.com/global-mobile-threat-report/>

encountered malicious applications in 2021. The firm also found that 75% of phishing sites specifically targeted mobile devices that year.

A study released in February 2023 by Netskope³, a supplier of secure access service edge services found that:

1. Over half of Australian organisations have not invested enough in cyber security in the past three years, with nearly one in five believing it was not a priority
2. The underinvestment was starker among small companies, of which 69% had not invested enough in cyber security
3. Just 27% of Australian technology leaders today have well-defined and stringent incident response plans to face a variety of scenarios, and regularly exercise them.
4. There is no consensus on how to handle an incident. The 300 survey respondents were divided, with just half (51%) stating they would be unlikely to pay if they were victims of ransomware.

If you have followed the guidance in the CHIA NSW Information Technology and Cyber Risk Assessment framework / tool, you should be logging digital online access in your cyber risk register and in your cybersecurity risk matrix.

So, why do this? Why implement digital initiatives if they make you more open to further risk?

As mentioned in **01 Digital Transformation Implementation Guide.pdf**, and in terms of background to this document, digital transformation is about:

1. Better ways of **doing** things
2. **Creating** value
3. **Improving** the customer / supplier experience
4. **Automating** tasks
5. Improving how services are provided in more **efficient** ways to deliver experiences in a **co-ordinated, consistent and cost-effective way**.
6. **Building collaborative capabilities** that can better support CHOs in delivering services
7. **Fostering business resilience** and capabilities for the future and thereby reinforcing CHOs' growth potential.
8. **Focussing on people and processes as well as technology** - the latter is the catalyst for helping or supporting you to provide these better ways of doing things and providing solutions.

The benefits that digital transformation offers to your CHO far outweighs the cybersecurity risks, however, you need to identify and quantify these risks and define appropriate mitigation strategies.

The document **08 Digital Transformation Planning Toolkit.xlsx** provides a worksheet to record the risks associated with your digital objectives and projects. Digital transformation WILL create IT security risk. Any vulnerabilities can be potentially exploited by cybercriminals who can deploy ransomware to encrypt files and extract sensitive data, such as records relating to tenants,

³ https://www.computerweekly.com/news/365530312/Australian-organisations-underinvesting-in-cyber-security?utm_campaign=20230214_Noventiq+eyes+APAC+IT+services+market&utm_medium=email&utm_source=MDN&source_ad_id=365530312&asrc=EM_MDN_260600608&bt_ee=1pi5oAsCHb0mh4My7Zy8YW%2F51FyNn7D4QPzKA6cWwMBh742mML%2FMLmezKyOHhXh7&bt_ts=1676368241298

household members, contact details, income and financial information i.e. personally identifiable information (PII).

A successful digital transformation requires CHOs to balance the securing of digital assets without stifling innovation. Furthermore, as part of its digital transformation approach, CHOs will also face the challenge of how to establish secure processes again without stifling innovation. Based on this, there is therefore clearly a fine balance in ensuring that:

1. Your digital transformation initiatives will result in the array of desired improvements (as set out above)
2. Your IT security can be set up and managed to support the desired innovation whilst, at the same time, addressing the associated cybersecurity risks such that they have a minimal impact on your organisation being able to achieve its digital transformation goals.

In essence, digital transformation and cybersecurity are inextricably linked. With the increased use of technology and collection of personal data, the need for protection from cybercriminals increases.

In view of the cybersecurity risks associated with digital, it is logical that you should also cross-reference these with the organisation-wide risks you will have identified in following the guidance in CHIA NSW Information Technology and Cyber Risk Assessment Framework.

In addition to this, refer also to section 6.6 Risk in **07 Digital Transformation Implementation Guide.pdf**. This sets out the common digital risk factors which are as follows:

1. Potential complexity of IT environment driven by growing digitisation.
2. Lack of integration.
3. Increased cybersecurity attacks, breaches and incidents as the digital access and platforms expand.
4. Process automation, particularly with the addition of new technology, which may not have been fully considered.
5. Key changes to policies and procedures.
6. Resources and skill sets.
7. Growing importance of data privacy, trust, compliance and balancing this against increased analytical capabilities.
8. Shifts in working and attitudes towards technology use which can impact on operations.

So let us look in a bit more detail as to the cybersecurity implications of implementing digital transformation initiatives taking into account the following considerations:

- | | |
|----------------------------|---|
| 1. Situation / opportunity | What is the current situation or future opportunity that could give rise to a cybersecurity threat arising from a digital initiative? |
| 2. Risk implications | What are the risk implications that can be identified from the situation or opportunity and what needs to be assessed? |
| 3. Measures / action | What action is needed to mitigate the risk? |

2.1 Digital Transformation Planning

Consideration	Assessment
Situation / Opportunity	Digital transformation overall provides many opportunities for CHOs to improve how they deliver services and how they can increase the number of communication channels.
Risk Implications	Cybersecurity risk must form an intrinsic part of your planning. Securing technology is becoming harder in view of the growing number of attacks across various industries. Community housing is not immune and never will be.
Measure / Action	<ol style="list-style-type: none"> 1. Prepare a digital transformation strategy, setting out all risks as indicated above, including cybersecurity. Assess how you will protect your digital assets. 2. Ensure your budgets include provision for IT security. If you have a budget for IT security, determine whether the amount allocated is sufficient. 3. Ensure security considerations are incorporated as part of any digital transformation initiative. 4. Ensure you have staff with IT security knowledge and skill sets. Alternatively, you will need to rely on third-party advisory organisations. 5. Ensure your management team is aware of how any inability to secure digital assets could potentially harm the CHO. 6. Verify the security capabilities of every digital app that you will be procuring. 7. Implement a security governance approach.

The following sections are set out in alphabetical order by topic.

