

THC Risk Assessment

!!Mock report details do not refer to any real individual or organisation!!

H,Z

June 9, 2023

Executive Summary

This cyber security report provides an assessment of the risks to Trusted Health Care Clinic. The assessment follows the standards AS ISO 31000:2018 and AS/NZS ISO/IEC 27005:2012 to conduct a thorough and comprehensive assessment of the assets, threats and vulnerabilities present in THC's operating context. Critical to conducting an effective risk assessment is identifying THC's value creating activities along with the roles within the organisation and the assets they are responsible for. This informs an appropriate scope of risk in the form of an appetite statement to frame the clinic's goals and cautions. The assets, threats and vulnerabilities are analysed and evaluated to identify the operationally critical assets that are most at risk due to the likelihood or impact of exploitation. Post analysis, a mitigation strategy is put in place with recommendation of treatment plans to avoid, reduce, share, or retain the risk.

Contents

1	Introduction	3
1.1	Cybersecurity Risk Assessment Approach	3
1.2	THC Context Establishment	3
1.2.1	Value Creating Activities	3
1.2.2	Internal and External Context	3
1.2.3	Historical Threats	3
1.2.4	Compliance Requirements	4
1.3	Proposed Risk Appetite Statement	4
2	Assessment	5
2.1	Risk Identification	5
2.1.1	Roles and Information Assets	5
2.1.2	Information Flow	5
2.1.3	Assets Threats and Vulnerabilities	7
2.2	Risk Analysis	9
2.2.1	Critically at Risk Assets	10
2.3	Risk Evaluation	11
2.3.1	HealthCare One and CKB	11
2.3.2	Backup Facility	11
2.3.3	Business Practices	11
2.3.4	Cloud Technology	12
2.4	Risk Treatment	12

3	Recommendations	13
3.1	Awareness and Training	13
3.2	Access Control	13
3.3	Identification and Authentication	13
3.4	System and Communication Protection	13
3.5	Incident Response	13
3.6	Maintenance	14
3.7	Physical and Environmental Security	14
A	Risk Definitions	15
A.1	Appetite Definition and Tolerance	15
	A.1.1 Preventative	15
	A.1.2 Conditional	15
	A.1.3 Encouraged	15
A.2	Impact Levels	15
A.3	Likelihood Levels	16
A.4	Risk Levels	16
B	Asset Lists	16
B.1	Assets By Category	16
B.2	Weighted Factor Analysis	18
B.3	ATV	18

1 Introduction

1.1 Cybersecurity Risk Assessment Approach

The following risk management procedures aim to identify, evaluate and mitigate current security threats to the THC organisation and its operationally critical information assets. The risk assessment primarily will be conducted utilising the AS ISO 3100:2018 standards and the AS/NZS ISO/IEC 27005:2012 standards and to a lesser degree the NIST 800-30 r1.

In accordance with these frameworks, THC's critical information assets, organisational roles, responsibilities and stakeholders will be identified, to produce a relevant and updated situational awareness of THC's external and internal context. Following this, the organisation's information assets, threats and vulnerabilities can be catalogued and prioritised (*ISO 31000:2018 Risk management — Guidelines Ed. 2* 2018). With a complete understanding of the security landscape, risk treatment decisions can be made to avoid, share or retain the risks (Information technology - Security techniques - Information security risk management (*Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2012, MOD)* 2012).

The following findings should be adopted by executive management to ensure distribution of policies, with clear lines of communication established to ensure adaptive and continual risk management procedures (*ISO 31000:2018 Risk management — Guidelines Ed. 2* 2018).

1.2 THC Context Establishment

1.2.1 Value Creating Activities

THC has found its niche in providing efficient tele-health services. This is enabled through the use of the clinical knowledge base which uses proprietary algorithms to provide resolutions to callers. It is THC's high capacity of providing services that drives the success of business operations. Thus the protection, use and expansion of the CKB, along with the systems that support its function are paramount to business continuity.

1.2.2 Internal and External Context

Management of medical supplies, human resources, and the information systems, such as the CKB, Healthcare One and the Web server are conducted in-house. These components form the internal context of THC. THC also maintains multiple business relations, to ensure the quality of their services. Allied Health Professionals are granted access to THC systems to facilitate the communication of necessary patient details and thus provide specialist care. Furthermore, THC uses a specialist backup company to provide redundancy of clinic data. There are also proposals for the use of cloud services to manage HR and acquisitions. These elements form the external context of THC. The clinic must also integrate with HICAPS and Medicare for patient insurance and government healthcare systems.

