ABISHEK BALAKRISHNAN SELVAM

Swinburne University of Technology

Risk Assessment Report

Contents

[Executive Summary 0](#_Toc11838753)

[1.0. Introduction 1](#_Toc11838754)

[2.0. Scope 1](#_Toc11838755)

[2.1. System Characterization 2](#_Toc11838756)

[2.2. Risk Assessments Approach 2](#_Toc11838757)

[2.3. Assumptions 3](#_Toc11838758)

[3.0. Risk Assessments 3](#_Toc11838759)

[3.1. Threat Identification 3](#_Toc11838760)

[3.2. Vulnerability Identification 6](#_Toc11838761)

[3.3. Control Analysis 8](#_Toc11838762)

[3.4. Likelihood, Impact and Risk Determination 9](#_Toc11838763)

[3.4.1. Likelihood 9](#_Toc11838764)

[3.4.2. Impact 9](#_Toc11838765)

[3.4.3. Risk Determination 9](#_Toc11838766)

[3.5. Risk Priority 9](#_Toc11838767)

[4.0. Risk Mitigation 12](#_Toc11838768)

[4.1. Feasibility and Effectiveness Control and Cost-Benefit Analysis 13](#_Toc11838769)

[4.2. Controls Implementation 13](#_Toc11838770)

[4.3. Residual Risk Statement 13](#_Toc11838771)

[5.0. Conclusion 14](#_Toc11838772)

[References 15](#_Toc11838773)

[Appendices 20](#_Toc11838774)

[Appendix A Scope 20](#_Toc11838775)

[Table A.1. System Characterization 20](#_Toc11838776)

[Appendix B Threat Identification 23](#_Toc11838777)

[Table B.1. Identification of Adversarial Threat Sources and Events 23](#_Toc11838778)

[Appendix C 30](#_Toc11838779)

[Table C.1. Assessment Scale – Vulnerability Severity 30](#_Toc11838780)

[Table C.2. Identification of Vulnerabilities 30](#_Toc11838781)

[Appendix D 32](#_Toc11838782)

[Table D.1. Existing Controls 32](#_Toc11838783)

[Appendix E Likelihood, Impact and Risk Determination 35](#_Toc11838784)

[Table E. 1. Assessment Scale - Likelihood of Threat Event Initiation (Adversarial) 35](#_Toc11838785)

[Table E.2. Assessment Scale - Likelihood of Threat Event Occurrence (Non-Adversarial) 35](#_Toc11838786)

[Table E.3. Assessment Scale - Likelihood of Threat Event Resulting in Adverse Impacts 35](#_Toc11838787)

[Table E.4. Assessment Scale - Overall Likelihood 36](#_Toc11838788)

[Table E.6. Assessment Scale - Impact of Threat Events 36](#_Toc11838789)

[Table E.7. Assessment Scale - Level of Risk (Combination of Likelihood and Impact) 37](#_Toc11838790)

[Table E.8. Assessment Scale - Level of Risk 37](#_Toc11838791)

[Table E.9. Identification of Level of Risk 38](#_Toc11838792)

[Appendix F Control Implementation 58](#_Toc11838793)

# Executive Summary

The innovation and growth of Banksia Pathology increases the connectivity, complexity and dependency of the internal and external systems that process and records a vast amount of sensitive medical and organizational data. Without proper risk management, threats exploit weaknesses associated with current and future operations, which may result in negative impacts to the organization.

All IS/IT related threats, vulnerabilities, likelihood and impacts will be identified and assess, to determine risks and prioritize the four major risks that the organization is facing. These risks are risk in disruption of service and cyberattacks running business functions using legacy systems, risk of cyberattacks due to lack of information security control and initiatives, risk of non-compliance due to limited governance and monitoring activities on third-party, and risk in facility closure due to non-compliance.

The purpose of this report is to provide a framework for management in identifying, assessing and mitigating risks associated with current and future operations of Banksia, with the emphasize on the four major risks. As part of the risk mitigation process, a list of appropriate controls is identified in the effort to reduce or eliminate the four major risks. Peer-reviewed and industry references are used to support the argument of the risk management efforts.

# Introduction

The growth of Banksia is a representative of a complex modern healthcare where technology, human risk factors, geographical scope and scope of service are interconnected and sometimes inseparable (van Deursen et al 2013, p. 31). During the expansion, employees are becoming more mobile, more business functions are outsourced to local and international third parties, and data is moving through more interconnected networks. These shifts create unclear organization boundaries.

As Banksia progressively traverses through rapidly expanding business transformations, major concern revolves around its information technology and security initiatives (Prananto 2019, Safa et al. 2018, p. 248). When threat sources exploit weaknesses of the organizational information systems, it may cause negative consequences that hinders or ends future growth of the company. This phenomenon is classified as risk. Risks materialize when a group of threat events takes advantage of one or more vulnerabilities (National Institute of Standard and Technology (NIST) 2012, p. 10). For example, while cloud-based portals increase flexibility in accessing data, they also increase information security risks as they are exposed to the cloud environment which is vulnerable to cyberattacks. However, cyber risk is not the only risk associated from IT implementation and usage that management should be concerned about.

The goal of risk management to protect the organization and its ability to perform its mission by identification, assessments and mitigation of risks where possible (Prananto 2019). This Information Systems/Information Technology (IS/IT) risk management report will start by risk assessments procedure that assess, analyses and identifies threat events and sources, vulnerabilities, likelihood of occurrence and adverse impacts, and highlights the most critical risks faced by Banksia which call for a strategic management approach in risk mitigation. The report continues with recommended risk mitigation strategies including suggested controls, cost-benefit analysis and implementation of controls.

# Scope

This section defines the scope of the risk management effort to create this report.

## System Characterization

The scope of the assessment focuses on the resources, information, boundaries, and controls that constitute the system. It includes any internal and external personnel, entities, processes and activities that affects IS/IT systems of Banksia. It includes, but not limited to, partnerships with other medical organizations, patients, third-party vendors, systems used, internal business processes, lab facilities, data between the entities and government agencies (See Appendix A Table A.1.).

## Risk Assessments Approach

The approach taken in conducting the risk assessments adapts the Special Publication 800-30 Rev.1 (SP 800-30 Rev.1) framework *Guide for Conducting Risk Assessments* by National Institute of Standards and Technology (NIST). SP 800-30 Rev.1 framework is followed to provide a thorough risk assessment and analysis of current IS/IT landscape of Banksia for senior leaders and/or executives of the organization in determining the appropriate courses of action in response to identified risks.

Qualitative approach is selected in the assessments. Qualitative approach provides a simpler representation of risks and its contributing factors which supports communicating results to decision makers (NIST 2012, p. 14). Assessments provide a range of values of the risk factors and the combination of risk factors to analyze the risks (NIST 2012, p. 6). Assessment scales of threat sources and threat events (Appendix B), vulnerabilities (Appendix C), likelihood and impacts (Appendix E) and risks (Appendix E) are adapted from SP 800-30 Rev.1 framework with minor modifications.

The analysis in this report followed the threat-oriented approach in which threats sources and events will be identified and described first, vulnerabilities are then identified in the context of threats, the likelihood of threat events occurring measured against the likelihood of occurrence of adverse impacts of the threats, and analysis of control, impacts and level of risks (NIST 2012 p. 15). Threats are classified into two main categories i.e. adversarial and non-adversarial.

## Assumptions

Several assumptions are made as basis of this report. They are:

* Banksia’s in-house Compliance and Legal Department is responsible to ensure that the business adheres to external rules, e.g. government regulations, industry accreditation, industry standards, and internal controls that adequately measures and manage regulatory risks.
* IS/IT governance is governed by IS/IT Department.
* Assumptions with regards to controls are elaborated in the Scope and Control Analysis section.

# Risk Assessments

## Threat Identification

Pathology laboratories and services, such as Banksia, are an integral component of the healthcare industry as they hold highly confidential and complex patient’s data (Parwani 2017, p. 56). Therefore, it is imperative for the senior management at Banksia to realise these imminent threats and their potentially adverse impact on business processes, facilities, information security, data confidentiality, availability, integrity, customer growth, market share and business continuity (NIST 2012, p. 1).

A threat is “any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorised access, destruction, disclosure, or modification of information, and/or denial of service” (NIST 2012, p. 8). This segment explores three major adversarial and non-adversarial threats, amongst the other threats as listed in Table B.1. of Appendix B, facing the Banksia.

**System Failure & Downtime**

Banksia’s growth in terms of colossal business expansion, large-scale human resources, growing affiliation network and mobile service offerings has added numerous complications to their operations. IT systems that are outdated and inadequate in accommodating such complex and growing business operations increases the possibility of future system failure or downtime (Bowman 2013, p. 3). Currently, the IS/IT systems at Banksia Pathology Services are regarded as legacy systems, as they have gone through plenty of major developments since 2010. These legacy systems, often lacking implemented security patches, will eventually and inevitably expose confidential patient data and crucial organization information to internal/ external attackers, competitors and third parties (Weber 2006).

Often these legacy systems hinder in operating business functions through slower systems loading, denied access in certain departments and will most definitely result in system failure and downtime. As the legacy systems are so deeply ingrained in current business operations at Banksia, considerable capital investment as well as substantial organizational change will be a concern while replacing such systems (Deloitte 2008, p. 16).

System’s failure or downtime causes by an amalgamation of moderate to high adversarial and non-adversarial threat events (See Appendix B, Table B.1., identifier A7, NA1 – NA2, NA14 – NA16). IT services becoming partially or imminently unavailable, exacerbated by outdated systems that are overcapacity and overdeveloped needing frequent software maintenance classified as non-adversarial threats, leading to adversarial attempt of perpetrators exploiting the legacy system’s loopholes (Wang et al. 2016, p. 309). Such threats lead to delay in business operation, catastrophic errors in patient care, inaccurate report production, damage to or loss of information assets, theft and disclosure of data, and affect compliance to regulation. Probable to result in excessive damage to Banksia’s reputation, market position and relations with partners, vendors, customers and service providers, and potential fines, suspension and/or cancelation of facility as classified inTable E.9of Appendix E.

**Cyberattacks carried out by insiders and/or outsiders**

Upon review of the Table B.1. in Appendix B, threats such as A1, A2, A8 – A13, NA18 involve adversarial and non-adversarial cyber-attacks. Globally, organizations have experienced a growth of 82 percent in cyberattacks (Fortinet 2017, p. 9). This is concerning as the arise of recent attacks against healthcare institutions, such as WannaCry ransomware attack, which successfully invaded and locked out the systems of over fifty UK hospitals (Coventry & Branely 2018, p. 50).

Healthcare institutions, including pathology laboratories, experience two times higher threat of cyber-attacks pertaining to the possession of exceedingly vulnerable data, such as confidential/sensitive patient records, genetic information, interaction with government systems i.e. Medicare, health insurance, regulatory compliance among others (Parwani 2017, p. 56). If compromised, this can result in extensive financial and legal costs, and reputational damage for Banksia.

Cyber adversary such as malware, hacking, ransomware among others are expected and have a very high likelihood to occur in Banksia’s case carried out by threat sources, such as adversarial or non-adversarial employee, third-party vendors, partner organizations, and outside attackers adamant on obtaining financial gain, exploiting data for identity theft or potential competitive advantage (Danko & Steingartner 2017, p. 89). Among these, intentional or unintentional insider attacks are a major threat to the business because of their legacy system usage along with frequent software maintenance, cloud dependency, higher number of internal/ external users accessing the system, over-reliance on third-party services as well as dependence on the interconnected devices, API and Middleware integration potentially exposes Banksia pathology services as conspicuous beacon for cybercrime.

**Mishandling of Compliance Data Requirement**

There is limited evidence of existing organisational practices or guidelines pertaining to ensure lawful conduct and regulatory compliance, especially on third parties. Reliance on the third parties, including the appointed data backup facility provider, can be an extreme liability to organisations that are highly regulated, such as healthcare. Therefore, adhering to compliance requirement pose a major concern for Banksia’s management to ensure continuity of operations (Kruse et al. 2017, p. 2).  Such vulnerability is expected to result in higher threats of data corruption, mismanagement and mishandling for Banksia which are classified as High (See Appendix B, Table B.1., identifier A6, A18 – A22, A24, NA7 amongst others)

Reliance on third-party service providers for performing critical business functions are regarded as an ongoing concern within the healthcare industry (Krivin et al. 2013, p. 2). Thus, this increases business exposure along with an increased risk of data breaches, supply chain attacks and security compromise by either third parties or perpetrators attacking through such access (Kwon & Johnson 2012, p. 47). Banksia may incur adverse impact such as legal actions, financial sanctions, non-adherence to contractual requirements, catastrophic damage to patient records and care amongst others in event of regulatory non-compliance within the organizations (Chew & Ramadhany 2017, p. 6).