2.2 Artificial Intelligence

Consideration	Assessment
Situation / Opportunity	<p>AI is very much in its infancy in the CHO sector, however as indicated in 03 Assessing IT Improvements.pdf and 10 Digital Channels & Utilisation.pdf, it has the potential to add much value to CHOs in how it can be used to predict events and behaviour as well as suggest actions for a CHO to consider and implement.</p> <p>Not only can AI be used to inform the development and implementation of new housing initiatives and policies, it can also be used as an aid to addressing cybersecurity. AI can potentially detect patterns of behaviour across networks and in theory, be able to quickly detect vulnerabilities and</p>

Consideration	Assessment
	<p>threats before an attack happens. AI improves its knowledge to understand cybersecurity threats by consuming billions of data artifacts.⁴</p> <p>IBM states that adopting AI and automation in security saves more than 14 weeks in threat detection and response times, and helps to reduce the overall costs of a data breach.⁵</p>
Risk Implications	<ol style="list-style-type: none"> 1. AI algorithms can be used by hackers to identify systems with weak security or that are likely to contain valuable data among the millions of computers and networks connected to the Internet. It is therefore imperative that CHOs assess the risks associated with their systems and review security levels. 2. Attackers can use AI tools to constantly change malware signatures to evade detection as well as large amounts of malware to increase the power of attacks. 3. AI can also be used to create large numbers of personalised phishing emails designed to trick receivers into divulging sensitive information and have become increasingly good at evading automated email defense systems designed to filter out this type of mail. 4. AI has even been used to artificially mimic the voices of senior executives in an effort to fraudulently authorise transactions. 5. Machine learning algorithms can be exploited by altering functionality through data manipulation.
Measures / Action	<ol style="list-style-type: none"> 1. To a certain extent, any measures that a CHO can implement will be influenced by the current level of maturity and use of AI in the sector. The measures suggested in subsequent sections below highlight the varying measures that can be taking in mitigating cybersecurity risks as best as possible. CHOs are advised to keep abreast of the evolving benefits that AI can offer not only to their operations and data analysis but also assess how this medium could be used to address cybersecurity risk. Clearly, use of AI will require the development of appropriate skill sets in each CHO which choose to deploy it. 2. Various policies and standards have been proposed by the Brookings Institution⁶ and the ETSI Industry Specification Group⁷ in relation to AI security. As AI technology matures, it is to be hoped that standards will be universally accepted and followed. 3. Almost 75% of IT security executives have indicated that deploying AI improves the efficiency and accuracy of security measures and allows IT security staff to respond faster to incidents.⁸

⁴ <https://www.ibm.com/security/artificial-intelligence>

⁵ <https://securityintelligence.com/posts/ai-capabilities-transform-security/>

⁶ <https://www.brookings.edu/research/how-to-improve-cybersecurity-for-artificial-intelligence/>

⁷ <https://www.etsi.org/technologies/securing-artificial-intelligence>

⁸ <https://www.capgemini.com/gb-en/insights/research-library/reinventing-cybersecurity-with-artificial-intelligence/>

Consideration	Assessment
	<p>4. In the United States, the National Security Commission on Artificial Intelligence (NSCAI) has highlighted the importance of building trustworthy AI systems that can be audited through a rigorous, standardised system of documentation. To that end, the commission has recommended the development of an extensive design documentation process and standards for AI models, including what data is used by the model, what the model’s parameters and weights are, how models are trained and tested, and what results they produce. These transparency recommendations address some of the security risks around AI technology, but the commission has not yet extended them to explain how this documentation would be used for accountability or auditing purposes⁹</p>

⁹ <https://www.nsc.ai.gov>

2.3 Cloud Strategy & Platforms

Consideration	Assessment
Situation / Opportunity	<p>Many CHOs are migrating to cloud-based systems and platforms, implementing IT operating models that can support their growth, digitisation and diversity.</p> <p>One of the most significant changes caused by digital transformation is increased migration to the cloud.</p> <p>Cloud providers such as Google, Microsoft and AWS have invested huge resources into product security and, as described further below, system developers need to abide and comply with their guidelines.</p> <p>Some CHOs may be particularly vulnerable to cyberattacks such as ransomware because they do not have the resources on improving their cybersecurity. Moving to the cloud could improve their overall security because the cloud providers have some of the most robust security currently available. It can be argued that moving data to the cloud is more secure than keeping it on-site due to the security provisions implemented, however, that does not remove the risk as cybercriminals become ever more sophisticated in launching attacks.</p> <p>Cloud computing offers a range of advantages as set out in 03 Assessing IT Improvements.pdf.</p>
Risk Implications	<ol style="list-style-type: none">1. Digital transformation can significantly increase reliance on third parties, specifically cloud providers and best of breed digital software suppliers. Whilst many CHOs will rely on their main systems supplier for all of their products and needs, with digital transformation posing a diversity of solutions and approaches, it is distinctly possible that the number of cloud suppliers providing services and products to the CHO sector will increase.2. Your data will be held off-site. In effect, you are relying on your supplier to look after it for you as well as providing you with the system or application to access it. You are therefore trusting your supplier to keep your data safe. You therefore need to be aware of this risk and seek assurances from your supplier as to the cloud security measures it has deployed.3. While cloud-based data storage can be equipped with cybersecurity measures to prevent data breaches, if a CHO has a large amount of valuable customer data, even a partial breach can have far-reaching negative effects.4. An organisation's cloud storage contains enormous hordes of extraordinarily valuable data, if an attacker gains access to merely a fraction of these data, it can cause significant damage.5. Though cloud storage programs such as Google Cloud, Microsoft Azure and Amazon Web Services (AWS) may have strong security measures in

Consideration	Assessment
	<p>place, client mistakes can lead to dangerous malware and online scams, which can result in cloud storage breaches.</p> <ol style="list-style-type: none"> 6. If your CHO experiences a ransomware attack, and unless your support contract states otherwise, it will be you who will be paying the hacker. If your data is compromised, it will be you who will need to explain what happened. This highlights why cybersecurity must be one of your highest priorities, ensuring you have trained staff, log your cyber risks and have mitigation strategies in place. 7. The shift to agile working and increasing dependency on cloud-based systems means cyberattack is an ever-present risk to CHOs.
<p>Measures / Action</p>	<ol style="list-style-type: none"> 1. Implement a holistic cloud security strategy, focusing on access management, threat monitoring and incident response. 2. Ensure systems provide multi-factor authentication (MFA) which requires the user to provide two or more verification methods to access an account, system, application or network. 3. Conduct regular penetration testing. 4. Ensure your suppliers conduct regular penetration testing as part of your support contracts. 5. Refer also to section 3 below on security topics to address when procuring software and services from cloud providers. Seek assurances on how your provider has invested in managed detection and response solutions and how traffic is monitored. Also clarify how patch management is administered and deployed. 6. Before procuring any software or services, check the contract being provided by the supplier and consider the cybersecurity measures and implications. <ol style="list-style-type: none"> a. ISO 27017 is an information security framework for organisations using (or considering) cloud services. b. Cloud service providers need to comply with this standard because it keeps their cloud service customers (and others) safer by providing a consistent and comprehensive approach to information security. (Refer also below to section 3.1.1)

2.4 Contractor / Supplier Portals

Consideration	Assessment
<p>Situation / Opportunity</p>	<p>Interaction with third-party suppliers and contractors is a key function of any CHO.</p> <p>Increasingly, CHOs are deploying supplier / contractor portals as the means of communication and interaction with their suppliers and contractors.</p> <p>Some of the main system suppliers to the community housing sector offer a contractor / supplier portal as standard.</p>