1.2.3 Historical Threats

There are a variety of threats the THC has already encountered, as of yet none have resulted in a data breach. THC receives up to 8000 calls a year, recently many have been Covid related scams. Furthermore, a spear phishing campaign was targeted at the practice manager aiming to intercept credentials to access patient data. Recent weather forecasts predict a severe flood

warning which could affect the availability of THC's services. To combat downtime THC has already invested in creating backups of their critical data, and networked services.

1.2.4 Compliance Requirements





As a clinic THC needs to meet compliance requirements for healthcare information systems and the Australian privacy principles. The privacy principles dictate the responsibilities of handling private data, ensuring it is up to date and correct, that the collection is disclosed and that use cases are given with permission. Furthermore, it is important that data is anonymized when required. This ensures the security of personally identifiable information (Australian Information Commissioner 2022). There are additional compliance requirements for healthcare systems so that critical patient information is available to clinicians and that the records are accurate to support quality of care. The record keeping should comply with privacy principles and regular audits are mandated (NSQHS 2014).

Through the identification of the security context and business goals the following mission statement is proposed under section 1.3

1.3 Proposed Risk Appetite Statement

THC's first priority is to provide quality care to its patients, and ensure full compliance with privacy principles. Our aim is to improve our services through innovation and technological integration which will result in better patient outcomes and faster resolutions. Below (Table 1) we highlight our primary goals and the associated willingness of controlled risk.

Table 1: Risk Appetite by Objective

	Preventative	Conditional	Encouraged
Patient Data			
THC Service			
Compliance			
Innovation			

As seen in Table 1, we will not concede risks related to compliance obligations. Our patients should have confidence that their data is being handled according to best practice. However in the pursuit of research, innovation and utilising technology to enhance our practice there is a much greater acceptance of risk.

For definitions of the risk appetite and the associated risk tolerances see appendix A.1

2 Assessment

2.1 Risk Identification

2.1.1 Roles and Information Assets

Roles were identified at THC and their responsibilities over the information assets have been associated in Table 2. A variety of information assets have been found to not currently be maintained by the roles at THC. Furthermore, there are a few assets relating to CKB and HealthCare One that are handled by multiple roles without a proper hierarchy of management.

A complete list of information assets can be found in Appendix B.1 along with a weighted factor analysis in Appendix B.2 to identify the top 7 operationally critical assets. These analysis considers the assets relation to revenue, compliance obligations, reputation, and whether the assets are actively being maintained.

2.1.2 Information Flow

An identification of the handling, processing and storage of information assets are illustrated in Figure 1.

Table 2: Organisational Roles and Assets

Role (Held By)	Responsibility	Information Assets
Managing Director/ Executive Staff (Brad Hill, Angelique Farelli)	Policy Creation and Approval Risk Management Incident Response Compliance and Regulation	Internal Staff Allied Health Professionals ^{1,2} Contractor Procedures ^{1,2} IR Procedures ^{1,2} RM Procedures ^{1,2} Information Management- Procedures ² All Data ^{1,2} Audit Reports
Practice Manager (Susan Brown)	Clinic Processes Patient Information Handling	Internal Staff Patient Medical Data Patient Personal Data ² Staff Data ² Allied Health Professionals- Data Call Records
Accounts Manager (Colleen Hayes)	Clinic Finances Business Information Handling	Staff Data ² Supply Lists ² Financial Data
Accounts Reconciliation Officer (³ Sally Brent, Vacant)	Ordering critical supplies Depositing finances	Supply Lists Suppliers
Continued on next page		

Table 2: Organisational Roles and Assets *Continued*

Role (Held By)	Responsibility	Information Assets
HR Manager (Rebecca Adams)	Human Resources Payroll	Staff Data Internal Staff Allied Health Professionals- Data Allied Health Professionals
Health Informations System Specialist (Felix South)	Maintenance of the healthcare systems Compliancy of systems	HealthCare One HealthCare One (Data Store) CKB CKB (Data Store) HealthCare One (Documentation) CKB (Documentation) Backup in locked case
Software Developer (Felix Sout, Jock Jordan)	Developing applications and systems	HealthCare One (Code) ¹ HealthCare One (Documentation) ¹ CKB (Code) ¹ CKB (Documentation)
Nurses (On Call) (Filled)	Resolving patient calls using CKB.	CKB HealthCare One Patient Medical Data
Allied Health Professionals (Filled)	Providing Specialist Care	CKB HealthCare One Patient Medical Data
General Administrators (Filled)	Handling patient intake Day-to-Day Administrative Tasks	HealthCare One Patient Personal Data
Independent Auditor (Vacant)	Conducting Audits of Health Care Systems and Procedures	¹ Audit Reports
Cybersecurity Specialist (Jock Jordan)	Handling Incident Response and Risk Management Procedures	¹ IR Procedures ¹ RM Procedures ¹ Information Management- Procedures

¹The info asset is not currently being actively managed or maintained by the role²The role is ultimately responsible for the asset, but its handling is delegated to another role (Peltier 2004).³The individual previously held the position.