Additionally, senior management is advised to establish, implement and monitor a security centric culture, by incorporating administrative actions towards replacing or enhancing obsolete systems, limiting user access, introduce security and regulatory compliance practices through frequent in-house education and training sessions (Hu et al. 2012, p. 647).  Vigilance towards employees, third party as well as privilege user access and security conduct instilled and administered by senior management through motivators and evaluations such as key performance indicators, promotions, bonuses and other rewards (Hu et al. 2012, p. 648).

## Vulnerability Identification

A vulnerability is “a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source” (NIST 2012, p. 9). Though there are known vulnerabilities, new vulnerabilities will emerge as the company expands, and new stakeholders and new technologies are involved. Please see Appendix C Table C.2. for a list of Banksia IS/IT vulnerabililies.

**Reliance on Legacy Internal Systems**

Currently, the IS/IT infrastructure at Banksia Pathology Services comprises of the outdated, often known as legacy systems, running since its inception (Prananto 2019). Such obsolete system, having gone under frequent software/ hardware maintenance, has not been able to cope up with the expanding business, facilities, partner affiliations and increased user access (Prananto 2019).

This legacy system, often lacking implemented security patches, will eventually and inevitably expose confidential patient data and crucial organization information to internal/ external attackers, competitors and third parties (Spears & Barki 2010, p. 505).

Often these legacy systems hinder in operating business functions through slower systems loading, denied access in certain departments and will most definitely result in system failure and downtime (Aziz 2012). As the legacy system is so deeply ingrained in current business operations at Banksia, considerable capital investment as well as substantial organizational transition will be a concern for senior management while replacing such systems (Wessel et al. 2016, p. 73).

**Lack of Internal Cyber Security Controls and/or Initiatives**

Based on the historical events, Banksia has not faced any attempts of major cyber-attacks; hence, it is assumed that only basic controls such as firewalls and off-the-shelf anti-virus software are implemented to reduce the likelihood of threat occurrence (Prananto 2019). Considering the vast amount of sensitive data stored in the system that adversary trying to target with more sophisticated tools, the same level of protection will be insufficient as the system has been added with multiple components to support the business activity further opening up many vulnerabilities for a potential attacker to exploit it (Business Link UK 2019).

**Limited or No Evidence of IS/IT Governance on Third-Party Security Control Implementation**

Governance defines as the activities such as managing company’s IT operation, relationships between company’s management, shareholders and stakeholder (Racz, Weippl & Seufert 2011, p. 1). Furthermore, it was identified that Banksia also has of lack of IS/IT governance that relates them with their third-party vendors. This is a very high vulnerability severity (See Appendix C, Table C.2) can lead to risk in mishandling and disclosure of data due to lack of governance of third-party vendor. For example, the user or employee of the third-party vendor could expose the confidential data to other staff or outsider group which can lead to the risk of identity theft. Moreover, limited evidence of IS/IT governance on implementation of security controls (Prananto 2019) by the third party can cause information security breach that could cause Banksia loss of assets, privacy breach leading to compliance issues, damaging the relationship between patient/clients, partners and financial loss. Thirdly, due to non-existing of incident recover plan (IRP) could lead to the risk in unauthorised access and data theft due to potential threat of delay in reporting the incident that happened.

**Lack of Compliance Monitoring on Third Parties**

Compliance defines as “process that assured the adherence of an organization to regulatory, legal, contractual and other obligations” (Racz, Weippl & Seufert 2011, p. 1). In the previous 10 years of Banksia operating, they have not experienced any suspension, penalties and system they use are compliant and very up to date (Pranoto 2019). However, working with a third party back up provider with very limited experience constitutes as a very high vulnerability. This might lead to the inability to respond to IS/IT related incidents and leads to the risk in suspension/cancelation of facilities due to non-compliance of the third-party vendor.

## Control Analysis

According to Stoneburne, Goguen and Feringa (2002, p. 19) the control analysis defines as the analysis of the current controls by a company or organization to reduce the likelihood of threats and this analysis also focuses on what can be planned for the future in order to further minimise the current risk (Braga, Wisburd & Turchan 2018, p. 205). In order to carry out the current controls, there different types of internal controls such as deterrent, preventive, detective, recovery, corrective and compensating (Lousteau et al. 2003, p. 39). Deterrent controls can be used to “change offender behaviour” by carrying out strategy such as policy that is connected with the law enforcement (Kennedy 2008 cited in Braga, Wisburd & Turchan 2018, p. 206), preventive is to avoid occurrence of unwanted events such as training (Lousteau et al. 2003, p. 39), detective can include reviewing or uncover problems after incidents have occurred such as audit and logs. Recovery controls is to help organization to recover from loss of resources, corrective is the attempt to correct problems after discovering events (Lousteau et al. 2003, p. 39) such as termination of connection. Lastly, compensating is to put extra layer of the controls that has been implemented such as back up procedure or extra training programs.

When the system is developed in 2010, it can be assumed that simple controls were implemented. Lab testing was carried out in accordance despite having manual labelling of the sample container. The other controls that they have were investigation of any issue that they have. Furthermore, as the growth of Banksia’s from 2010, their control over their system has been a challenge where maintenances and other controls was needed to keep the system operating well (See Appendix D).

## Likelihood, Impact and Risk Determination

Risk is determined by comparing the likelihood of a threat event’s occurrence and potential adverse impact shall the event occur (NIST 2012, p. 12).

### Likelihood

Likelihood of occurrence is “a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or a set of vulnerabilities)” (NIST 2012, p. 10). The overall likelihood of associated threat event (Appendix E Table E.4.) is determined by assessing the likelihood that the threat event will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events), and the likelihood of threat event results in adverse impact (NIST 2012 p. 33).

### Impact

Adverse impact is the magnitude of harm of a threat event after it successfully exploits a vulnerability or a set of vulnerability (NIST 2012, p. 11). The magnitude of impact is determined by evaluating the characteristics of threat sources, the vulnerability and the susceptibility of existing or planned control (See Appendix E Table E.6.).

### Risk Determination

Level or risk is determined by considering the likelihood of the events occurring and the impact that would result from the threat events (NIST 2012, p. 35). The level of risk of associated threat event represents the degree of severity of such event if it exploits the organization’s vulnerability.

The overall likelihood (Appendix E Table E.4) and impact of threat events (Appendix E Table E.6.) are combined to determine the level of risk (Appendix E Table E.5.).

## Risk Priority

Risk prioritization will enable Banksia to determine the threat events that could cause major business disruption. This effort will empower Banksia to place imminent controls to deter and counter respective adversarial attempts towards the organization. Based on the assessment, risks that are determined as Very High and High are classified into four major risks that management of Banksia should be aware of. These risks are prioritized based on the magnitude of impact that they have on the organization and used as basis for risk mitigation effort.

**Poor Performance Delivery and Potential Data Loss Risk**

Running on outdated and obsolete legacy systems increases the likelihood to incur risk of poor performance delivery as well as potential data loss. Currently, Banksia’s IS/IT infrastructure is unable to accommodate the expanding business operations, facilities, users and functionalities (Prananto 2019). Bawa (2016) suggests that even though engineering such legacy systems in sync with business processes and user service delivery, ultimately these systems will be unsupportive and unmaintainable as not being able to cope up with the emerging innovations, and transitions. Hence, performance and service delivery to patient’s is at risk because of delay in processes and erroneous report production because of system breakdown or downtime respectively (Wang et al. 2016, p. 309).

Legacy systems tend to become susceptible to potential cyber-attacks intended to stealing data if security controls are not properly installed. Lack of security measures in place by Banksia, is a major attraction for internal/ external attackers, employees, competitors, third party vendors and affiliated partners, thus, compromising the confidentiality and integrity of crucial patient’s data such as patient genetic history, payment details, medical history amongst others (Plotkin et al. 2015).

Banksia should uptake an agile approach while understanding the opportunity cost of continuing their operations through these legacy systems while incurring expensive maintenance. Operating and maintaining these obsolete systems distract management focus in exploring new opportunities and investment for the business (Norman 2007, p. 326). Lageschulte et al. (2017, p. 20) believes that while replacing the legacy system might seem the best mitigation strategy towards this risk, Banksia’s senior management must be immensely cautious and vigilant of the data migration in the new system.

In addition, senior management is advised to follow an agile approach towards establishing resilient infrastructure management, security and compliance framework and regulations. This can be achieved through integrated senior leadership rooted in the organizational culture ensuring such regulations are being collaboratively implemented and followed through all the departments at Banksia (Seigel 2018, p. 376).

**Risk of cyberattacks due to limited or lack of internal security control or initiatives**

The next major risk that Banksia faces would be cyber risk due to the organization’s dependency on the information system and its lack of security measures and/initiatives. These risks are determined as Very High and High on Table E.9. (See Appendix E). The threat source could be either internal or external entity whose sole intention is to disrupt the business by launching a cyber-attack using various infiltration methods (Kadivar 2014) which could directly result in data loss or theft, system unavailability, system lockout or data inconsistency. However, these are considered minimal loss. Major loss is associated with lawsuits in some cases (Victoria Department of Health 2019). Assuming that basic controls are already in place, adversary constantly improve their techniques to bypass security measures and target large organizations due to the sensitive data it holds (Sood, Enbody & Loshin 2014). Once system is accessed, adversary may disclose sensitive data which may lead to reputational and financial damage, potential legal actions pursued by affected party, and privacy breach which leads to non-compliance.

The attacks can also be directed towards external individual or entities, such as partner organization, client who’s using our system or to the cloud were our application may run or even at the data center where the backups are stored since we are connected to the organization to which the attack is focused our system might have to face that attack or it might even be our asset that might get hit. Controls such as setting up of VPN, Training the employee on best security practices, Monitoring employee activities and setting access control, hiring a team to monitor the data flow or even hiring an individual to handle the system from client’s end (van Schaik et al. 2017).

**Risk in mishandling and disclosure of data due to lack of governance of third-party**

Moeller (2011, p.24) argues that there has been increase of problems involving the exposure and abuse of power by conducting a criminal activity such as data theft, breach of compliance and service disruptions. Furthermore, it is important to understand the risk of Banksia third party governance as they are lacking IS/IT governance. For example, mishandling or exposure of data from the third-party provider. Due to lack of governance of third party such as monitoring and out of date contracts (Wayma 2013, p. 42), it is very difficult to understand their system because ineffective governance can lead to loss of customer satisfactions. Another reason why this risk is important because Banksia would also like to expand their services using third party service overseas, which then more governance is needed from the them.  Thus, it is important for Banksia to consider this risk of data loss caused by exposure of internal third-party employee and not all third-party providers have the same governance.

**Risk in penalties, suspension and/or cancelation of facility due to non-compliance**

According to Deursen, Bchanan and Duff (2013, p. 32) as the increase use of technology, it is hard to determine when employees are currently performing their job due to everything has becoming mobile.  Furthermore, Wayman (2013, p. 41) also mentioned that as it is very common for business to outsource their activities, there are also legal compliance risk associated with it. Direct appointment of the third-party data backup provider presents a risk as there was not any prior assessment on their operations (Wayman 2013, p. 43), including their IT controls and their approach to how manage Banksia’s partnership, collection centres and most importantly vast patient data.

Pathology laboratories are highly governed by medical standards and accreditations i.e. NATA/RCPA as the operations retain sensitive information. Other than protecting confidential data, vague written rules and regulations (Moeller 2011, p. 27) by the third-party vendor could also affect Banksia when they are handling and reporting incident in untimely manner which could lead to more data loss and disclosure of data by adversary. Such breach may lead incur penalties imposed by the governing bodies, or worse, suspension or cancelation of business.