Consideration	Assessment
	Some CHOs deal with sizeable suppliers / contractors and in some instances, a sole facilities management maintenance provider.
Risk Implications	<ol style="list-style-type: none"> 1. Supply chain weaknesses can make CHOs highly vulnerable to attack. 2. Hackers could potentially gain access to your systems / network via the systems used by your suppliers / contractors, with the risk of behaviour being perceived as being legitimate. 3. Data could be obtained through third party breach and held to ransom or with phishing emails being sent to tenant contacts.
Measures / Action	<ol style="list-style-type: none"> 1. As part of the supplier procurement process, seek details on how their systems and IT infrastructure are protected. How often is this audited? 2. Seek guarantees and verification on the security measures that each supplier / contractor has implemented. 3. As part of any tendering process, include details of your requirements to obviate any future cyber breaches. 4. Ensure that security is incorporated in any supplier / contractor contracts. 5. Explore use of third-party organisations specialising in network monitoring and threat identification.

2.5 Customer Relationship Management / Personal Data

Consideration	Assessment
Situation / Opportunity	<p>Customer relationship management is featured as a separate section in view of its relevance to holding such a potential wide range of information on tenants, household members, applicants and all other types of contacts and organisations who interact with a CHO.</p> <p>The principles in terms of risks and measures in relation to cybersecurity are equally as relevant for any back-office system which is being used to support tenancy and property management functions.</p> <p>Some suppliers provide customer relationship management (CRM) functionality as integral to their core housing management system but not currently all. Others provide similar features to a point within the structure of their housing or tenancy and property management system.</p> <p>Systems with good customer relationship management can benefit your operations by helping you to centralise, optimise and streamline communications with your tenants, clients, applicants, household members, stakeholders, agencies and other third parties.</p> <p>CRM functionality can be used to organise and manage contacts and all forms of communications as well as automating key tasks. It tracks and manages all interactions and communication your staff have with all people you deal with. It enables you to know more about people other than your tenants.</p>

Consideration	Assessment
	<p>CRM-based as well as tenancy and property management systems have or <i>should have</i> established user security protocols to control both access and what users can view and update.</p>
<p>Risk Implications</p>	<ol style="list-style-type: none"> 1. Any system used to manage tenancies (irrespective of whether this is a CRM or a core housing management system) and hold personal data is at risk of cyber-attack. 2. Such systems hold a considerable array of PII data. CHOs have a serious responsibility to ensure they protect it in view of the potentially serious consequence on their tenants if it falls into the wrong hands. 3. Personal data can be used can be used by hackers to make money, by selling it on in order to carry out scams or steal identities or obtain more information. 4. Systems providing CRM functionality contain an abundance of data about any person or organisation. That is their primary purpose. The key risk therefore is what would happen to this data if a cybercriminal gained access to your CRM system. 5. As an example, in late July 2022, Clarion, a UK housing association managing 125,000 homes, was subject to a cyber-attack on its CRM system which affected a number of its services as well as phone lines. It advised residents not to contact it by phone unless an emergency repair was needed and to assume that any email sent to it by 17 June 2022 had not been received.¹⁰ Clarion said the cyberattack could result in a long period of disruption and that it would have to rebuild some of its systems completely. Clarion residents raised concerns about their rent payments not going through with confusion over accounts showing tenants in arrears, and home sales potentially falling through. It is one of a string of UK social landlords to be hit by cyberattacks in the past 18 months. Other UK housing associations Flagship and Bromford were also hit by security breaches, and councils such as Hackney and Gloucester City Council also still feeling the impact of cyberattacks that took place earlier in 2022.
<p>Measures / Action</p>	<ol style="list-style-type: none"> 1. Ensure you have MFA applied to your systems. 2. Ensure you retain digital copies of your core system data and manage your backups. 3. Ensure your systems are maintained and updated. 4. Segregate your networks. <ol style="list-style-type: none"> a. The Australian Cybersecurity Centre (ACSC) recommends segregating networks into multiple zones to protect servers and

¹⁰ <https://www.insidehousing.co.uk/news/no-evidence-passwords-or-customer-information-accessed-in-cyberattack-says-clarion-76740>

Consideration	Assessment
	<p>services as well as data.¹¹ (Refer also to the measures listed above for cloud computing).</p> <ul style="list-style-type: none"> b. Network segmentation involves partitioning a network into smaller networks; while network segregation involves developing and enforcing a ruleset for controlling the communications between specific hosts and services. c. Once an adversary compromises a network, usually through the compromise of a host under the control of a legitimate user by means of social engineering, they will attempt to move around the network to locate and access sensitive information, hosts and services. In order to minimise the impact of such a network intrusion, it should be as hard as possible for the adversary to find and access such information, move undetected around the network and remove information from the network. d. ACSC highlight examples of organisations which have been subject to ransomware attacks, have been able to confine these to particular parts of their network, and protect other segments, including vital data. <p>5. In addition, adopt the measures set out in section 2.3 for those CRM systems being offered to the CHO sector as cloud-based products accessed via a web browser.</p> <ul style="list-style-type: none"> a. Note that some tenancy and property management systems currently being supplied to the sector are NOT cloud based. b. Refer to 03 Assessing IT Improvements.pdf as to the definitions and differences between cloud and hosted systems.

2.6 Customer Self-Service

Consideration	Assessment
Situation / Opportunity	<p>A self-service portal is an additional channel by which a tenant can either make an enquiry online or submit a service request to the CHO.</p> <p>A good, well designed self-service portal offers the potential to reduce the demands on your front-line staff. Self-service portals provide tenants with instant access to information, allow personalisation, and save valuable time and organisational resources.</p> <p>Self-service features include self-resolution of issues through use of a knowledge base, password reset, self-logging of incidents, collaborative spaces, service requests and chat services. Refer also to 03 Assessing IT Improvements.pdf and 10 Digital Channels and Utilisation.pdf for further details.</p>