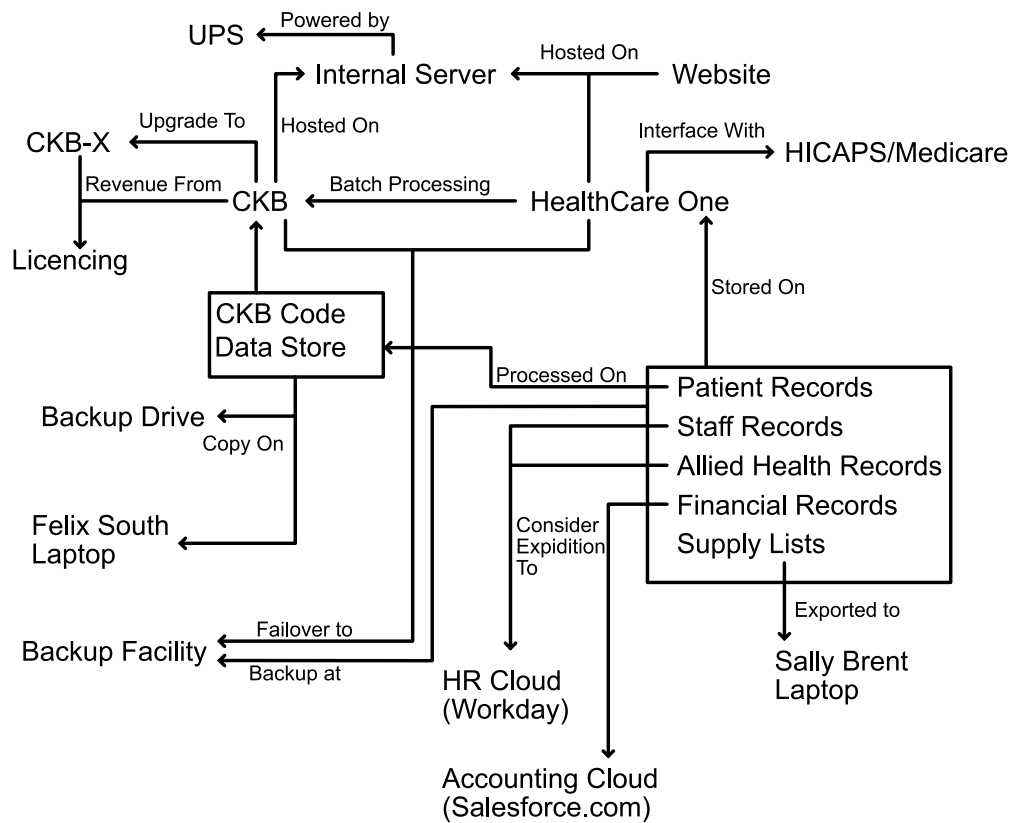


Figure 1: Flow of information in THC

2.1.3 Assets Threats and Vulnerabilities

The top operationally critical assets were identified as follows: CKB, HealthCare One, Patient Data; both medical and personal, Allied Health Professional Data, Patient Call-records, Supply Lists and Staff Data. Some of these have sub components to the assets which were analysed based on differing threats and vulnerabilities outlined in Table 3. A complete ATV table of all assets can be found in Appendix B.3