# Risk Mitigation

Risks mitigation is the next step in risk management approach that aims to reduce the likelihood that a threat will occur. It is important for Banksia to set risk appetite, which defines the acceptable level of risk that the organization can accept. For example, an employee damages a small equipment twice a year. The likelihood and impact are miniscule therefore implementation of controls may be more costly. Therefore, such risk is accepted.

For risk that is categorized as Moderate to Very High, management can either choose to control them by either reducing the likelihood, compensate the loss or even spreading them across multiple businesses so that impact of the threat event would be reduced. While many high risks need immediate attention, there are also risks that have to be either avoided or transferred to another organization, such as an insurance provider. Additionally, risks that cause major business disruption and creating a control won’t be a feasible option so the organization might choose to avoid the risk (Prananto 2019).

## Feasibility and Effectiveness Control and Cost-Benefit Analysis

In attempt to mitigate the top risks, a list of controls is recommended to reduce the likelihood or impact that a risk may possess. Assessment on feasibility and effectiveness of control is conducted through cost-benefit analysis (See Appendix F Table F.1.) (Prananto 2019).

The cost-benefit analysis evaluates the cost to reduce the damage of the risk against the cost of the damage that the risk itself imposed if incurs without any controls. A qualitative value of the cost of control must be weighed against the cost of exposure. If cost of control is higher, a less costly control will be recommended, or accept the risk as the control cost more than exposure (See Appendix F Table F.1.) (Prananto 2019).

## Controls Implementation

The identified controls are assigned to an individual or an entity internal or external to the organization. External entity can involve a trusted and fully assessed third-party vendor with the expertise in the implementing the control optimally and timely (See Appendix F Table F.1.) (Prananto 2019).

## Residual Risk Statement

It is important to recognize that risks cannot be eliminated. Therefore, a risk appetite for the organization must be set in place in order to determine the level of impact an organization can accept. After the accepted control has been implemented, the control the risk’s occurrence rate goes down and the severity of impacts decrease. In other words, inherent risks are now becoming residual risks.

# Conclusion

While the expansion of Banksia presents unprecedented opportunities to the company, it also comes with a set of risks derived internally and externally that require management’s attention. The risk assessment report concludes that current operations of Banksia are faced by numerous IS/IT-related risks that are classified from Moderate to Very High.

The findings of this report calls for involvement of the senior executive management and the board members to view risks in a holistic approach, which consider the threats, likelihood and impacts, and due diligence practices, rather than solely focus under the threats of system downtime, cyber-attacks, third party governance and non-compliance.

Risk mitigation strategies are suggested to ensure continuity of organisational expansion and to provide guidelines to reduce the likelihood of threats occurrence and the adverse impacts that they have on the organisation.

# References

Aziz, O 2012, 'Into the sunset: agile risk management for replacing aging legacy systems', PMI Global Congress, Vancouver, Canada, Conference Proceedings, Project Management Institute, viewed 20 April 2019,   
<https://www.pmi.org/learning/library/agile-risk-management-legacy-systems-6080>

Bawa, R 2016, Cloud and infrastructure: The legacy of legacy—the ultimate drag on condensing into a cloud, Deloitte, viewed 29 April 2019, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-cons-cloud-and-infrastructure-legacy-of-legacy.pdf>.

Bowman, S 2013, 'Impact of electronic health record systems on information integrity: quality and safety implications'. Perspectives in health information management, vol. 10, pp. 1-20.

Braga, AA, Weisburd, D & Turchan, B, 2018,’Focused deterrence strategies and crime control: An updated systematic review and meta‐analysis of the empirical evidence’, *Criminology & Public Policy*, vol. 17, no. 1, pp .205-250.

Business Link UK 2019, *The challenges of growing a business - and how to meet them*, viewed 19 May 2019, <https://www.infoentrepreneurs.org/en/guides/the-challenges-of-growing-a-business---and-how-to-meet-them/>.

Chew, D & Ramadhany, S 2017, Third party risk management: Managing risks in your extended enterprise, Deloitte, viewed 15 April 2019, <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sg-risk-third-party-risk-management-brochure.pdf>.

Darko, G & Steingartner, W 2017, ‘Combining Cybersecurity and Cyber Defence to Achieve Cyber Resilience’, IEEE 2017 14th International Scientific Conference on Informatics, Poprad, Slovakia, Conference proceedings, pp. 87-93.

Deloitte 2008, When legacy is not enough, Deloitte, viewed 10 April 2019,   
<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-us-why-legacy-is-not-enough-2008.pdf>

Hu, Q, Dinev, T, Hart, P, & Cooke, D 2012, 'Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences', vol. 43, no. 4, pp.615-660.

Kadivar, M 2014, "Cyber-Attack Attributes", Technology Innovation Management Review, vol. 4, no. 11, pp. 22-27.

Krivin, D, Samandari, H, Walsh, J & Yueh, E 2013, Managing third-party risk in a changing regulatory environment, McKinsey & Company, viewed 19 April 2019, <https://www.mckinsey.com/~/media/mckinsey/dotcom/client\_service/risk/working%20papers/46\_third\_party\_risk.ashx>.

Kruse, CS, Federick, B, Jacobson, T & Monticon, DK 2017, ‘Cybersecurity in healthcare: A systematic review of modern threats and trends’, Technology and health care: official journal of the European Society for Engineering and Medicine, vol. 25, no. 1, pp. 1-10.

Kwon, J & Johnson, M.E 2012, 'Security practices and regulatory compliance in the healthcare industry', Journal of the American Medical Informatics Association, vol. 20, no. 1, pp.44-51.

Lageschulte, P, Nagaraj, K, Buffomante, A & Mouli, P 2017, Technology risk radar, KPMG, viewed 30 April 2019, <https://assets.kpmg/content/dam/kpmg/rs/pdf/2017/05/rs-kpmg-technology-risk-radar-2016.pdf>.

Martin, G, Martin, P, Hankin, C, Darzi, A & Kinross, J 2017, ‘Cybersecurity and healthcare: how safe are we?', BMJ, vol. 358.

Moeller, R.R., 2011. *COSO enterprise risk management: establishing effective governance, risk, and compliance processes*. John Wiley & Sons, Hoboken, New Jersey.

National Institute of Standards and Technology 2012, *Guide for Conducting Risk Assessments*, U.S. Department of Commerce, viewed 7 May, < <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>>

Norman, T 2007, Integrated Security Systems Design: Concepts, Specifications, and Implementation, Butterworth-Heinemann, Ebook Central (Proquest).

Parwani, AV 2017, ‘Healthcare industry steps up security as cyber-attacks increase', Medical Laboratory Observer, vol. 49, no. 11, pp.56.

Plotkin, G, Roy, P, Snyder, M & Stephens, G 2015, Taking the legacy system leap: Why legacy system projects often fail to deliver, KPMG, viewed 29 April 2019, <https://assets.kpmg/content/dam/kpmg/pdf/2015/08/mz083-fif-standalone-taking-the-legacy-v1.pdf>.

Prananto, A 2019, "Risk Assessment & Risk Mitigation", Presentation.

Prananto, A 2019, ‘Banksia Pathology Case Study’, INF80043 IS/IT Risk Management, learning materials via Canvas, Swinburne University of Technology, 4 March, viewed 18 April 2019.

Racz, N, Weippl, E & Seufert, A, 2011,’Governance, risk & compliance (GRC) software-an exploratory study of software vendor and market research perspectives’,*44th IEEE Hawaii International Conference on System Sciences*, 4 January – 7 January 2011, *Kauai, HI, USA,*pp. 1-10, viewed 18 May 2019, < https://ieeexplore-ieee-org.ezproxy.lib.swin.edu.au/stamp/stamp.jsp?tp=&arnumber=5718984>.

Seigel, M 2018, ‘Building resilient organizations: Proactive risk management in organizations and their supply chains’, Journal of Business Continuity & Emergency Planning, vol. 11, no. 4, pp. 373-384.

Sood, A, Enbody, R & Loshin, P 2014, Targeted cyber-attacks, Elsevier, Amsterdam.

Spears, J.L & Barki, H 2010, 'User participation in information systems security risk management', MIS quarterly, vol. 34, no. 3, pp. 503-522.

Stoneburner, G, Goguen, AY & Feringa, A, 2002, Sp 800-30, risk management guide for information technology systems.

van Schaik, P, Jeske, D, Onibokun, J, Coventry, L, Jansen, J & Kusev, P 2017, "Risk perceptions of cyber-security and precautionary behaviour", Computers in Human Behavior, vol. 75, pp. 547-559.

Van Deursen, N, Buchanan, WJ & Duff, A 2013,’Monitoring information security risks within health care’, *computers & security*, vol. 37, pp.31-45.

Victoria Department of Health 2019, IHI Risk Assessment Report, Victoria Government, Melbourne, viewed 17 May 2019, <https://www2.health.vic.gov.au/Api/downloadmedia/%7BA0FB6D84-EE91-4AE9-B8D0-CE3BC68E2B23%7D>.

Wang, Y, Coiera, E, Gallego, B, Concha, O.P, Ong, M.S, Tsafnat, G, Roffe, D, Jones, G & Magrabi, F, 2016, 'Measuring the effects of computer downtime on hospital pathology processes', Journal of Biomedical Informatics, vol. 59, pp. 308-315.

Wayman, M, 2013,’Curbing outsourcing risks: internal audit should examine closely the oversight of the organization's third-party relationships to enhance effective governance and decrease risk’, *Internal Auditor*, vol. 70, no. 1, pp .41-45.

Weber, C 2006, Assessing Security Risk in Legacy Systems, Department of Homeland Security, viewed 15 April 2019,   
<https://www.us-cert.gov/bsi/articles/best-practices/legacy-systems/assessing-security-risk-in-legacy-systems>.

Wessel, M, Leview, A & Siegel, R 2016, 'The problem with legacy ecosystems', Harvard Business Review, vol. 94, no. 11, pp. 68-74.

Wood, B, Gagliardi, M & Bianco, P 2014, "Migrating a large-scale legacy IT system to a system with current technology", Presentation.

# Appendices

## Appendix A Scope

### Table A.1. System Characterization

|  |  |
| --- | --- |
| System Characterisation | Description |
| Hardware | * Laboratory machineries * Organization-owned mobile computing devices * Individual-owned mobile computing devices * Servers * Backup servers * Point-of-Sale machines * EFTPOS machines |
| Software | * Intranet portal i.e. Pathology Intranet Portal (PIP) * Client/partners portal i.e. Patient Management Portal (PMP) * Back-office system |
| System Interfaces | * Internal connectivity of information systems locally and interstates via cloud-based software * Internal systems controlling lab machineries * Internal back-office system * External connectivity with third-party or off-the-shelf systems via API and middleware * External connectivity with government systems (e.g. Medicare, HealthConnect/eHealth) * Wired and wireless internet connectivity with Internet Service Provider |
| Data and Information | * Patient administrative and medical data * Employee data * Organizational data * Third-party data |
| People | * Employees in collection centres, main clinical labs, central laboratory lab * Patients * Partner organizations i.e. GP offices, nursing homes, independent-living centres * Third-party vendors, i.e. off-the-shelf software vendors, system maintenance vendor, computing devices vendors, medical equipment vendors |
| System Mission | * To support business functions by processing and storing of data |
| System and data criticality | Due to strict standards and accreditation imposed on medical laboratories, government regulations and standards in interconnectivity and interchange with government systems, industry standards governing credit cards transactions, the system requires the **highest level** of protection to maintain system and data confidentiality, availability and integrity. |
| System and data sensitivity | * Systems are constantly used as they support the main business functions * Systems reach the maximum capacity due to rapid growth of business, which increase number of users and data size. |
| The functional requirements of the IT system | PIP system: To manage various Human Resources-related functions (e.g.  rostering, processing salary of staff, processing annual leave, handling contract related enquiry) and displaying job-related information including compliance and review of clinical test    PMP system: To schedule appointment, manage progress of patients, check results, test history.    Back-office system: (There is limited evidence what constitute in back-office system; hence, assumptions are made.) To manage back-office daily functions. |
| System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices) | * Pathology laboratory standards and accreditation by the National Association of Testing Authorities (NATA)/RCPA Laboratory Accreditation Program * Other medical laboratories standards and regulations, such as National Pathology Accreditation Advisory (NPAAC) (managed by the Australian Government Department of Health International) - *Requirements for Medical Pathology Service, Second Edition 2018*, Organization for Standardization (ISO) standard ISO 15189:2003, *Medical Laboratories – Particular Requirements for Quality Competence* * Government requirements for interchange and interconnectivity with government systems * Privacy Act 1988 * Other jurisdiction’s privacy and data protection regulation, such as EU General Data Protection Regulation (GDPR) * Payment Card Industry Data Security Standard (PCI DSS) |
| System security architecture | There is limited/no information provided on system security architecture. |
| Current network topology | There is limited/no information provided on current network topology. |
| Information storage protection that safeguards system and data availability, integrity, and confidentiality | * Assumption made that current information storage protection is maintained by third-party security organization and off-the-shelf anti-virus programs |
| Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart) | Input: Lab results, patient information (i.e. contact details, payment details etc), employee information (i.e. contact details, bank details, salary details, availability of work, contract details etc).  Output: Lab reports, confirmation of appointment, logged payment history, roster, payslip, confirmation of leave etc. |
| Technical controls used for the IT system, encryption methods) | As there is limited/no evidence in technical controls, assumptions are made based on observation on the case study and references to industry standards and practices. They are:   * Secured login credentials to access computing devices * Off-the-shelf anti-virus software installed * Centralised data backups facility * System maintenance by third-party vendor |
| Management controls used for the IT system | As there is limited/no evidence in management controls, assumptions are made based on observation on the case study and references to industry standards and practices. They are:   * IS/IT policy/governance * Staff training on using information systems * System maintenance |
| Operational controls used for the IT system | As there is limited/no evidence in operational controls, assumptions are made based on observation on the case study and references to industry standards and practices. They are:   * Personnel security * System maintenance by third-party vendor * Segregation of user functions, i.e. privileged and standard user access |
| Physical security environment of the IT system | As there is limited/no evidence in physical security environment, assumptions are made based on observation on the case study and references to industry standards and practices. They are:   * Access card for staff * Physical lock with password on server room * Alarms * CCTV camera |
| Environmental security implemented for the IT system processing environment | As they limited evidence on environmental security implemented, assumptions are made based on observation on the case study and references to industry standards and practices. They are:   * Control for humidity and temperature in server room |