¹¹ <https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation>

Consideration	Assessment
	<p>Implementation of a self-service portal offers an array of potential benefits. They can empower tenants to find information, request services, and resolve their issues. Such portals also provide tenants with a fast and direct way of getting answers to a variety of questions and issues. From uploading documents and submitting transactions to communicating with the CHO's service teams, tenants can stay in one app or user interface to complete business tasks.</p>
<p>Risk Implications</p>	<ol style="list-style-type: none"> 1. Poorly designed and / or managed customer self-service portals can risk the integrity of personal and financial data. 2. Security vulnerabilities could potentially happen at any level of the portal such as from the client interface through to the back-office system. 3. Subject to their design and security, self-service portals could be open to fraudulent activity in view of the extent of PII data held. 4. As portals store and manage a significant amount of tenant data, it is absolutely critical to secure your portal to avoid exposing tenants to significant risk.
<p>Measures / Action</p>	<ol style="list-style-type: none"> 1. As customer self-service portals store and manage much PII data, it is vital to ensure that access is properly controlled and managed. 2. Clearly define your requirements in terms of purpose and use of the portal. From this, determine the security measures needed to ensure proper and secure access. 3. Provide secure user two-factor authentication functions when logging in. Ensure security is embedded in the design of the portal. Consider using a mobile number to serve as primary authentication, irrespective of whether the client is accessing it from a laptop, tablet or mobile device. 4. Ensure that web application firewalls are in place with secure-socket-layer certification (SSL), network monitoring and fraud analytics. 5. Check and verify what your digital portal supplier provides in terms of data security. 6. Seek assurances from your supplier as part of your procurement approach on how the products have been designed taking into account cybersecurity risks and capabilities. Refer also to section 3 below which sets out the approach you should take to procurement. 7. Ensure that security features are embedded as standard in the portal solution. Remember that self-service portals are accessible by users with different means, such as mobiles, tablets as well as laptops and PCs and using different browsers. Consider using a mobile app to serve as the primary authentication device for desktop access. 8. Check that the application you are procuring has been certified under major privacy and security standards.

Consideration	Assessment
	<ol style="list-style-type: none"> 9. If the product is hosted under a specific platform such as Google, Microsoft, Amazon Web Services (AWS) etc., check how the security architecture has been designed and developed using the respective platforms. For example, the AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud, used by software suppliers in developing their products. The AWS Security Pillar is one key feature of this framework. 10. Ensure you have solid reporting tools to analyse customer activity, including suspicious patterns of email activity, location and access activity, to determine whether to continue granting access to the portal.

2.7 Internet of Things / Smart Asset Management

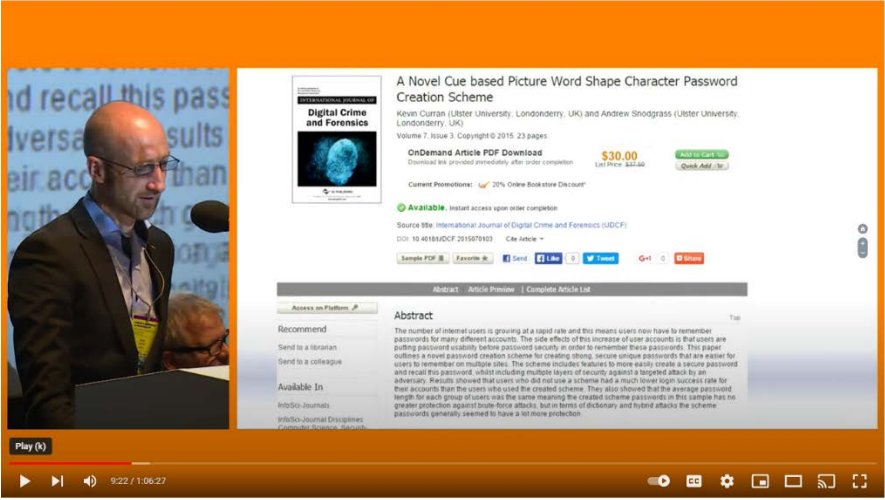
Consideration	Assessment
Situation / Opportunity	As discussed in 10 Digital Channels & Utilisation.pdf , deployment of Internet of Things (IoT) initiatives has enormous potential in terms of how use of sensors can be used for smart asset management, fire protection and personal well-being. Such deployment is likely to result in massive amounts of data.
Risk Implications	<ol style="list-style-type: none"> 1. IoT sensors, smart meters and other similar devices which may seem to be collecting seemingly-harmless data can reveal details about the behavioural habits of their users more than what one may initially think. 2. Every sensor or device could potentially be open to attack and a doorway to install ransomware. Hackers use malware to infect IoT devices and turn them into botnets, which hackers can use to probe and explore onboarding processes to find the best way to gain network access. Other hackers search for valid credentials present in IoT device firmware that is not disabled, removed or updated. Attackers then use the infected device as the entry point into the corporate network as has been experienced in recent years in other industries. 3. Hackers use IoT devices to gain access to corporate networks because they do not typically store data. Access through a trusted device means they are able to remain inside the network longer, giving them more time to circumvent even the most refined detection tools. Hackers might also use fileless malware that operates in device or software memory. 4. Control of sensors could potentially be gained by cyber criminals leading to a ransomware incident. 5. Though there are possibly a large number of component combinations that may create an IoT product, it is helpful to think of three specific kinds of IoT product components (other than the IoT device itself, which is always present in an IoT product):

Consideration	Assessment
	<ul style="list-style-type: none"> a. Specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used). b. Companion application software (e.g., a mobile app for communicating with the IoT device). c. Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device). <p>These product components have access to the IoT device and the data it creates and uses and are therefore potential risks that could impact the IoT device, customer, and others (e.g., via attacks on systems, local networks, or the Internet at large). Since these additional components can introduce new or unique risks to the IoT product, the entire IoT product, including auxiliary components, must be securable.¹²</p> <ul style="list-style-type: none"> 6. Maintaining confidentiality, integrity, and availability of data is fundamental to cybersecurity for IoT products.
<p>Measures / Action</p>	<ul style="list-style-type: none"> 1. Seek confirmation of how security functionality has been incorporated in the design of sensors and devices as well as the supporting software to reduce the risk that any component could be compromised. 2. To what extent does the device and supporting software comply with the variable IoT standards currently available? 3. Confirm whether the device has been independently assessed in relation to data security. 4. Seek confirmation of how the supplier will manage the data volumes to prevent cyber-attacks. 5. Seek assurances from your supplier as part of your procurement approach on how the products have been designed taking into account cybersecurity risks and capabilities.¹³ 6. Specifically check for cybersecurity criteria in IoT products.¹⁴ 7. Check the supplier’s approach to software updates as part of the support and maintenance agreement and seek assurances on the security in delivering future security patches. 8. Check whether the device will alert you if it starts to operate in unexpected ways, such that unauthorised access may be being attempted or malware is being loaded etc. 9. Create and implement a disaster recovery procedure that includes ransomware processes. 10. Invest in the latest firewalls and other network monitoring tools to detect and prevent new intrusions. 11. Ensure regular and proper backups of all data.

¹² <https://doi.org/10.6028/NIST.CSWP.02042022-2>

¹³ <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>

¹⁴ Ibid.