Table 3: Operationally Critical ATV

Index	Asset	Threat	Vulnerability
0	CKB (Applica- tion)	Deviation in QoS	Backup facility untested and lo- cal to region
1	CKB (Data)	Espionage	Single Privilege Access
2		Information Extortion	Stored on personal laptop
3		Software Attacks	Accessible through internet
4	CKB (Code)	Compromises of IP	Stored on personal laptop
5	CKB (Server)	Forces of Nature	Backup facility untested and lo- cal to region
6	HealthCare One (Application)	Deviation in QoS	Backup facility untested and local to region Improper development of quick fixes and patches
7		Technological Obsoles- cence	Improper development of quick fixes and patches Single qualified technician
8	HealthCare One (Data)	Espionage	Single Privilege Access
9		Information extortion	Accessible through internet
10		Software Attacks	Lack of training
11	HealthCare One (Server)	Software and Hardware failures	Improper development of quick fixes and patches Documentation not maintained
12		Forces of Nature	Backup facility untested
13	Patient Data (Personal and Medical)	Espionage	Single Privilege Access
14		Information Extortion	Accessible through internet
15		Sabotage	Information is transmitted as batch process
16		Human Error	Lack of Training on systems
17	Allied Health Pro- fessional Data	Theft	Single Privilege Access Accessible through internet
18	Patient Records	Call- Theft	Single Privilege Access Accessible through internet No staff security training
19	Supply lists	Sabotage	CSV copy on unsecure laptop Single Privilege Access Accessible through internet
20	Staff Data	Theft	Single Privilege Access Accessible through internet Lack of training about phishing

2.2 Risk Analysis

The risk analysis in Table 4 first identifies the likelihood of the threat exploiting the asset, and the impact of the data loss if the threat compromises the asset. This is informed from the previously identified vulnerabilities, and the weighted factor analysis in the Appendix B.2. For definitions of the likelihood and impact scales, as well as quantitative values used in the risk table see Appendix A.3 and A.2.

Table 4: Likelihood Impact Rating

Index	Impact	Likelihood	Risk Rating	Justification
0	Minor (2)	Probable (3)	6	Issues with the application will only result in less efficient resolutions. Nurses should still be able to come to decisions for callers. There was an attack on the web server which led to 4.5 hr outage, could occur to healthCare One
1	Severe (5)	Likely (4)	20	Compliance issues and data breach, reputation damage. Stored on personal unsecured laptop
2	Severe (5)	Probable (3)	15	Compliance issues, Data breach and financial loss.
3	Severe (5)	Probable(3)	15	Allow for pivoting to compromise the data, and other assets.
4	Severe (5)	Likely (4)	20	This may affect the ongoing licensing discussion resulting in significant losses. Stored on personal unsecured laptop.
5	Major (4)	Unlikely (2)	8	A flood may result in long term outages for the CKB server,as the backup facility is local. While there have been weather event warnings severe events wouldn't be too frequent.
6	Moderate (3)	Probable (3)	9	This will mean that all sectors of the clinic will be less effective at their tasks. There was an attack on the web server which led to 4.5 hr outage, could occur to healthCare One.
7	Minor (2)	Probable (3)	6	The documentation isn't maintained and thus it's built on rushed patches.
8	Severe (5)	Likely (4)	20	Compliance issues and data breach, reputation damage.
9	Severe (5)	Likely (4)	20	Compliance issues, data breach and financial loss.

Continue on next page

Table 4: Likelihood Impact Rating *Continued*

Index	Impact	Likelihood	Risk Rating	Justification
10	Severe (5)	Likely (4)	20	Software attacks of the application could allow for pivoting to compromise the data, and other assets.
11	Moderate (3)	Rare (1)	3	Backups are already installed
12	Major (4)	Unlikely (2)	8	A flood may result in long term outages of HealthCare One, and the backup facility is local. While there have been weather event warnings severe events wouldn't be too frequent.
13	Major (4)	Probable (3)	12	Compliance issues and data breach, reputation damage.
14	Major (4)	Likely (4)	16	Compliance issues, data breach and financial loss.
15	Severe (5)	Rare (1)	5	This could affect treatment of patients, leading to fatalities if the medical data is tampered with.
16	Moderate (3)	Unlikely (2)	6	Staff aren't effectively trained on the systems; there may be minor errors to do with managing records.
17	Moderate (3)	Likely (4)	12	CSV stored on unsecure laptop
18	Major (4)	Probable (3)	12	Unable to determine supplies and may lead to shortages.
19	Major (4)	Often(5)	20	Business deals could be disrupted leading to financial loss. Supply lists on a lost laptop and useful for phishing attacks through pretending to be a supplier.
20	Severe (5)	Often (5)	25	Lack of security training of staff leading to theft. Clinic receives 8000 calls a year, some of which have been Covid scams. If credentials are stolen it will compromise other assets.

2.2.1 Critically at Risk Assets

Each asset has multiple threats and vulnerabilities, Table 5 prioritises the assets based on the highest risk, threat and vulnerability tuple for each asset. This summarises the critically at risk assets. Definitions for the risk categories are in Appendix A.4.