## Appendix B Threat Identification

### Table B.1. Identification of Adversarial Threat Sources and Events

|  |  |  |  |
| --- | --- | --- | --- |
| Identifier | Threat Events | Threat Source | Threat Description |
| Adversarial Threats | | | |
| A1 | Outsider (Individual/Group) adversary | Ransomware attack to the main information system | Having a weak firewall, system security software or other security controls enables the attacker to place a ransomware attack to the system. |
| A2 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | Targeted malware attack into internal system | Adversary inserts malware into internal information systems and information system components specifically targeted to the hardware, software, and firmware of the organization. |
| A3 | Outsider adversary group | Adversarial campaign across multiple organizations to acquired information | Adversary targets multiple organizations that are connected to acquire specific information. |
| A4 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | Exploitation on vulnerabilities using zero-day attacks | Adversary deploys attack that exploits as yet unknown to or unaddressed by those who should be interested in mitigating the vulnerability. |
| A5 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | System and data breach on irregularly maintained system | Lack of IS/IT governance on internal system maintenance (e.g. software patching solution) leads to system and data breach by adversary causing adversary may damage or steal organizational data. |
| A6 | Adversary targeting low-security third-party systems | Ransomware to the overseas information systems | Since there is no evidence on IS/IT governance on implementation of security controls on third-party systems, including backup data service provider, external API-connected systems, overseas radiology centre and medical partner organizations. |
| A7 | Adversary, including individual outsiders, established/ad hoc outsiders' group, trusted insider, privileged insider | Destruction of critical information system components and functions | Adversary destroys or causes deterioration of critical internal information system. |
| A8 | Insider adversary, including authorised users, trusted insider (e.g. authorised users of partner organizations), privileged insiders | Internal system breach via physical access | Due to lack of internal cybersecurity controls/initiative, adversary breach internal system via physical access (e.g. plugging malicious USB to desktop, gaining unauthorised access to server room) and tampering or stealing sensitive/confidential organizational data. |
| A9 | Outsider (Individual/Group) adversary | Distributed Denial of Service (DDoS) attack | Cyber adversary uses multiple compromised devices/systems to attack a single target, thus cause denial of service for users of the targeted devices/systems. |
| A10 | Insider adversary, including authorised users, trusted insider (e.g. cloud service provider, partner organizations) | Cause disclosure of critical and/or confidential information by authorised users | Adversary with authorised access to systems inadvertently expose, disclose or mishandle sensitive/confidential information. |
| A11 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | Conduct brute force login attempts/password guessing attacks | Adversary establish communication channel to the organization or targeted information system through brute force login or numerous password guessing attempts. |
| A12 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | Data theft by unauthorised access | Adversary steals confidential/sensitive information through unauthorised access. |
| A13 | Outsider (Individual/Group) adversary | Conduct externally based session hijacking | Adversary hijacks already established, legitimate information system sessions between organizations and third-parties (e.g. users connecting from remote location). |
| A14 | Outsider (Individual/Group) adversary | Phishing attacks | Without guidelines nor training on cybersecurity awareness, employees may be unaware of adversary counterfeiting communications from a legitimate source to gain access to sensitive/confidential information. |
| A15 | Outsider (Individual/Group) adversary | Spear phishing attacks | Adversary deploys phishing attacks to high value targets, such as senior executive management, who lacks in proper security practices. |
| A16 | Adversary, including insiders (e.g. employees), trusted insider (e.g. partner organizations), privileged insider | Exploit split tunnelling | Adversary exploits external organizational information systems (e.g. laptops at remote locations) that are simultaneously connected securely to organizational internal information systems or networks and to non-secured remote connection. |
| A17 | Privileged insiders across different facilities, third- party vendors and partner organizations | Insider attacks | Increasing system access and number of devices causes more probability of insider attacks, where the organization's data, processes and assets are compromised due to adversarial actions of users. |
| A18 | Adversary attacking third-party systems/networks/infrastructure, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | Delivery of known/modified/targeted malware to third-party systems | Third-party data backup facility was appointed without proper assessment on security controls. Thus, adversary may use common communication mechanisms to install known malware. |
| A19 | Adversarial insiders | Data theft | Data theft by dishonest authorised users of third-party partner organizations or vendors. |
| A20 | Adversary, including individual outsiders, established/ad hoc outsiders’ group, trusted insider, privileged insider | Internal system breach via physical access at third-party facility | Adversary breaches internal system via physical access at third-party facility (e.g. plugging malicious USB to desktop, gaining unauthorised access to server room) and tampers/steals sensitive/confidential organizational data, which may be Banksia's patient data. |
| A21 | Insider adversary in third-party organizations, including authorised users, trusted insider (e.g. cloud service provider, partner organizations) | Cause disclosure of critical and/or confidential information by authorised users | Adversary with authorised access to systems inadvertently expose, disclose or mishandle sensitive/confidential information. |
| A22 | Adversary targeting low-security third-party systems | Distributed Denial of Service (DDOS) attacks to third-party systems | Due to limited security controls of third-party systems and infrastructure, adversary use multiple compromised devices/systems to attack a single target. |
| A23 | Adversary gains unauthorised access | Delay in incident reporting | Due to delay in reporting an incident, e.g. stolen or missing laptop, adversary already gains unauthorised access to the device. |
| A24 | Adversary targeting backup data facility | Exploit recently discover vulnerabilities | Adversary exploits backup data facility to inadvertently expose, disclose or mishandle sensitive/confidential information. |
| A25 | Adversary, including individual outsiders, established/ad hoc outsiders' group, trusted insider, privileged insider | Malware attack | Due to its connectivity, cloud-based system is used as a point of malware attack for adversary. |
| A26 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), competitor with ill-intent, trusted insider (e.g. cloud service provider, partner organizations) | Conduct data scavenging attacks in cloud environment | Cyber adversary obtains data used and then deleted by organizational processes running in cloud environment. |
| A27 | Adversary on infected IoT device accessing internal systems | Cyberattacks to the internal system via external devices | A user trying to access internal cloud-based systems from his/her own device that is infected in malware; thus, resulting in attacks in internal system. |
| A28 | Insider and outsider adversary | Stolen or missing hardware device | Adversary take possession company's devices (e.g. laptop) and gains unauthorised access to organizational information systems. |
| A29 | Adversary, including individual outsiders, established/ad hoc outsider group, trusted insider, privileged insider | Network sniffing of internal exposed networks | Adversary gains access to organization's exposed wired or wireless data channels, such as publicly available Wi-Fi, used to transfer information, uses network sniffing to identify components, resources and protection. |
| A30 | Adversary, including individual outsiders, established/ad hoc outsider group, trusted insider, privileged insider | Compromise critical information system via physical access | Adversary obtains physical access to organizational information systems of third parties and tampers data. |
| A31 | Adversary, including individual outsiders, established/ad hoc outsider group, trusted insider, privileged insider | Exploitation of systems on API (system communication), such as parameter attack, identity attack, MITM attack | API is a channel for third-party application integration allowing communication between systems and access into internal database containing sensitive/confidential information. Adversary finds a loophole in the integration and exploits the communication using different techniques. |
| A32 | Adversary, including individual outsiders, established/ad hoc outsider group, trusted insider, privileged insider | Supply chain attacks targeting and exploiting critical hardware, software, or firmware | Adversary targets and compromises the operation of software (e.g. through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components. |
| A33 | Outsider adversary, including thief, hacker | Unauthorised access to stolen mobile computing devices | Adversary gains possession of organization-owned mobile computing device, e.g. laptop, and easily gains access to data stored in the device due to lack of security control. |
| A34 | Individual/Group Outsider Adversary | Exploit multi-tenancy in cloud environment | Adversary takes advantage of multi-tenancy to observe behaviour of organizational processes, acquire organizational information, or disrupt with the timely or correct functioning of organizational processes. |
| A35 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), competitor with ill-intent, trusted insider (e.g. cloud service provider, partner organizations) | Campaign of multi-stage attacks | Adversary moves the source of malicious commands or actions from one compromised information systems to another, making analysis difficult. |
| A36 | Individual/Group adversary targeting Internet Service Provider systems/network | Adverse cyber events affecting Internet Service Provider network | Adversary launches attack on the infrastructure of contracted Internet Service Provider. |
| A37 | Adversary, including insiders (e.g. employees), individuals/group outsiders (e.g. hackers), trusted insider (e.g. cloud service provider, partner organizations) | Creation, modification and/or deletion of data on publicly accessible information systems | Unauthorised access to sensitive/confidential information by adversary through publicly available devices. Adversary may create, modify or delete critical data. |
| A38 | Adversary, including insiders and outsiders | False/Fraudulent patient information recorded in the system | There is no evidence of identity authentication of patient allowing adversary to intentionally record wrong information to systems, or outsiders register with someone else's identity. |
| A39 | Insider and outsider adversary | Password sharing by an insider to an outsider | An insider shares password with an adversarial outsider who gains access to the system using the insider's credentials. |
| A40 | Terrorist or terrorist group | Terrorist attack in one of the major Australian cities | Terrorist attack conducted in one of the major Australian cities causing some fatalities and/or injuries or loss of life. |
| A41 | Adversary, including insider and outsider | Physical attacks on organizational facilities | Adversary performs physical attack on organization facilities, e.g. sets a fire, robbery. |
| A42 | Insider adversary, e.g. employees handling payment | Theft | Insider adversary, e.g. staff handling cash payment, takes advantage of the manual process of cash handling and steal cash payment. |
| Non-adversarial Threats | | | |
| NA1 | Outdated, overdeveloped and over-capacity internal systems | Depletion of functional system | Degraded storage or processing performance to due internal systems depletion. |
| NA2 | Outdated systems with slow processing performance, constant scheduled maintenance performed on internal systems | System failure/breakdown | Outdated systems fail to operate due to over-capacity, aging, constant maintenance, and is unable to cope up during peak hours of business operations. |
| NA3 | IS/IT department and risk management team | Delayed response in attending to IS/IT related incident | Without proper Incident Response Plan or Disaster Recovery Plan, can result in lack of response when adverse events occur causing greater damage or loss in information assets, physical assets, physical injuries, and damage to trust relationships which can lead to damage to organizational reputation. |
| NA4 | Compliance Officers | Mishandling of compliance data requirements on handling payment data and transactions. | There is no evidence that the company is exercising its due diligence in making sure that handling credit card transactions remains compliant. |
| NA5 | IS/IT department in setting up backup policy and practice | System fails to backup all data | Backup of data is conducted every 30 day instead of instantly once data is written to the system. Interruption/incident may occur between the scheduled backup. |
| NA6 | Compliance Officers | Mishandling of compliance data requirements | There is limited evidence that the company is exercising its due diligence in making sure that operations and operations of third parties, are compliant with laws and regulations. |
| NA7 | Compliance Officers | Regulations oversight of third party in another jurisdiction | Overseas third-party fails to comply with governing bodies regulations or change in regulations within their country in handling sensitive medical data causing service disruption, disclosure of sensitive data causing financial and reputational damage, and breach of compliance which may lead to imposed sanctions. |
| NA8 | Individual business unit | Unauthorised procurement of IS/IT systems by other departments | Unauthorised purchase of IS/IT related procurement by other department that does not adhere to the IS/IT governance, causing disintegrated system. |
| NA9 | IS/IT department | Improper assessment of third-party vendor | Without following IS/IT governance in third-party vendor selection, direct appointment of data backup provider is not properly assessed in handling data that contains confidential/sensitive information. For example, the facility may lack proper security controls. |
| NA10 | Data backup service provider | Failure to respond to IS/IT-related incidents | Hiring a start-up data backup service provider can put the data at risk as they would not know what to do in a crisis situation that jeopardizing data security. |
| NA11 | Radiologists and medical professionals at the overseas facility | Incorrect analysis of radiography data/images | Limited evidence in governance on monitoring third-party radiology centre in handling radiology images. |
| NA12 | IS/IT department in monitoring third-party vendors performance | Contractual breach | Limited evidence of due diligence performed by IS/IT department in monitoring performance of third-party vendors, which resulting in contractual breach. |
| NA13 | Non-adversarial electrical failure or other resources triggering fire | Non-adversarial fire incident at the data backup facility | Non-adversarial fire incident at main or backup facility causes inoperable facility or destroys backups of data, software, configurations and/or logs. |
| NA14 | IS/IT department in development and upgrade of internal systems | Unavailability of desirable system functionalities | The internal system is outdated and thus, lacks some functionalities that are desirable for more effective service delivery, such as sending automatic reminders to patient, which may lead to ineffective operations. |
| NA15 | IS/IT department performing constant system maintenance during peak business hours | Periods of non-availability of systems during peak business hours | IS/IT department or contracted third-party vendor for system maintenance perform constant system maintenance needed to ensure systems are running properly during peak business hours. |
| NA16 | Outdated, overdeveloped and over-capacity internal systems | Slow data processing capability | Functional speed of internal systems is deteriorated due to over-development and over-capacity internal systems causing disruption in service delivery. |
| NA17 | Improperly trained employees in handling data | Mishandling of critical and/or confidential information by authorised users | Authorised users, e.g. employees, inadvertently expose critical/sensitive information due to lack of knowledge in handling data. For example, employee accidentally sends an email containing confidential information to a wrong recipient. |
| NA18 | Improperly trained employees | Spill confidential information | Authorised employee erroneously contaminates information system, device or network by placing on it, or exposing sensitive/confidential information. The information is exposed to access by unauthorised individual and causing the device/network/system to become unavailable until the spill is investigated and mitigated. |
| NA19 | Employees | Damage to hardware, equipment, component parts and other physical assets | Employees accidentally damage hardware, equipment, component parts or other physical assets that are used to manage organizational data. |
| NA20 | Employees installing free software containing malicious content | Unauthorised download and/or install of non-approved software in company's devices | No evidence of IS/IT governance on use of company's devices resulting in employees to download and install non-approved software/applications, causing increased network architecture exposure to cyber adversary activities. |
| NA21 | Non-adversarial human error by authorised third-party employees | Mishandling of patient data by third-party authorised users | Authorised users of third-party, e.g. employees, inadvertently expose critical/sensitive information due to lack of knowledge in handling data. |
| NA22 | Off-the-shelves software products installed in the information systems | Inherent vulnerabilities into software products | Inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into the commonly used off-the-shelves software products which are used by the organization to perform business functions. |
| NA23 | System error due to defect functionalities | Incorrect sample analysis report | Non-adversary incorrect patient sample analysis report due to defect in the functionality of the Haematology Analyser System. |
| NA24 | Non-adversarial human error by authorised employees | Incorrect labelling of sample container | Non-adversarial human error during manual labelling process of samples causing incorrect labelling of sample container. |
| NA25 | Non-adversarial human error by authorised employees | Inaccurate laboratory report production | Non-adversarial human error in manual laboratory report production resulting in accurate report/laboratory results. |
| NA26 | Non-adversarial human error by authorised employees | Incorrect data recording | Non-adversarial human error in during sample processing causing mishandle of patient information by inputting patient data into the system incorrectly. |
| NA27 | Third-party employees | Accidental damage to hardware, equipment, component parts and other physical assets at third-party facilities | Employees accidentally damage hardware, equipment, component parts or other physical assets at third-party facilities that are used to manage organizational data |
| NA28 | Compliance Officers | Mishandling of compliance interchange and interconnectivity government system regulations and standardisations | There is no evidence that the company is exercising its due diligence in making sure interchange and interconnectivity with government systems are always in compliant with the standards and regulations. |
| NA29 | IS/IT department | Hardware failure during operations | Hardware, such as servers, analyser systems, individual desktops, are not regularly maintained as there is no evidence on IS/IT governance on hardware maintenance. |
| NA30 | IS/IT department | Disk error | Corrupted storage due to disk error of aged or depleted computing hardware. |
| NA31 | Frequent use of system | System failure of analyser system | Due to frequent use, the Haematology Analyser System fails to function during peak business hours. |
| NA32 | Non-adversarial disruption to Internet Service Provider infrastructure/network, e.g. scheduled network maintenance | System is inaccessible by clients and facility due to loss or interruption of internet connection | Non-adversarial activities by contracted Internet Service Provider causing disruption to system connectivity to the cloud thus disabling access to the internal systems. |
| NA33 | Third-party organizations, including partner organizations and IS/IT vendors | Hardware failure during operations | There is no evidence that regular hardware maintenance is performed by third-party organizations, which results in hardware failure during operations. |
| NA34 | Non-adversarial driver's negligence, external factors beyond driver's control (e.g. distracted driver crash to sample transfer van) | Road accident during sample transfer | Non-adversarial road incident during sample transfer leading to injury of driver, loss of collected samples causing delay in data processing or laboratory report production and lengthy investigation process. |
| NA35 | IS/IT department, System admins | Incorrect privilege settings | Authorised privileged administrator or user inadvertently assigns a user exceptional settings or set privilege requirements on a resource low. |
| NA36 | Electricity provider | Power outage at main or backup facility | Electricity outage at main or backup facility causing operational disruption of hardware which rely on electricity to function normally (e.g. servers, desktops, analyser system) in processing data. |
| NA37 | Natural disaster - flood | Flood at main or backup facility | Non-adversarial flood incident at main and backup facility causes inoperable facility or destroys backups of data, software, configuration and/or logs. |
| NA38 | Natural disaster - earthquake | Earthquake at one of the sites or all sites destroying physical assets | Earthquake at a large magnitude affect the laboratories. |