Consideration	Assessment
	<p>12. Segment data and critical networks from access by IoT devices. Refer also to the recommendations of the Australian Cybersecurity Centre (ACSC) in segregating networks into multiple zones as described above.¹⁵</p> <p>13. Disable unnecessary or unused services on devices.</p> <p>14. A useful video to watch is a presentation to a Housing Europe conference in 2018 by Kevin Curran, Professor of Cybersecurity from the University of Ulster covering the Internet of Things (video starts at 08:37). https://www.youtube.com/watch?v=a2ggoQHm_sA&t=1204s</p>
	 <p>The screenshot shows a YouTube video player with a presentation slide. The slide title is "A Novel Cue based Picture Word Shape Character Password Creation Scheme" by Kevin Curran (Ulster University, Londonderry, UK) and Andrew Snodgrass (Ulster University, Londonderry, UK). The slide includes a price of \$30.00 and an abstract. The abstract discusses the number of internet users growing at a rapid rate and the side effects of this increase on password security. It mentions that users are putting password usability before password security, leading to weaker passwords. The paper outlines a novel password creation scheme for creating strong, secure, simple passwords that are easier for users to remember on multiple sites. The scheme includes features to more easily create a secure password and recall the password, whilst including multiple layers of security against a brute-force attack by an adversary. Results showed that users who did not use a scheme had a much lower login success rate for their accounts than the users who used the created scheme. They also showed that the average password length for each group of users was the same meaning the created scheme passwords in this sample has no greater protection against brute-force attacks, but in terms of dictionary and hybrid attacks the scheme passwords generally seemed to have a lifetime protection.</p>

2.8 Mobile Staff Portal

Consideration	Assessment
Situation / Opportunity	<p>Mobile working offers a tremendous opportunity to introduce many service efficiencies and improvements however the lack of mobile functionality can provide a huge gap for CHO staff and is likely to be a source of much frustration in view of the impact on:</p> <ol style="list-style-type: none"> 1. Data duplication i.e., manually recording notes and then entering data into the system being used once back in the office 2. Manual data capture 3. Needing accurate and current information when on-site
Risk Implications	<ol style="list-style-type: none"> 1. The increased use of mobile technology by CHOs in better supporting staff whilst on-site combined with the amount of personal data stored or accessed on mobile devices makes mobile apps a lucrative target for attacks. 2. The evolving use of mobile apps across the CHO sector can ultimately result in apps replacing operating systems as the most prominent

¹⁵ [Ibid](#)

Consideration	Assessment
	<p>avenue of cyberattack. It only takes one device to be compromised for an attacker to gain access to a CHO's network.</p> <ol style="list-style-type: none"> 3. Increasing use of mobile apps pose the following risk implications: <ol style="list-style-type: none"> a. Mobile malware - malicious software that can steal login credentials while bypassing two-factor authentication (2FA). Viruses, worms and spyware are examples of malware targeting mobile devices. b. Mobile ransomware – an attack can encrypt a mobile device, locking the user out. 4. With increasing use of cloud-based system, attackers could potentially intercept, delete or alter data sent between two devices. 5. Furthermore, in some industries, there has been a trend to the 'Bring your own device (BYOD)' approach potentially resulting in increased risk of cyberattack unless the device is not subject to stringent data security assessment. 6. Loss of a device can happen and therefore the risk to data security and loss of personal data is high.
<p>Measures / Action</p>	<ol style="list-style-type: none"> 1. As with traditional desktop and enterprise applications, mobile apps can have security vulnerabilities that could be exploited by attackers to gain access to sensitive information and resources. Unlike desktop applications, precise location information, contact details, sensor data, photos and messages can be exposed through mobile apps. The combination of traditional software vulnerabilities, the additional information and services accessible through mobile apps, and the number of mobile apps demands a different approach to security. Consider how mobile device hardware can be used to enhance cybersecurity through use of cameras, facial recognition and fingerprint scanning. 2. Ensure each device being used by your CHO has mobile antivirus software. 3. Ensure each device having access to the CHO's network is tightly controlled. 4. Assess whether data is encrypted whilst in transit, such that if data is stolen, it is unreadable. Check with your supplier whether such a feature is provided. 5. Create and enforce a BYOD policy with relevant training covering all mobile devices and users. 6. Ensure policies are enacted to ensure that security patches are downloaded to all CHO-owned or BYOD devices with updates automatically applied. 7. Consider device wiping mechanisms in the event of loss by a staff member.

Consideration	Assessment
	8. Seek confirmation from your supplier(s) that the mobile apps your CHO is procuring or has procured, have been developed to conform to secure coding standards and architecture. Insecure code can become a key cybersecurity issue in relation to mobile app development.

2.9 Remote Working

Consideration	Assessment
Situation / Opportunity	<p>As a result of the Covid-19 pandemic, more staff are tending to work directly from home.</p> <p>Some CHOs already have flexible working practices enabling staff to work from home.</p> <p>In parallel to this, the evolution of mobile staff portal solutions is also better enabling staff to work from home, which can also serve as their operating base from which they can go out on site directly, without needing to first go into the office.</p>
Risk Implications	<p>Remote working can potentially increase the risks to cybersecurity that the CHO has to address as set out below relating to:</p> <ol style="list-style-type: none"> 1. System access rights <ol style="list-style-type: none"> a. CHOs may need to widen access rights to back-office systems by enabling off-site access and potentially increase cyber risk. b. Some users may not have strong multifactor authentication. Changes in access rights may increase cyber risk 2. Personal devices used by staff (BYOD) <ol style="list-style-type: none"> a. Some staff may be allowed to use their own devices. If these are not centrally-controlled for network access and data protection, they could be vulnerable to cyber-attack. b. Data may be shared over non-secure channels 3. Phishing uncertainties <ol style="list-style-type: none"> a. In working at home, staff who are uncertain about suspicious emails may not necessarily ask what they should do or seek guidance. 4. Limitations of anti-virus software <ol style="list-style-type: none"> a. Possibility of anti-virus software failing to identify a new and aggressive type of ransomware for a remote working employee. When the employee connects to the network over the VPN, the malware spreads its infection to any shared drive, server, or PC it could reach, before attempting to extract security credentials for any Active Directory controllers.
Measures / Action	<ol style="list-style-type: none"> 1. Assess rights: ensure the access control standards set out in ISO27001 are established:

Consideration	Assessment
	<ul style="list-style-type: none">a. Segregation of duties: Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisation's assets.b. User access management: To ensure authorised user access and to prevent unauthorised access to information systems.c. User registration: There shall be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services.d. Privilege management: The allocation and use of privileges shall be restricted and controlled.e. Review of user access rights: Management shall review users' access rights at regular intervals using a formal process. <p>2. Network access controls: the ISO27001 standards for network access control (see also Section 3.1.1 below) are to prevent unauthorised access to networked services:</p> <ul style="list-style-type: none">a. User authentication for external connections: Appropriate authentication methods shall be used to control access by remote users.b. Equipment identification in networks: Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.c. Remote diagnostic and configuration port protection: Physical and logical access to diagnostic and configuration ports shall be controlled.d. Segregation in networks: Groups of information services, users, and information systems shall be segregated on networks.e. Network connection control: For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.f. Network routing control: Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.g. Change control procedures: The implementation of changes shall be controlled by the use of formal change control procedures. <p>2. Prioritise actions based on business risk scenarios.</p> <p>3. Ensure tight security controls are in place such as reviewing and testing multifactor authentication.</p>

Consideration	Assessment
	<ol style="list-style-type: none">4. Implement secure remote-working tools.5. Re-assess your security strategy to include a working from home attack.6. Ensure regular awareness of cybersecurity risks in relation to remote and home working is maintained. Focus on telling staff what to do.7. Monitor any high-risk users that you are aware of.8. Assess costs of working from home compared to the risk of BYOD.9. Adopt a zero-trust policy, assuming every device and user is a possible attack. In a report published May 2022, Gartner make the following key points on implementing a zero-trust policy:¹⁶<ol style="list-style-type: none">a. Zero trust is a security approach that explicitly identifies users and grants them just the right amount of access so that the business can operate with minimal friction while risks are reduced.b. The above point may seem like the obvious. Why shouldn't this apply as standard? Why does it merit a separate term? The term itself is a misnomer — it does not mean that <i>no-one should be trusted</i> however what it means is that no-one will be <i>implicitly</i> trusted, and that only the right trust will be granted.c. An effective zero trust strategy in a CHO means focusing on balancing the need for security combined with the need to run its operations and business. An appropriate level of protection is critical, but equally so is ensuring that employees, contractors and partners have the access they need to enable the business to succeed. It means building a structure where everyone gets all the access they need to do their job when they need it, but no more, therefore reducing possible incidents whether accidental or malicious.

3. Cybersecurity and Procurement

Implementing digital transformation initiatives also means you will be procuring software, apps and / or services at some point, which you will have determined as part of defining your IS / IT strategy, aligning your needs to business objectives as well as determining and prioritising your digital goals.

Broadly speaking, you either procure software, whether that be a fully integrated suite from one supplier or you procure a matrix of best of breed systems or applications for different types of purposes and functions, and then on top of that you may have digital apps or mobile products and apps provided by your main software supplier or you procure them individually as needed. As well as this you can procure managed services such as Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS), or you can outsource some or all of your IT services to a specialist provider and finally

¹⁶ <https://www.gartner.com/doc/reprints?id=1-2B8RGSKD&ct=220927&st=sb&submissionGuid=7c120f6a-b0c7-4472-8a8c-bb0a21588f6d>

you will procure hardware for an array of purposes, whether that be servers, smartphones, laptops, PCs etc.

A key question therefore that needs answering is where does cybersecurity fit in with your IS / IT strategy and your digital transformation planning? Do you have an IS / IT strategy and or has your experience been that you have procured something fill a gap or solve a problem and the cybersecurity implications of this procurement did not figure much in your decision to buy what you did? If it is included in your IS / IT strategy in terms of the measures you have or intend to take in relation to cybersecurity this **should** be used as part of your overall procurement and evaluation process. This should give you a good indication of what to measure and evaluate your future procurement against when it comes to cybersecurity.

When procuring technology, software and / or services, it is vitally important you undertake sufficient due diligence by setting out what you need and what you want. Cybersecurity must be a key aspect in this amongst many other aspects you need to consider when procuring technology and it cannot be easily dismissed or taken for granted. Never assume. The product or service either does it or it doesn't. It is as simple as that. It's not a case of *it can do it* or *it will do it*. So, check, clarify, get it in writing, confirm, verify.

It is therefore vitally important that in ANY procurement, you apply thorough due diligence to the process, set out your requirements and seek details on how the product should comply with relevant standards and IT guiding principles.

Consider the following:

1. What is your cybersecurity situation like now?
2. What cybersecurity policies do you have?
3. What do you need reflected / supported in whatever you are procuring?
4. Think about the security implications and what you would expect a new product or service to provide.
 - a. You need to define your functional requirements relating to security such as password management, user roles, authentication, systems access and so on
5. In addition, what do you want your supplier to provide and how will it support it?
6. Have you considered your current security configuration and how would you set out in a specification?
7. What do you need to include to ensure cybersecurity is comprehensively covered in your intended procurement?

3.1 Procurement Topics

3.1.1 Standards

The first thing you need to do is to ensure that your supplier complies with all relevant information security standards.

For all the sections in this document where related products and services are being procured, in your procurement documentation, ensure you include a section on information management standards and ask each respondent to set out how they comply.

1. ACSC Cloud Computing Security Guidelines

- a. If you are seeking a new software suite, in your procurement documentation, ask each respondent to set how they comply to the ACSC within your procurement documentation.

2. ISO27001

- a. ISO 27001 is the international standard for best-practice information security management systems.
- b. It is a rigorous and comprehensive specification for protecting and preserving your information under the principles of confidentiality, integrity, and availability.
- c. The documentation relating to ISO27001 is extensive but you need to know how your future supplier has applied its principles and standards to its products and / or its services.
- d. In your procurement documentation, ask respondents how their product complies to the standard. For example, ISO27001 covers
 - i. Network controls:
 - Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
 - ii. Security of network services:
 - Control Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

3. ISO27017

- a. ISO 27017 is an information security framework for organisations using (or considering) cloud services.
- b. Cloud service providers need to comply with this standard because it keeps their cloud service customers (and others) safer by providing a consistent and comprehensive approach to information security.

4. ISO27018

- a. ISO 27018 is a security standard part of the ISO 27000 family of standards.
- b. It was the first international standard about privacy in cloud computing services which was promoted by the industry.
- c. It was created in 2014 as an addendum to ISO 27001. It helps cloud service providers who process personally identifiable information (PII) to assess risk and implement controls for protecting.

5. ISO22301

This standard covers business continuity.

- a. It provides a systematic approach to business continuity management, and it is applicable to any organization, regardless of type, size and sector.