Table 5: Risk Prioritisation Matrix

Likelihood			Allied Health Data	Supply Lists Patient Data	Staff Data CKB(Data) CKB(Code) Healthcare One(Data)
		CKB (Application)	Healthcare One (Application!50)	Patient Call Records	
				CKB(Server) Healthcare-One(Server)	
	Impact				

2.3 Risk Evaluation

The risks identified are discussed further to identify underlying causes and the relationship between the risks. Thus this provides insight into the possible solutions for creating an effective and efficient risk mitigation strategy.

2.3.1 HealthCare One and CKB

HealthCare One is a single point of failure for the company, as it stores all financial data, patient data, records and supply lists. It sits around the high risk mark. This is because every user has full privileges to all functions of HealthCare One. Furthermore, it is accessible through the internet to allow for allied health services to update records on the system. Both CKB and HealthCare One are at risk of significant data loss, due to datastores being replicated on unsecured laptops, and a lack of a remote backup service as discussed in 2.3.2

2.3.2 Backup Facility

The backup facility is to mitigate some risks related to downtime of servers and data loss as it provides failover services and data store replication of the HealthCare One and CKB services. However, the backup facility is local to the region, thus it does not mitigate the risks present from flooding of the area.

2.3.3 Business Practices

Many employees seem to desire the ability to work remotely. This is currently being enacted through allowance from management for individuals to download copies of the financial and service data onto personal laptops, this exposes these datasets to easy theft and espionage. Thus the patient and staff records sit at the high and critical risk level respectively. Additionally, compromise of staff credentials would lead to unauthorised access of all systems due to the single privilege access of healthcare one.

2.3.4 Cloud Technology

Workday and Salesforce are two cloud software providers that have been considered to manage the HR and Business records. These companies will often store data outside of Australian jurisdiction (*Privacy Statement — Workday* 2023), (*Privacy Policy — Salesforce* 2023). However, THC is still ultimately responsible for the data under the Australian Privacy Principles (ADHA 2021). This means there may be reparations to THC, for mishandling of data by the cloud service provider. This could present a higher degree of risk if the data is stored in a jurisdiction with weaker security laws.

2.4 Risk Treatment

The following lists the category of control based on NIST 300-80 (Joint-Task-Force-Transformation-Initiative 2012). The controls are explained in Section 3

Table 6: Mitigation Strategies

Index	Strategy	Control Category
0	Reduce	Physical and Environmental Security
1	Avoid	Access Control, Identification and Authentication
2	Avoid	Awareness and Training
3	Avoid	Access Control, System and Communication Protection
4	Avoid	Awareness and Training, System and Communication Protection
5	Reduce	Physical and Environmental Security
6	Reduce	Physical and Environmental Security
7	Avoid	Maintenance
8	Avoid	Access Control, Identification and Authentication
9	Avoid	Awareness Training, System and Communication Protection
10	Avoid	Access Control, System and Communication Protection
11	Avoid	Maintenance
12	Reduce	Physical and Environmental Security
13	Avoid	Access Control, System and Communication Protection
14	Avoid	Awareness and Training, System and Communication Protection
15	Share	Incident Response (Insurance)
16	Avoid	Awareness and Training
17	Avoid	Access Control, System and Communication Protection
18	Avoid	Access Control, System and Communication Protection
19	Avoid	Awareness and Training, System and Communication Protection
20	Avoid	Identification and Authentication, System and Communication Protection
21	Avoid	Awareness and Training

3 Recommendations

3.1 Awareness and Training

The staff of THC should be properly trained with regard to the following issues:

1. Identification of phishing attempts, this will reduce compromise of systems, from viruses in email attachments and phishing calls attempting to get sensitive details.
2. Appropriate use of business data. There should be policies to prevent the use and storage of data on personal devices such as downloading CSV exports or documentation, code and data stores.
3. Staff should be appropriately trained in systems relevant to their area of employment. Proper policy regarding induction and staff training should be formalised.

3.2 Access Control

- The critical systems of THC including Healthcare One and CKB and its network should be appropriately segregated.
- Users should only have access to the critical functions required to efficiently complete their job requirements.
- Network access control should be implemented in the form of a firewall which only allows known allied health services to connect to THC services.