## Appendix C

### Table C.1. Assessment Scale – Vulnerability Severity

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability. |
| High | The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective. |
| Moderate | The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective. |
| Low | The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective. |
| Very Low | The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective. |

(Source: NIST 2012, p. F-2)

### Table C.2. Identification of Vulnerabilities

|  |  |  |
| --- | --- | --- |
| Identifier | Vulnerability Source of Information | Vulnerability Severity |
| A1 | Lack of internal cybersecurity controls and/or initiatives | High |
| A2 | Lack of internal cybersecurity controls and/or initiatives | High |
| A3 | Zero-day vulnerability | Very High |
| A4 | Limited evidence of IS/IT governance on internal system maintenance | Moderate |
| A5 | Limited evidence of IS/IT governance on internal system maintenance | Moderate |
| A6 | Limited evidence of IS/IT Governance on implementation of security controls by third-party on their systems | High |
| A7 | Legacy internal systems | High |
| A8 | Lack of internal cybersecurity controls and/or initiatives | High |
| A9 | Lack of internal cybersecurity controls and/or initiatives | High |
| A10 | Lack of internal cybersecurity controls and/or initiatives | High |
| A11 | Lack of internal cybersecurity controls and/or initiatives | High |
| A12 | Lack of internal cybersecurity controls and/or initiatives | High |
| A13 | Lack of internal cybersecurity controls and/or initiatives | High |
| A14 | Poor security practices by employees | High |
| A15 | Poor security practices by employees | High |
| A16 | Limited evidence of IS/IT Governance on company's device usage | High |
| A17 | Too many users with excessive access privileges | Low |
| A18 | Limited evidence of IS/IT Governance on implementation of security controls by third-party on their systems | Very High |
| A19 | Limited evidence of IS/IT Governance on implementation of security controls by third-party on their systems | Very High |
| A20 | Limited evidence of IS/IT Governance on implementation of security controls by third-party on their systems | Very High |
| A21 | No evidence of IS/IT governance regarding data processing and management in third-party facilities | Very High |
| A22 | Limited evidence of IS/IT Governance on implementation of security controls by third-party on their systems | Very High |
| A23 | Limited or no evidence in implementation of Incident Response Plan | Very High |
| A24 | Inexperienced data backup provider in implementation of security controls | Very High |
| A25 | Dependency on cloud-based software and cloud environment | Moderate |
| A26 | Dependency on cloud-based software and cloud environment | Moderate |
| A27 | Increased connectivity of devices to access internal portals | High |
| A28 | Lack of internal cybersecurity controls and/or initiatives | High |
| A29 | Lack of proper network infrastructure | Moderate |
| A30 | Limited evidence of IS/IT Governance on implementation of security controls by third-party on their systems | High |
| A31 | Reliance on API integration with third-party system | Moderate |
| A32 | Reliance on third-party systems | High |
| A33 | Lack of internal cybersecurity controls and/or initiatives | High |
| A34 | Dependency on cloud-based software and cloud environment | Moderate |
| A35 | Lack of internal cybersecurity controls and/or initiatives | High |
| A36 | Reliance on the service provided by Internet Service Provider | Moderate |
| A37 | Lack of internal cybersecurity controls and/or initiatives | High |
| A38 | No evidence in procedure imposed in verifying patient information with governing body | Very Low |
| A39 | Poor security practices by employees | Moderate |
| A40 | Geopolitical vulnerability | Very Low |
| A41 | Vulnerability to physical attacks | Low |
| A42 | Manual processing of cash payment at facility | Very Low |
| NA1 | Legacy internal systems | High |
| NA2 | Legacy internal systems | High |
| NA3 | No evidence in existing of Incident Response Plan or Disaster Recovery Plan | Very High |
| NA4 | Lack of governance framework that provides continuous monitoring of compliance in handling confidential payment information and transaction | Low |
| NA5 | Infrequent data backup policy/practice | Very High |
| NA6 | Lack of governance framework that provides continuous monitoring of compliance | Moderate |
| NA7 | Lack of governance framework at overseas partnered organisations that provides continuous monitoring of compliance in handling sensitive data | Very High |
| NA8 | Limited governance framework imposed on IS/IT procurement | High |
| NA9 | Limited governance framework imposed on IS/IT procurement | High |
| NA10 | Inexperienced data backup provider | Very High |
| NA11 | Limited evidence on IS/IT governance imposed on third-party in handling laboratory data | Moderate |
| NA12 | Limited evidence of third-party performance monitoring framework | Moderate |
| NA13 | Vulnerability to natural and man-made disaster | Low |
| NA14 | Legacy internal systems | High |
| NA15 | Legacy internal systems | High |
| NA16 | Legacy internal systems | High |
| NA17 | Employee negligence | Moderate |
| NA18 | Lack of internal cybersecurity controls and/or initiatives | High |
| NA19 | Employee negligence | Moderate |
| NA20 | Limited evidence on IS/IT governance imposed in using company's device | High |
| NA21 | No evidence of IS/IT framework regarding data processing and management in overseas facility | Very High |
| NA22 | Limited governance framework imposed on IS/IT procurement | High |
| NA23 | High dependency on analyser system | Very Low |
| NA24 | Manual process of sample collection, labelling and reporting | Very Low |
| NA25 | Manual process of sample collection, labelling and reporting | Very Low |
| NA26 | Manual process of sample collection, labelling and reporting | Very Low |
| NA27 | Employee negligence at third-party facilities | High |
| NA28 | Lack of governance framework that provides continuous monitoring of compliance on interchange and interconnectivity with government systems | High |
| NA29 | No evidence in IS/IT governance in hardware maintenance | High |
| NA30 | No evidence in IS/IT governance in hardware maintenance | High |
| NA31 | High dependency on analyser system | Very Low |
| NA32 | Reliance on the service of Internet Service Provider | Low |
| NA33 | No evidence on regular hardware maintenance by third-party organisations | High |
| NA34 | Mobile sample collection services | Low |
| NA35 | Employee negligence | Low |
| NA36 | Vulnerability to infrastructure failure/outage | High |
| NA37 | Vulnerability to natural and man-made disaster | Low |
| NA38 | Vulnerability to natural and man-made disaster | Low |