- b. It provides a practical framework for setting up and managing an effective business continuity management system, which aims to safeguard an organisation from a wide range of potential threats and disruptions.
- c. So, you need to know **how** your supplier can ensure **YOUR** business continuity should an incident or breach occur in relation to the service it is providing to you.
- d. Ask them how their data management infrastructure is set up

6. System and Organisation Controls 1 – Internal Control over Financial Reporting (SOC 1)

- a. Documents internal controls relevant to an audit of a user entity's financial statements.
- b. SOC1 is suited to service providers offering financial reporting services and may therefore not be specifically relevant to CHOs.

7. System and Organisation Controls 2 – Trust Services Criteria (SOC 2)

- a. Used when an organisation outsources technological and data-related services, such as data hosting, colocation, data processing and Software-as-a-Service (SaaS).
- b. Focuses on controls relating to security, availability, processing integrity, confidentiality and privacy of a service organisation's technological systems, operations and regulatory compliance. Sets out the controls needed to ensure you handle their data correctly in a wider context than just financial reporting.
- c. SOC 2 requirements govern engaged, technology-based service providers which store client information in the cloud.
- d. While ISO 27001 deals with IT security, SOC 2 is about handling third-party data, for example by a cloud computing service provider.

8. System and Organisation Controls 3 – Trust Services Criteria for General Use SOC3

- a. SOC3 is a higher-level compliance report than SOC2 and is designed to meet the needs of user entities that need specific information about certain criteria of a SOC 2 report
- b. It includes an assessment of the design and operating effectiveness of security controls and covers only a period of time and not the level of detail that a SOC 2 report entails

9. SOC Principles

- a. SOC audits help you keep track of how well you and your outsourcing provider is protecting important company and client information. The question that CHO IT managers need to sort out is which type of SOC they require.
- b. The SOC for Cybersecurity framework offers guidelines on the best ways for you to document your own cybersecurity risk management program. It also provides a number of controls and objectives that you may use to stay on track for the best possible cybersecurity.
- c. SOC reporting is a regulatory requirement for industries registered under the Australian Prudential Regulation Authority. For any other organisation, having an increased understanding of how a service provider treats information can bring many benefits as it demonstrates your control measures to pre-defined standards, giving client confidence in your organisation and ability to provide a service securely.

10. Other useful reference sources

- a. Australian Government Information Security Manual (ISM)
- b. The Information Systems Audit and Control Association is a global association that provides IT professionals with knowledge, credentials, training and community in audit, governance, risk, privacy
- c. US Department of Commerce National Institute of Standards and Technology (NIST)

3.1.2 Information Security Management

Next you need to focus on **how** each respondent has developed its product to ensure stringent data security functionality and that it has robust processes and functionality in place for information security management. In turn these are:

1. Has the supplier developed a security framework for its product based on ISO27001 and others in the ISO family?
2. For software products, a security framework typically covers:
 - a. Governance
 - b. Application Design and Architecture
 - c. Application Build Processes
 - d. Application Security Testing
 - e. Application Hosting Components
 - f. Application Hosting Operation

Based on this, what resources has the supplier used for the development of its framework – some examples are:

- a. NIST Cybersecurity Framework (CSF) and Special Publications, National Institute of Standards and Technology, [nist.gov](https://www.nist.gov)
- b. OWASP (a non-profit foundation that works to improve the security of software)
- c. ENISA, Cloud Computer Information Assurance Framework, European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework>
3. Ask whether arrangements are in place to provide assurance that hardware and software used in the delivery of the service are genuine and have not been tampered with.
4. Ask whether secure development practices incorporated into relevant product or solution development life cycles.
5. Is administrative access to the firewall and/or network edge device blocked from the internet? Best practice is to manage firewalls and routers on the edge of the network from inside the network NOT from the Internet.

3.1.3 Data Retention Policies

Seek details from your prospective suppliers covering the following

1. What is the supplier's approach to data retention, periods and archiving policies?
2. Does the product automatically archive ageing data?
3. Does the product allow you to define an archiving policy and automatically archive data to a separate SQL database?

3.1.4 Audit Certificates

Seek details from your prospective suppliers as to how often is a security audit undertaken?

3.1.5 Independent Assessments

Seek details from your prospective suppliers covering the following

1. Determine whether the supplier has undertaken an IRAP assessment (Information Security Registered Assessors Program) which reviews and confirms all aspects of the product's security framework.¹⁷
2. Include questions as to how often an IRAP assessment is undertaken and who do they use.

3.1.6 Security Monitoring

Seek details from your prospective suppliers covering the following

1. How does the supplier monitor the security of its service or product?
2. Does it run an active information security program including:
 - a. Policies and controls and processes to manage compliance.
 - b. Identification and management of information security risks.
 - c. A vulnerability management program.

3.1.7 Data Storage

Include questions as to how the prospective supplier stores your data and the controls provided to guarantee its security.

3.1.8 Patch Releases

Seek confirmation of how the prospective supplier manages patch releases of its software and the extent to which these include data security elements.

It is possible that suppliers only focus on functionality improvements to the extent that data and user security may not be a high priority.

3.1.9 Supplier Cybersecurity Risks & Capabilities

Following on from that, you then need to assess each supplier's risks and their capabilities from a cybersecurity perspective:

1. **Cybersecurity practices**
 - a. What practices has the supplier implemented to address cybersecurity and prevent data breaches?
 - b. What is the supplier's policy?
 - c. Seek assurance that an organisation's external systems are protected from unauthorised access or change and whether the supplier tests to provide further assurance that no significant weaknesses exist on the network infrastructure or individual systems that could allow one internal device to intentionally or unintentionally impact on the security of another.

¹⁷ <https://www.cyber.gov.au/acsc/view-all-content/programs/irap>

- d. Seek details on whether the supplier undertakes a hands-on assessment that covers scanning for missing patches, penetration testing, and review of firewall rules and server, PC and wireless network configurations.
 - e. Pose questions whether relevant products and solutions supplied protect all data in transit using current, proportionate and appropriate encryption products and standards?
2. **Penetration testing**
 - a. Does the supplier use independent organisations to undertake penetration testing?
 - b. When was the last time they did this and what were the results?
3. **Incident management**
 - a. What is the supplier's approach to managing incidents should one occur?
 - b. Ask whether the supplier has a disaster recovery plan that describes what would happen in the event of a serious incident impacting the availability of 'normal' IT resources. This needs to be tested to ensure it works in practice.
4. **Data location**
 - a. Where is your data to be stored?
 - b. What control will you have if your data is stored outside Australia?
 - i. It is a State Government requirement that no data is stored outside of Australia?
 - How important is this to your CHO?
 - If this is a requirement for your CHO, then state it
 - ii. Will your data be shared?
5. **Operational disruption**
 - a. Aligned to ISO22301, what will the supplier do to minimise operational disruption?
 - b. Ask them what their policies and procedures are.
 - c. Ask whether an up-to-date Business continuity plan is in place that is tested regularly.
 - d. Has this ever happened to one of their customers and what did they do to minimise the disruption?
6. **Cyber risk profile**
 - a. As part of your procurement document, you can compile a cyber risk profile which you can ask respondents to complete, from which you can assess each supplier's cyber risk.
7. **Contract / Support**
 - a. Ensure provision is made in the contract and support agreements for cybersecurity provisions – who will do what, when and how and what guarantees will the supplier provide.
 - b. Some cloud providers will usually include e.g., the standard Microsoft agreement and point you to Microsoft terms and conditions
8. **What are your minimum cyber requirements?**
 - a. Set these out so the supplier knows.