3.3 Identification and Authentication

Along with access control it is a requirement that users should have strong passwords to reduce the effectiveness of password cracking attempts. Furthermore, for the IT users there should be separate administrator and low privilege accounts. IT staff should use a regular low privilege account for day to day work on CKB and Healthcare One, only logging into the administrator accounts when necessary.

3.4 System and Communication Protection

It is apparent that there is a desire to be able to work remotely from THC as evident through the amount of data being exfiltrated to personal devices. Thus it is recommended that THC implement a VPN service to allow secure access to the internal resources. This also would secure the allied health professionals access to HealthCare One which is required.

Additionally an anti-malware and intrusion prevention system should be installed to identify and inhibit the effectiveness of software, malware and network attacks. Encryption of data in storage should also be considered to increase the cost of espionage.

3.5 Incident Response

There should be formalised plans by the head security officer, to respond to incidents if they do occur. In this plan there should be purchase of an insurance policy in the event of significant fines for data loss, particularly if a cloud management provider has been used, of which THC would ultimately be responsible for the data managed.

3.6 Maintenance

A proper policy regarding patching and updates should be established to ensure that changes made to the HealthCare One and CKB system are well documented and timely, to limit the vulnerability window.

3.7 Physical and Environmental Security

The use of a UPS and Backup service provider is beneficial as it provides redundancy and failover services. However currently the backup facility is local to the region and thus subject to flooding in the same weather event as THC. Thus there should be investment into backup solutions that are not local to the region. There should also be consideration of cold backups that are stored completely offline to limit the possibility of ransomware attacks on the backups.

References

- Peltier, Thomas R. (Sept. 2004). "Risk Analysis and Risk Management". In: *Information Systems Security* 13, pp. 44–56. DOI: 10.1201/1086/44640.13.4.20040901/83732.7.
- Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2012, MOD)* (2012).
- Joint-Task-Force-Transformation-Initiative (Sept. 2012). *NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments*. URL: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final> (visited on 04/05/2023).
- NSQHS (2014). *Action 1.16 — Australian Commission on Safety and Quality in Health Care*. Safetyandquality.gov.au. URL: <https://www.safetyandquality.gov.au/standards/nsqhs-standards/clinical-governance-standard/patient-safety-and-quality-systems/action-116> (visited on 03/22/2023).
- ISO 31000:2018 Risk management — Guidelines Ed. 2* (Feb. 2018).
- Whitman, Michael E and Herbert J Mattford (2019). *Management of information security*. 6th ed. Cengage Learning.
- ADHA (Oct. 2021). *CLOUD SERVICES Considerations for healthcare organisations A guide for healthcare providers*. URL: https://www.digitalhealth.gov.au/sites/default/files/2020-11/Cloud_services-Considerations_for_healthcare_organisations.pdf.
- Australian Information Commissioner, Office of the (2022). *Australian Privacy Principles quick reference*. OAIC. URL: <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference> (visited on 03/22/2023).
- Privacy Policy — Salesforce* (2023). Salesforce. URL: <https://www.salesforce.com/au/company/privacy/> (visited on 04/05/2023).
- Privacy Statement — Workday* (2023). www.workday.com. URL: <https://www.workday.com/en-gb/privacy.html> (visited on 04/05/2023).

A Risk Definitions

A.1 Appetite Definition and Tolerance

A.1.1 Preventative

■ Preventative represent zero tolerance for risk. This objective is critical to business continuity and thus must be managed with priority. The tolerances are as follows:

- 0% data loss of information assets
- >90% compliance
- Identification of non-compliance should be resolved in the period of 1 week

A.1.2 Conditional

■ A conditional appetite represents a cautious attitude to taking on risk. The pursuit of business goals should allow for some risk without compromising the preventative appetite. The tolerances are as follows:

- <5 minute wait for THC call in service
- Resolutions should be found within 15 minute consultation
- <1 hour downtime of IT services each quarter

A.1.3 Encouraged

■ Encouraged attitude is a willingness to take on higher degrees of risk in the attainment of business objectives. The tolerances are as follows:

- Minimum risk options should be favoured
- Higher degrees of risk accepted based on incremental improvements of 20% of predicted business gain

A.2 Impact Levels

Severe (5): This would result in immediate shutdown of clinic and/or legal repercussions and/or national reputation damage and/or >1,000,000 loss in revenue

Major (4): This would result in temporary shutdown of clinic and/or significant fines and/or minor reputation damage and/or <1,000,000 loss in revenue

Moderate (3): This would result in temporary disruption to services and/or minor reputation damage and/or <500,000 loss in revenue

Minor (2): This would result in temporary reduce in quality of services and/or individual reputation damage and/or <10,000 loss in revenue

Insignificant (1): This would result in negligible reduction in quality of service and/or negligible loss in revenue.