## Appendix D

### Table D.1. Existing Controls

|  |  |  |
| --- | --- | --- |
| Controls | Type | Description |
| Log in and Passwords. | Preventive | In order to determine who will be logging in to the portal, log in procedure needs to be completed in order to be able to access one’s information. |
| Antivirus detection/System monitoring | Detective | This antivirus detection alerts user if there are any malware or other attack appeared. For example, message will appear if there is any suspicious malware has been detected.    The senior executive and the head of IT department must create suitable defence or practices to prevent malware to occur due to antivirus is can only provide little protection to Banksia. |
| Policies | Deterrent | Banksia’s policy set by board of directors and currently managed the legal team that is responsible for any legal policy that is related to any issues. This policy includes protecting classified information due to the importance of customer medical data, industry standards of credit card transactions. |
| Physical Security | Detective | Banksia’s physical security’s objective is to detect and records any suspicious physical act. This includes alarms, CCTV cameras.    However, more control is needed by the IS/IT to set up cameras. |
| Data Backups | Recovery | Banksia are aware of the confidentiality of data and their current strategy is to back up files of corporate, partnership and big data of patient/client every month.    However, monthly data backup is considered as not frequent considering the vast data of patient/client. Furthermore, IS/IT team needs to review their backup policy with their other executives. |
| Backup Facility | Compensating | Banksia data centre facility provides redundant back up facility that liked with storage with high speed broadband connections along with RAID removable HDD storage.    However, they must consider physical corrective control if non adversarial events happen or man-made events which could affect loss of physical assets. |
| System Maintenance | Recovery | This refers to the ability of the IS/IT team to recover from system or portal breakdown.    However, Banksia must recognise that having so many system maintenances can lead to operational efficiency and loss of financial and resource (Prananto 2019). |
| Training | Preventive | Banksia’s also carry out training to new employee to understand them how to operate well based on their departments. For example, basic knowledge employee training regarding their security system, standard operating procedure (SOP) and all basic training checklist that new employee needs to learn.    Training that Banksia provided needs to be more detailed in order to carry out the right training policy to handle security of the system and how to tackle problems from internal and external attackers. |
| Access Card | Preventive | Whenever Banksia’s employee needs to come into restricted room, they must tap their access card in order for them to gain access to authorised access only. |
| Humidity Control in Server Room | Preventive | Humidity control in server room detects and controls humidity ensuring the condition of the room supports servers to running functionally. |

## Appendix E Likelihood, Impact and Risk Determination

### Table E. 1. Assessment Scale - Likelihood of Threat Event Initiation (Adversarial)

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | Adversary is almost certain to initiate the threat event. |
| High | Adversary is highly likely to initiate the threat event |
| Moderate | Adversary is somewhat likely to initiate the treat event |
| Low | Adversary is unlikely to initiate the threat event. |
| Very Low | Adversary is highly unlikely to initiate the threat event. |

(NIST 2012, p. G-2)

### Table E.2. Assessment Scale - Likelihood of Threat Event Occurrence (Non-Adversarial)

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year |
| High | Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year. |
| Moderate | Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year |
| Low | Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years. |
| Very Low | Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years. |

(NIST 2012, p. G-2)

### Table E.3. Assessment Scale - Likelihood of Threat Event Resulting in Adverse Impacts

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | If the threat event is initiated or occurs, it is almost certain to have adverse impacts |
| High | If the threat event is initiated or occurs, it is highly likely to have adverse impacts |
| Moderate | If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts. |
| Low | If the threat event is initiated or occurs, it is unlikely to have adverse impacts. |
| Very Low | If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts |

(NIST 2012, p. G-2)

### Table E.4. Assessment Scale - Overall Likelihood

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood of Threat Event Initiation or Occurrence | Likelihood Threat Events Result in Adverse Impacts | | | | |
| **Very High** | **High** | **Moderate** | **Low** | **Very Low** |
| Very High | Low | Moderate | High | Very High | Very High |
| High | Low | Moderate | Moderate | High | Very High |
| Moderate | Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Moderate | Moderate |
| Very Low | Very Low | Very Low | Low | Low | Low |

(NIST 2012, p. G-2)

### Table E.6. Assessment Scale - Impact of Threat Events

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries. |
| Moderate | The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals’ other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries. |
| Low | The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals’ other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Very Low | The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals’ other organizations, or the Nation. |

(NIST 2012, p. H-3)

### Table E.7. Assessment Scale - Level of Risk (Combination of Likelihood and Impact)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
| **Very Low** | **Low** | **Moderate** | **High** | **Very High** |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

(NIST 2012, p. I-1)

### Table E.8. Assessment Scale - Level of Risk

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, and other organizations. |
| High | High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, and other organizations. |
| Moderate | Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, and other organizations. |
| Low | Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, and other organizations. |
| Very Low | Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, and other organizations. |

(Adapted from NIST 2012, p. I-1)