- b. If you have already defined where cybersecurity fits in with your IS / IT strategy, you should be able to set this out and ask suppliers to describe how they comply.

3.1.10 Functional Requirements

Once you have made provision for assessing cyber risk, you then need to think about specific functional requirements and be specific about what you need the product or app to do. In terms of security, consider the following:

1. Security requirements

- a. Think about functionality such as user roles and group-based security in terms of who can do and see what, access to sensitive information, link roles to portfolios or regions, locations etc, password management, password updating, administration, security monitoring
- b. Privileged user access to essential service systems should be carried out from dedicated separate accounts that are closely monitored and managed. Good practice is for their system activity to be logged or at least subject to review.

2. Authentication controls

- a. Does the system security provide for two factor authentication?
- b. Does the system synchronise the user profile and authenticate access through the network Active Directory?
- c. Is user access based on current Active Directory password and account status?
- d. Are current Microsoft Active Directory protocols supported?

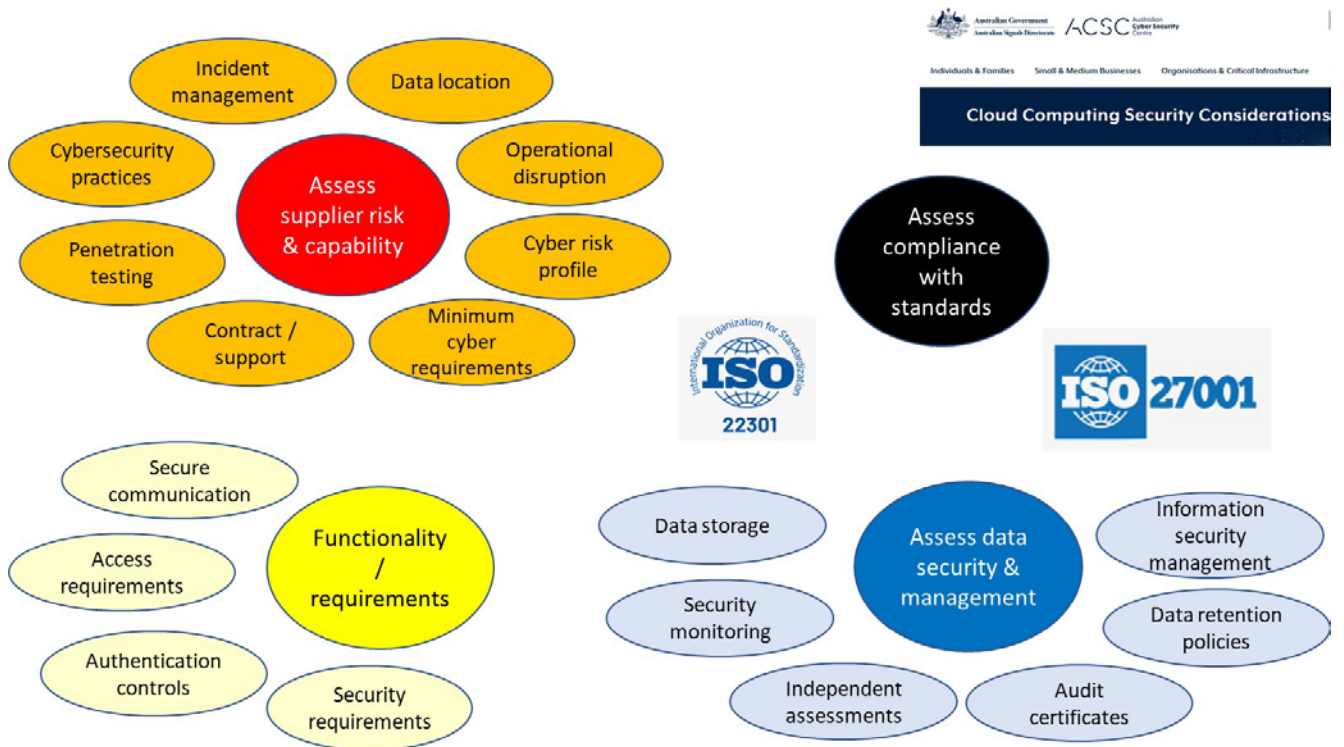
3. Access requirements

- a. Access to information assets should follow the principles of need to know and least privilege.
- b. It is good practice to establish a documented policy which details the level of access for users and groups so ask the supplier how this is provided.
- c. Systems and services should grant users only the access and functionality they require to do their job.

4. Secure communications

- a. Seek written responses on whether the product supports secure encryption, signatures and transmission of data to third party agencies and external systems.

In essence, the above form the following matrix to follow as set out below:



3.2 Key Procurement Actions

Procurement is of course a significant topic in itself. For the purposes of cybersecurity and procuring software, apps or services, the key actions you must do are:

1. Structure procurement documentation.
2. Clearly set out what you want / need.
3. Break down your functional and non-functional security requirements so that suppliers can state their level of compliance
 - a. Think about this in terms of full compliance, partial compliance, complies in next release or if any development is required.
 - b. Also seek written descriptions of HOW the supplier meets the requirements
4. Seek written answers on how the supplier provides the service and the product as well as what they do.
5. Set out questions based on the above security related topics in section 3.1 above.
 - a. Leave no stone unturned.
 - b. Make sure your questions are comprehensive.
6. Be clear on what you asking.
7. Thoroughly evaluate proposals
 - a. Set out pre-requisites
 - b. Score the responses
 - c. Analyse the levels of compliance
 - d. Identify questions
 - e. Identify shortlist for demonstrations or presentations.

8. Maintain a clarification register and seek written clarifications as these should go in the contract.
9. Assess risks, set up a risk register and identify impact, likelihood and the mitigation actions which you need to take.
10. Take up references either before or after presentations.
11. Identify a preferred supplier, ensuring the contract covers you for cybersecurity protection based on the supplier's service and the product you are procuring.