A.3 Likelihood Levels

Often (5): Occurs on a monthly basis

Likely (4): Occurs on a quarterly basis

Probable(3): Occurs on a yearly basis

Unlikely (2): Occurs on a 2-yearly basis

Rare (1): Occurs on a 5-yearly basis

A.4 Risk Levels

Critical (21-25): At least Avoid or Reduce

High (15-20): At Least Avoid or Reduce

Medium (8-14): At Least Reduce or Share

Low (4-7): At Least Share or Retain

Trivial (1-3): At Least Retain

B Asset Lists

B.1 Assets By Category

Table 7 is a descriptive lists of the information assets of value to THC. These are organised by the categories identified by Whitman and Mattford 2019

Table 7: Information Assets By Category

Category	Asset	Description
People	Internal Staff	Know-how of systems (suppliers, healthcare one maintenance, CKB development)
	Allied Health Professionals	Access HealthCare One and CKB
	Backup Facility Contractors	Backup CKB and HealthCare One Data Store
	Suppliers	Suppliers that provide critical medical resources.
Procedures	CKB	Documentation Stored on personal Laptop
	Health Care One Documentation	Unmaintained
	Audit Reports	Missing or not conducted
Procedures	Contractor Procedures	Decision making for which suppliers, service providers to contract

Continued on next page

Table 7: Information Assets By Category *Continued*

Category	Asset	Description
Data	Internal Information Management Procedures	Internal communication and access to systems like HealthCare One and the CKB
	IR Procedures	Procedures and policy documents for incident response
	RM Procedures	Procedures and policy documents for risk management
	Patient Call-Records	Stored on HealthCare One (searchable database), Phone number, Transcript, Decision Reached
	CKB Data Store	Stored on Internal Server and laptop and locked drive. Update through batch process form Healthcare one
	Patient Medical Data	Social welfare history, Health risk factors, Allergies, Medication, visitations
	Patient Personal Data	Demographic information, Payment methods (auto), Rebate info via HICAPS/Medicare
	Allied Health Professional Data	Stored on HealthCare One, Demographic information, Qualification, Areas of specialisation
	Staff Data	Stored on HealthCare One. Consideration for Cloud-Based Workday. Roster, Payroll Details, Address and Contact
	Financial Data	Includes payroll info, clinic revenue and profit. Subscription, invoices, bills, quotes.
Software	Supply Lists	Stored on HealthCare One. Consideration for Cloud-based Salesforce.com. CSV of data on personal laptop
	CKB (Application)	Efficient Tele-health Resolution Run on Internal Server, Expansion plans for AI integration
	CKB (Code)	Stored on Personal Laptop. Backup on hard drive in locked file cabinet.
	Healthcare One (Application)	Management of Patient Details, Staff Details, Alerts, HR, Supply
Hardware	Business Applications	Microsoft Office, etc
	Internal CKB Server	Hosts CKB
	Web Server	Hosts webpage
	UPS	Supplies Internal servers
Hardware	Backup Facility	Provided by specialist company

Continued on next page

Table 7: Information Assets By Category *Continued*

Category	Asset	Description
Networking	Failover Hardware	Provided by specialist company
	Backup Drive	Locked in case, contains backup of CKB
	HealthcareOne (patient communication)	Alerts generated to patients regarding appointments. Follow up reminders, Patient scheduling
	HealthCareOne (allied communication)	Messages and Access for Allied Health Professionals to patient information. Active prescriptions, Electronic referrals, Patient reports
	HealthcareOne & CKB Batch Processing	Data stores in transit from HealthcareOne to CKB. Patient history, Previous treatment, Phone-ins, Disease and drug interaction, Care directions
	WiFi and Mobile Network	Provide communication to CKB for Allied Health Professionals, Provide CKB Data Store, HealthCareOne Data Transmission to Backup facility

B.2 Weighted Factor Analysis

A weighted factor analysis was used to determine the operationally critical information assets (Whitman and Mattford 2019). The key factors were identified as being: compliance, reputation, revenue, and whether the asset was currently being maintained. The results are shown in Table 8

B.3 ATV

A complete list of Assets, Threats and Vulnerabilities can be found in Table 9.