### Table E.9. Identification of Level of Risk

### 

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Identifier | Likelihood of Threat Event Occurrence | Likelihood of Threat Event Resulting in Adverse Impact | Overall Likelihood | Impact | Impact Assessment | Risk Title | Risk Description | Level of Risk |
| Adversarial | | | | | | | | |
| A1 | Very High | Moderate | High | Inability to perform current business function, financial loss, damage to trust relationships and reputation. | Very High | Risk of cyberattacks due to lack of internal cybersecurity controls causing service/business disruption, damage to trust relationship, reputation, and financial loss | Having a weak firewall, system security software or other security controls enables the attacker to place a ransomware to the system which makes system inaccessible, and may cause inability to perform current business function, financial loss, damage to trust relationships and reputation. | Very High |
| A2 | Very High | Moderate | High | Damage to or loss of information assets, privacy breach leading to compliance issues, damage to reputation, damage to trust relationships with patients and partner organizations, potential lawsuits from party whose data is affected, identity theft, sanctions from regulatory bodies due to non-compliance, and financial loss. | Very High | Risk of cyberattacks due to lack of internal cybersecurity controls causing service/business disruption damage to trust relationship, reputation, and financial loss | Adversary inserts malware into internal information systems and information system components specifically targeted to the hardware, software, and firmware used by authorised users, causing damage to or loss of information assets, privacy breach leading to compliance issues, damage to reputation, damage to trust relationships with patients and partner organizations, potential lawsuits from party whose data is affected, identity theft, sanctions from regulatory bodies due to non-compliance, and financial loss. | Very High |
| A3 | High | High | High | Unauthorised access to systems which may lead to data/identity theft, damage to or loss of information assets causing inability to deliver service in a sufficiently timely manner, disruption to service delivery may cause damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party, and financial and reputational damage due to legal actions. | Very High | Risk in reputational damage, financial costs, and failing to comply due to cyberattacks | Adversary targets multiple organizations that are connected to acquired specific information. Such campaign causes data theft, disclosure of sensitive/confidential data, damage to or loss of information assets, damage to reputation, lawsuits from affected party, and financial and reputational damage due to legal actions. | Very High |
| A4 | High | High | High | Damage to or loss of information assets, damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party whose data is leaked, and financial and reputational damage due to legal actions. | Very High | Risk in disruption of service and damage/loss of data and financial loss due to cyberattack. | Adversary deploys attack that exploits as yet unknown to or unaddressed by those who should be interested in mitigating the vulnerability. The attacks are based on adversary insight into the organizational information systems and adversary reconnaissance of organizations. This may result in damage to or loss of information assets, damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party, and financial and reputational damage due to legal actions. | Very High |
| A5 | Low | High | High | Damage to or loss of information assets, privacy breach causing issue on compliance, damage to trust relationships between organizations and patients, damage to reputation, and potential lawsuits from patient whose data is stolen and financial loss. | Very High | Risk of cyberattacks due to lack of IS/IT governance on monitoring activities causing damage or loss in data, trust relationships, reputation, and legal and compliance issue. | Lack of IS/IT governance on internal system maintenance (e.g. software patching solution) leads to system and data breach by adversary causing adversary may damage or steal organizational data that may result in damage to or loss of information assets, privacy breach causing issue on compliance, damage to trust relationships between organizations and patients, damage to reputation, and potential lawsuits from patient whose data is stolen and financial loss. | Very High |
| A6 | Very High | Moderate | High | Inaccessible systems, disruption of operations to Banksia as affected third parties are unable to provide data instantly, data theft or data loss, damage to trust relationships between patients and organizations, damage to reputation, and financial loss. | Very High | Risk of disruption of service, damage to reputation and financial loss due to absent/lenient IS/IT governance on implementation of security controls by third-party on their systems. | Since there is no evidence on IS/IT governance on implementation of security controls on third-party systems, including backup data service provider, external API-connected systems, overseas radiology centre and medical partner organizations, their systems may be inaccessible due to ransomware causing disruption of operations to Bankia, data theft or data loss, damage to trust relationships and reputation, and financial loss. | Very High |
| A7 | Moderate | High | Moderate | Inability to carry out missions or  business functions in a sufficiently timely manner and disruption to delivery of service in, which may cause damage to trust relationships with patients and partner organizations. | Very High | Risk of destruction of critical systems components or functions resulting in inability to perform business functions, disruption of service and damage to trust relationships | Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions and disruption to delivery of service in a sufficiently timely manner, which may cause damage to trust relationships with patients and partner organizations. | High |
| A8 | Very High | Low | Moderate | Damage to or loss of information assets, privacy breach causing issue of compliance, and damage to trust relationships between organizations and patients, damage to reputation | Very High | Risk of damage or loss of information assets, privacy breach, service disruption due to adversarial internal breach via physical access | Due to lack of internal cybersecurity controls/initiative, adversary breach internal system via physical access (e.g. plugging malicious USB to desktop, gaining unauthorised access to server room) and tampering or stealing sensitive/confidential organizational data. Such act may result in damage to or loss of information assets, privacy breach causing issue on compliance, and damage to trust relationships between organizations and patients, damage to reputation and financial loss. | High |
| A9 | High | Moderate | Moderate | Inability to perform business functions in a sufficiently timely manner, disruption of service which may damage trust relationships and reputation, data theft, potential legal lawsuit from parties whose data is affected, and financial loss. | Very High | Risk of cyberattacks due to lack of internal cybersecurity controls causing service/business dysfunction damage to trust relationship, reputation, and financial loss | Cyber adversary use multiple compromised devices/systems to attack a single target, thus cause denial of service for users of the targeted devices/systems, causing inability to perform business functions in a sufficiently timely manner, disruption of service which may damage trust relationships and reputation, data theft, potential legal lawsuit from parties whose data is affected, and financial loss. | High |
| A10 | Low | High | Moderate | Damage to organizational reputation, damage to trust relationships between patients and partner organizations, financial costs if incident resulting in lawsuits against the organization, and sanctions by regulatory body for failure to comply. | Very High | Risk in reputational damage, financial costs, and failing to comply due to disclosure of sensitive/confidential information | Adversary with authorised access to systems inadvertently expose, disclose or mishandle sensitive/confidential information. Such incident may result in damage to organizational reputation, damage to trust relationships between patients and partner organizations, financial costs if incident resulting in lawsuits against the organization, and sanctions by regulatory body for failure to comply. | High |
| A11 | Very High | Low | Moderate | Unauthorised access which may lead to data/identity theft, damage to or loss of information assets causing inability to deliver service in a sufficiently timely manner, disruption to service delivery may cause damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party, and financial and reputational damage due to legal actions. | Very High | Risk in reputational damage, financial costs, and failing to comply due to cyberattacks | Adversary establish communication channel to the organization or targeted information system through brute force login or numerous password guessing attempts. Such attack may result in unauthorised access, data/identity theft, damage to or loss of information assets causing inability to deliver service in a sufficiently timely manner, disruption to service delivery may cause damage to trust relationships with patients and partnered organizations, damage to or loss to information systems or networks, lawsuits from affected party, and financial and reputational damage due to legal actions. | High |
| A12 | Moderate | Moderate | Moderate | Damage to or loss of information assets, damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party whose data is leaked, and financial and reputational damage due to legal actions. | Very High | Risk in reputational damage, financial costs, and failing to comply due to cyberattacks | Adversary steals confidential/sensitive information through unauthorised access. This may result in damage to or loss of information assets, damage to trust relationships with patients and partnered organizations, damage to or loss to information systems or networks, lawsuits from affected party, and financial and reputational damage due to legal actions. | High |
| A13 | High | Low | Moderate | Damage to or loss of information assets, damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party whose data is leaked, and financial and reputational damage due to legal actions. | Very High | Risk in reputational damage, financial costs, and failing to comply due to cyberattacks | Adversary hijacks already established, legitimate information system sessions between organizations and third parties (e.g. users connecting from remote location), causing data theft, damage to or loss of information assets, which can cause disclosure of confidential | High |
| A14 | Moderate | High | Moderate | Breach or theft of sensitive/confidential information which may negatively affect company's reputation. | Very High | Risk of cyberattacks targeting employees lacking knowledge of safe security practices causing damage to or loss of information assets, and reputation | Without guidelines nor training on cybersecurity awareness, employees may be unaware of adversary counterfeiting communications from a legitimate source to gain access to sensitive/confidential information. For example, a phishing email may be sent instructing recipients to open websites that appear to be legitimate while actually stealing the entered information. Such attack may cause damage to or loss of information assets and damage to reputation. | High |
| A15 | Moderate | High | Moderate | Damage to or loss of information assets, damage to trust relationships causing reputational damage, lawsuits from affected party, and financial damage due to legal actions. | Very High | Risk of cyberattacks to employees due to lack of knowledge of safe security practices, causing breach of highly sensitive data and damage to reputation | Adversary deploys phishing attacks to high value targets, such as senior executive management, who lacks in proper security practices. Such action causes damage to or loss of information assets, damage to trust relationships causing reputational damage, lawsuits from affected party, and financial damage due to legal actions. | High |
| A16 | Moderate | Low | Low | Data theft, damage to or loss of information assets, damage to or loss of equipment, disclosure of sensitive/confidential data, thus causing damage to organizational reputation, damage to trust relationships, increase in legal costs if affected party pursues legal action and issue to being non-compliant. | High | Risk in data theft or loss that may cause legal, financial and reputational damage, due to split tunnelling | Adversary exploits external organizational information systems (e.g. laptops at remote locations) that are simultaneously connected securely to organizational internal information systems or networks and to non-secured remote connection. Such incident may result in data theft, damage to or loss of information assets, damage to or loss of equipment, disclosure of sensitive/confidential data, thus causing damage to organizational reputation, damage to trust relationships, increase in legal costs if affected party pursues legal action and issue to being non-compliant. | High |
| A17 | Moderate | Very High | High | Damage to or loss of information assets, data theft, damage to trust relationships between patients and partner organizations, damage to reputation, and financial loss. | High | Risk in data theft, reputational damage and financial loss due to cyberattacks by insider adversary | Increasing system access and number of devices causes more probability of insider attacks, where the organization's data, processes and assets are compromised due to adversarial actions of users. This may result in damage to or loss of information assets, data theft, damage to trust relationships between patients and partner organizations, damage to reputation, and financial loss. | High |
| A18 | High | Moderate | Moderate | Damage to or loss of information assets, privacy breach leading to compliance issues, damage to reputation, damage to trust relationships with patients and partner organizations, potential lawsuits from party whose data is affected, identity theft, sanctions from regulatory bodies due to non-compliance, and financial loss. | Very High | Risk of cyberattacks on third-party systems due to lack of governance on third-party security causing data breach, damage to trust relationships, non-compliance with regulations and financial loss | Third-party data backup facility was appointed without proper assessment on security controls. Thus, adversary may use common communication mechanisms to install known malware into the backup system causing damage to or loss of information assets, privacy breach leading to compliance issues, damage to reputation, damage to trust relationships with patients and partner organizations, potential lawsuits from party whose data is affected, identity theft, sanctions from regulatory bodies due to non-compliance, and financial loss. | High |
| A19 | High | Moderate | Moderate | Privacy breach, non-compliance issue, damage or loss of information assets, damage to trust relationships between organizations and patients, damage to reputation. | Very High | Risk of data theft via third-party operations due to lack of cyber security controls/initiatives | Data theft by dishonest authorised users of third-party partner organizations or vendors causing privacy breach causing issue of compliance, and damage to trust relationships between organizations and patients, damage to reputation. | High |
| A20 | Moderate | High | Moderate | Damage to or loss of information assets, privacy breach causing issue of compliance, and damage to trust relationships between organizations and patients, damage to reputation | High | Risk of damage or loss of information assets, privacy breach, service disruption due to system breach at third party facility | Adversary breaches internal system via physical access at third-party facility (e.g. plugging malicious USB to desktop, gaining unauthorised access to server room) and tampers/steals sensitive/confidential organizational data, which may be Banksia's patient data. Such act may result in damage to or loss of information assets, and damage to trust relationships between organizations and patients, damage to reputation and financial loss, privacy breach causing issue on compliance, and non-compliance can lead to fines/suspension/cancelation of facility by governing body, | High |
| A21 | Very High | Low | Moderate | Damage to organizational reputation, damage to trust relationships between patients and partner organizations, financial costs if incident resulting in lawsuits due to lack of due diligence on third party by Banksia, and issue to compliance. | Very High | Risk in damaging trust relationships and organizational reputation, increased legal costs, non-compliance issue due to disclosure of sensitive/confidential information via third-party | Adversary with authorised access to systems inadvertently expose, disclose or mishandle sensitive/confidential information. Such incident may result in damage to organizational reputation, damage to trust relationships between patients and partner organizations, financial costs if incident resulting in lawsuits due to lack of due diligence on third party by Banksia, and issue to compliance. | High |
| A22 | Very High | Low | Moderate | Inability to perform business functions in a sufficiently timely manner, which leads to disruption of service of Banksia whose systems are connected with the third parties. Such incident may damage trust relationships and reputation, data theft, potential legal lawsuit from parties whose data is affected, and financial loss. | Very High | Risk of cyberattacks due to lack of   cybersecurity controls of third-party systems causing service/business dysfunction damage to trust relationship, reputation, and financial loss | Due to limited security controls of third-party systems and infrastructure, adversary use multiple compromised devices/systems to attack a single target, thus cause denial of service for users of the targeted devices/systems, causing inability to perform business functions in a sufficiently timely manner, which leads to disruption of service of Banksia whose systems are connected with the third-parties. Such incident may damage trust relationships and reputation, data theft, potential legal lawsuit from parties whose data is affected, and financial loss. | High |
| A23 | High | High | High | Data theft, unauthorised access to internal system, disclosure of sensitive data, loss of physical assets, potential lawsuit from affected party, breach of customer privacy which can lead to non-compliance, non-compliance can result in severe fines, suspension or cancellation of facility. | Moderate | Risk in unauthorised access and data theft/loss, non-compliance due to delay in responding to an incident | Due to delay in reporting an incident, e.g. stolen or missing laptop, adversary already gains unauthorised access to the device which can result in data theft, unauthorised access to internal system, disclosure of sensitive data, loss of physical assets, potential lawsuit from affected party, breach of customer privacy which can lead to non-compliance, non-compliance can result in sever fines, suspension or cancellation of facility. | High |
| A24 | Moderate | High | High | Damage to organizational reputation, damage to trust relationships between patients and partner organizations, financial costs if incident resulting in lawsuits due to lack of due diligence on third party by Banksia, and breach of compliance. | High | Risk of disruption of service, damage to reputation and financial loss due to poorly assessed data backup service provider in implementation of control. | Adversary exploits backup data facility to inadvertently expose, disclose or mishandle sensitive/confidential information. Such incident may result in damage to organizational reputation, damage to trust relationships between patients and partner organizations, financial costs if incident resulting in lawsuits due to lack of due diligence on third party by Banksia, and issue to compliance. | High |