Table 8: WFA

	Compliance Obligations	Reputation	Revenue	Active Maintenance	Importance
<i>Weights</i>	<i>50</i>	<i>20</i>	<i>20</i>	<i>10</i>	<i>100</i>
Internal Staff	0.4	0.6	0.3	0.0	37
Allied Health Professionals	0.4	0.7	0.3	0.0	40
Backup Facility Contractors	0.5	0.2	0.2	0.1	34
Suppliers	0.6	0.2	0.2	0.4	42
CKB Documentation	0.2	0.1	0.1	0.2	16
Health Care One Documentation	0.2	0.1	0.1	0.8	22
⁴ Audit Reports	1.0	0.4	0.1	0.8	68
⁴ Contractor Procedures	0.1	0.2	0.4	1.0	27
⁴ Internal Information Management Procedures	0.7	0.3	0.1	1.0	54
⁴ IR Procedures	0.5	0.5	0.3	1.0	51
⁴ RM Procedures	0.5	0.5	0.3	1.0	51
Patient Call-Records	1.0	0.5	0.3	0.2	68
CKB (Data, Server, Application, Comms)	1.0	0.9	0.9	0.6	92
Patient medical Data	1.0	0.9	0.4	0.1	77
Allied Health Professional Data	0.9	0.9	0.4	0.1	72
Staff Data	0.7	0.5	0.4	0.1	54
Financial Data	0.5	0.4	0.8	0.1	50
Supply Lists	0.7	0.4	0.8	0.7	66
Healthcare One (Data, Application, Comms)	1.0	0.8	0.8	0.8	89
Web Server	0.3	0.7	0.7	0.2	45
UPS	0.1	0.1	0.4	0.1	16
Backup Facility	0.6	0.3	0.4	0.1	45
Failover Hardware	0.2	0.1	0.4	0.1	21
WiFi and Mobile Network	0.4	0.2	0.3	0.1	31

⁴Currently non-existent

Table 9: Full ATV Table

Asset	Threat	Vulnerability
Internal Staff	Poaching Human Error Insider Threat	Lack of Policies Lack of Training on systems
Allied Health Professionals	Poaching Human Error Insider Threat	Lack of Policies Lack of Training on systems
Backup Facility Contractors	Human Error Insider Threat	Lack of contractor Policies Lack of incident response policies
Suppliers	Espionage Sabotage	Lack of contractor Policies
CKB Documentation	Compromises of IP Theft and Espionage	Stored on personal laptop
Health Care One Documen- tation	Compromises of IP Theft and Espionage Technological Obsolescence	Stored on personal laptop Not actively maintained
Patient Call-Records	Theft or Espionage	Single Privilege Access Information is transmitted as batch process from Healthcare One to CKB
CKB (Data Store, Applica- tion, Server)	Espionage Compromises of IP Information extortion Software Attacks	Single Privilege Access Data Store, Code stored on personal laptop Accessible from internet
Deviation in QoS	Forces of Nature	Backup facility untested and local to region
Patient Medical Data	Espionage Information Extortion Sabotage	Single Privilege Access Exposed to internet Information is transmitted as batch process from Healthcare One to CKB
	Human Error	Lack of Training on systems
Patient Personal Data	Theft Information Extortion Sabotage	Single Privilege Access Exposed to internet Information is transmitted as batch process from Healthcare One to CKB
	Human Error	Lack of Training on systems

Continued on next page

Table 9: Full ATV Table *Continued*

Asset	Threat	Vulnerability
Patient Call Records	Theft Phishing Sabotage	Single Privilege Access Exposed to internet
Allied Health Professional Data	Theft or Espionage Sabotage	Single Privilege Access Exposed to internet
Staff Data	Theft or Espionage Sabotage	Single Privilege Access Exposed to internet
Financial Data	Theft or Espionage Sabotage Information extortion	Single Privilege Access Exposed to internet
Supply Lists	Theft or Espionage Information Extortion	Single Privilege Access Exposed to internet
Healthcare One (Data Store, Application)	Espionage Compromises of IP Information extortion Software Attacks	Single Privilege Access Exposed to internet Single qualified technician
	Deviation in QoS Forces of Nature	Backup facility untested and local to region
	Technological Obsolescence	Software and Hardware failures Improper development of quick fixes and patches Documentation not maintained
Web Server	Software/Hardware Failures Forces of nature Deviation in QoS	Backup facility untested and local to region
	Vandalism Software attacks	All users have privilege
Backup Facility	Espionage Information extortion Human error	Lack of contractor procedures
Business Applications	Software Attacks	Security configurations around macros etc.