| A25 | Very High | Low | High | Damage to or loss of information assets, privacy breach causing issue of compliance, and damage to trust relationships between organizations and patients, damage to reputation | High | Risk of system or data breach due to malware attack via cloud causing data theft and breach | Due to its connectivity, cloud-based system is used as a point of malware attack for adversary. Once access to internal system is gained, adversary may damage or steal organizational data that may result in damage to or loss of information assets, privacy breach causing issue on compliance, and damage to trust relationships between organizations and patients, damage to reputation. | High |
| A26 | Very High | Low | High | Damage to or loss of information assets, inability to perform current business functions in a sufficiently timely manner, disruption of service which can cause damage to reputation and trust relationships and declined business revenue due to loss in customers/business. | High | Risk of data scavenging attacks in cloud environment resulting in data theft, disruption of business functions and service, damage or loss trust relationships and business loss | Cyber adversary obtains data used and then deleted by organizational processes running in cloud environment, causing damage to or loss of information assets, inability to perform current business functions in a sufficiently timely manner, disruption of service which can cause damage to reputation and trust relationships, and declined revenue due to loss in customers/business. | High |
| A27 | High | Moderate | Moderate | Data theft, damage to or loss in information assets, identity theft causing damage to trust relationships between the organization, patients and partner organizations, damage to reputation and financial loss. | Very High | Risk in cyberattacks due to increased connectivity of internal systems and potentially malicious IoT device causing data theft, damage to trust relationships and reputation and financial loss | A user trying to access internal cloud-based systems from his/her own device that is infected in malware; thus, resulting in attacks in internal system. Unauthorised access created by such attack may result in data theft, damage to or loss in information assets, identity theft causing damage to trust relationships between the organization, patients and partner organizations, damage to reputation and financial loss. | High |
| A28 | Low | Low | Low | Damage to or loss of physical assets, damage to or loss of data, and disruption of service. | Very High | Risk in data theft, data loss, service disruption due to stolen device | Adversary take possession company's devices (e.g. laptop) and gains unauthorised access to organizational information systems, which may cause in damage to or loss of physical assets, damage to or loss of data, and disruption of service. | Moderate |
| A29 | Moderate | Low | Low | Data theft, damage to or loss of information assets causing inability to deliver service in a sufficiently timely manner, disruption to service delivery may cause damage to reputation and trust relationships with patients, damage to or loss to information systems or networks, and financial loss attributed to data loss. | Very High | Risk in data theft, data loss, service disruption due to cyberattacks | Adversary gains access to organization's exposed wired or wireless data channels, such as publicly available Wi-Fi, used to transfer information, uses network sniffing to identify components, resources and protection. Such attack may result in data theft, damage to or loss of information assets causing inability to deliver service in a sufficiently timely manner, disruption to service delivery may cause damage to reputation and trust relationships with patients, damage to or loss to information systems or networks, and financial loss attributed to data loss. | Moderate |
| A30 | Low | Low | Low | Damage to or loss of information assets, privacy breach leading to compliance issues, damage to reputation, damage to trust relationships with patients and partner organizations, potential lawsuits from party whose data is affected, identity theft, sanctions from regulatory bodies due to non-compliance, and financial loss. | Very High | Risk of cyberattacks on third-party systems due to lack of security controls by third party causing data breach, damage to trust relationships, non-compliance with regulations and financial loss | Adversary obtains physical access to organizational information systems of third parties and tampers data. Such incident may result in damage to or loss of information assets, privacy breach leading to compliance issues, damage to reputation, damage to trust relationships with patients and partner organizations, potential lawsuits from party whose data is affected, identity theft, sanctions from regulatory bodies due to non-compliance, and financial loss. | Moderate |
| A31 | Moderate | Moderate | Moderate | Breach of data and customer's privacy that lead to sanctions due to non-compliance, and data theft that may lead to damage or loss to trust relationship with clients, potential lawsuit from patients whose data is stolen, and financial loss. | High | Risk of exploitation on API resulting in privacy breach, harms due to non-compliance, trust relationship damage, financial loss and business loss | API is a channel for third-party application integration allowing communication between systems and access into internal database containing sensitive/confidential information. Adversary finds a loophole in the integration and exploits the communication using different techniques; thus causes breach of data and customer's privacy that lead to sanctions due to non-compliance, and data theft that may lead to damage or loss to trust relationship with clients, potential lawsuit from patients whose data is stolen, and financial loss. | Moderate |
| A32 | Moderate | High | Moderate | Disruption of service resulting in decrease in customer satisfaction, damage to reputation and trust relationships with patients, data theft, damage to or loss in information assets. | Very High | Risk in disruption of service, data theft and los, damage to reputation and trust relationships due to cyberattacks in the supply chain. | Adversary targets and compromises the operation of software (e.g. through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components. Such incident may cause disruption of service resulting in decrease in customer satisfaction, damage to reputation and trust relationships with patients, data theft, damage to or loss in information assets. | Moderate |
| A33 | Moderate | Moderate | Moderate | Loss of physical asset, may result in sensitive data theft, data leakage which may cause disclosure of data, and tampering of data. | Moderate | Risk in data theft/loss/disclosure due to unprotected/low-protected mobile computing device being stolen | Adversary gains possession of organization-owned mobile computing device, e.g. laptop, and easily gains access to data stored in the device due to lack of security control. Such action results in loss of physical asset, may result in sensitive data theft, data leakage which may cause disclosure of data, and tampering of data. | Moderate |
| A34 | Moderate | High | Moderate | Damage to organizational reputation, damage to trust relationships with patients and partner organizations. | High | Risk of cyberattacks on third-party affecting internal systems causes service disruption and damage to or loss of information assets. | Adversary takes advantage of multi-tenancy to observe behaviour of organizational processes, acquire organizational information, or disrupt with the timely or correct functioning of organizational processes. Such incident may cause damage to organizational reputation, damage to trust relationships with patients and partner organizations. | Moderate |
| A35 | Moderate | High | Moderate | Inaccessible system which disrupts delivery or service, damage to organizational reputation, disclosure of data which may lead to lawsuits from affected parties, breach to compliance, non-compliance can lead to sever fines, suspension/cancelation of facility. | High | Risk in cyberattacks due to poor enforcement of cyber security practices | Adversary moves the source of malicious commands or actions from one compromised information systems to another, making analysis difficult. Such attack may result in inaccessible system which disrupts delivery or service, damage to organizational reputation, disclosure of data which may lead to lawsuits from affected parties, breach to compliance, non-compliance can lead to sever fines, suspension/cancelation of facility. | Moderate |
| A36 | High | Low | Moderate | Unauthorised access to internal system, inability to perform current business functions, slowing down in-service delivery that may cause reputational damage, damage to or loss in information assets. | Moderate | Risk of cyberattacks on third-party affecting internal systems causes service disruption. | Adversary launches attack on the infrastructure of contracted Internet Service Provider. Without proper or updated security controls, such incident may result in disruption to operations due to lag/disruption in internet connectivity. | Moderate |
| A37 | Moderate | High | Moderate | Inaccurate/misleading information displayed, damage in trust relationships, damage in organizational reputation. | High | Risk in damaging trust relationships and organizational reputation due to cyberattacks | Unauthorised access to sensitive/confidential information by adversary through publicly available devices. Adversary may create, modify or delete critical data. Such attack may result in unauthorised access, data/identity theft, damage to or loss of information assets causing inability to deliver service in a sufficiently timely manner, disruption to service delivery may cause damage to trust relationships with patients and partner organizations, damage to or loss to information systems or networks, lawsuits from affected party, and financial and reputational damage due to legal actions. | Moderate |
| A38 | Low | Moderate | Low | Process of fraudulent data and compliance breach | Low | Risk in processing fraudulent data and compliance breach due to absence of patient identity authentication | There is no evidence of identity authentication of patient allowing adversary to intentionally record wrong information to systems, or outsiders register with someone else's identity. This situation causes fraudulent medical data processing and may cause compliance breach. | Low |
| A39 | Very Low | Very High | Low | Data theft, disclosure of data, cyberattacks on the system, vandalism of data. All these leads to potential lawsuit from affected party which cause financial and reputational damage, and breach to compliance, non-compliance can lead to sever fines, suspension/cancelation of facility. | High | Risk in cyberattacks due to poor enforcement of cyber security practices | An insider shares password with an adversarial outsider who gains access to the system using he insider's credentials. This threat can lead to data theft, disclosure of data, cyberattacks on the system, vandalism of data. All these leads to potential lawsuit from affected party which cause financial and reputational damage, and breach to compliance, non-compliance can lead to sever fines, suspension/cancelation of facility. | Low |
| A40 | Low | Low | Low | Inability to perform current and/or future business functions of facility located within proximity of the attack. | Moderate | Risk in service disruption due to terrorist attack | Terrorist attack conducted in one of the major Australian cities causing some fatalities and/or injuries or loss of life. Such attack may have impacted inability to perform current and future business functions if any of the facilities is in or within proximity of the incident. | Low |
| A41 | Low | Moderate | Low | Disrupt operations, injury or loss of life, damage to or loss of physical facilities, equipment and infrastructure, damage to or loss of information assets. | High | Risk of physical attacks causing disruption of service, damage/loss physical assets, financial loss, injury or loss of life. | Adversary performs physical attack on organization facilities, e.g. sets a fire, robbery. Physical attacks may disrupt operations, injury or loss of life, damage to or loss of physical facilities, equipment and infrastructure, damage to or loss of information assets. | Low |
| A42 | Low | Low | Low | Discrepancies in recorded payment information, minor loss in business | Very Low | Risk of discrepancy in payment information and business loss due to theft | Insider adversary, e.g. staff handling cash payment, takes advantage of the manual process of cash handling and steal cash payment. Stolen payment causes discrepancies in payment information recorded in the system and loss in business. | Very Low |
| Non-Adversarial | | | | | | | | |
| NA1 | High | High | High | Inaccessible, missing or inaccurate administrative or patient data that leads to disruption in service delivery | Very High | Risk in service disruption and information assets damage due to due to outdated, overdeveloped and over-capacity system | Degraded processing performance to due internal systems depletion. Depletion of internal system may cause disruption to operational activities and damage to or loss of information assets. | Very High |
| NA2 | Very High | Very High | Very High | Disruption of service which may lead to data loss, customer dissatisfaction, damage to organizational reputation, increase financial costs in fixing the system, and loss in business. | Very High | Risk in data loss and disruption of service due to outdated, overdeveloped and over-capacity system | Outdated systems fail to operate due to over-capacity, aging, constant maintenance, and is unable to cope up during peak hours of business operations. System failure causes disruption of service and may lead to data loss, customer dissatisfaction, damage to organizational reputation, increase financial costs in fixing the system, and loss in business. | Very High |
| NA3 | Moderate | Very High | High | Greater damage or loss in information assets, physical assets, physical injuries, and damage to trust relationships which can lead to damage to organizational reputation. | Very High | Risk in damage or loss of data, physical assets, physical injuries and damage to trust relationships and reputation due to delayed response in attending to IS/IT related incident | Without proper Incident Response Plan or Disaster Recovery Plan, can result in lack of response when adverse events occur causing greater damage or loss in information assets, physical assets, physical injuries, and damage to trust relationships which can lead to damage to organizational reputation. | Very High |
| NA4 | Low | Very High | High | Severe fines imposed, lose the ability to accept credit cards, loss of customers due to negative reputation. | Very High | Risk in severe penalties, inability to accept credit card payment and reputational damage due to non-compliance with PCI DSS | There is no evidence that the company is exercising its due diligence in making sure that handling credit card transactions remains compliant. Non-compliance with PCI DSS results in severe fines imposed, lose the ability to accept credit cards, loss of customers due to negative reputation. | Very High |
| NA5 | Very High | Very High | Very High | Loss of information assets, damage to reputation, damage to trust relationships with patients and partner organizations, inability to perform business functions in a timely manner, service disruption, and financial loss due to service disruption. | Very High | Risk in data loss, reputational damage, and service disruption due to failure of data backup | Backup of data is conducted every 30 day instead of instantly once data is written to the system. Interruption/incident may occur between the scheduled backup resulting loss of data, damage to reputation, damage to trust relationships with patients and partner organization, inability to perform business functions in a timely manner, service disruption, and financial loss due to service disruption. | Very High |
| NA6 | Low | High | Moderate | Non-compliant business operations, penalties imposed by regulatory body, suspension or cancellation of facility | Very High | Risk in non-compliance due to mishandling of compliance data requirements | There is limited evidence that the company is exercising its due diligence in making sure that operations and operations of third parties, are compliant with laws and regulations. Non-compliance with standards and regulations may result in severe penalties causing reputational and financial damage, or suspension or cancellation of facility. | High |
| NA7 | Low | High | Moderate | Service disruption, disclosure of sensitive data causing financial and reputational damage, and breach of compliance which may lead to imposed sanctions. | Very High | Risk in service disruption, disclosure of data, financial and reputational damage and non-compliance due to regulations oversight in another jurisdiction. | Overseas third-party fails to comply with governing bodies regulations or change in regulations within their country in handling sensitive medical data causing service disruption, disclosure of sensitive data causing financial and reputational damage, and breach of compliance which may lead to imposed sanctions. | High |
| NA8 | High | High | High | Issues to integration, creation of silos of data operation causing inefficiency in performing business functions | High | Risk in system integration and creation of silos of data due to unauthorised IS/IT procurement by individual business unit | Unauthorised purchase of IS/IT related procurement by other department that does not adhere to the IS/IT governance, causing disintegrated system which may create silos of data operation causing ineffective business functions. | High |
| NA9 | High | High | High | Increases the chances of cyberattacks to system which may result in disclosure of sensitive/confidential information, loss of information assets, disruption of service, reputational and financial damage, non-compliance in handling data, imposed fines or suspension/cancellation of facility by regulatory body | High | Risk in data loss, disruption of service, financial and reputational damage and non-compliance due to improper implementation of IS/IT governance | Without following IS/IT governance in third-party vendor selection, direct appointment of data backup provider is not properly assessed in handling data that contains confidential/sensitive information. For example, the facility may lack proper security controls. Skipping this activity increases the chances of cyberattacks, which may result in disclosure of sensitive/confidential information, loss of information assets, disruption of service, reputational and financial damage, non-compliance in handling data, imposed fines or suspension/cancellation of facility by regulatory body due to non-compliance. | High |
| NA10 | High | Low | Moderate | Loss of information assets, disruption of service, reputational and financial damage, non-compliance in handling data, imposed fines by regulatory body and potential business shutdown due to non-compliant. | Very High | Risk in data loss, reputational and financial damage, and non-compliance due to inexperienced data backup provider in handling crisis/incident. | Hiring a start-up data backup service provider can put the data at risk as they would not know what to do in a crisis situation that jeopardizing data security. This may lead to loss of information assets, disruption of service, reputational and financial damage, non-compliance in handling data, imposed fines or suspension/cancellation of facility by regulatory body due to non-compliance. | High |
| NA11 | High | High | High | Incorrect processing of patient data, damage to trust relationships with patients which leads to damage to organizational reputation, and financial loss. | High | Risk in business loss and reputational damage due to limited monitoring activities on offshore third-party in handling data | Limited evidence in governance on monitoring third-party radiology centre in handling radiology images, causing incorrect processing of patient data, damage to trust relationships with patients which leads to damage to organizational reputation, and financial loss. | High |
| NA12 | High | High | High | Loss of revenue, non-compliance with regulatory bodies, mishandling of customer information, legal action | High | Risk in contractual breach due to lack of governance framework in monitoring third-party vendors performance, causing mishandling of data which lead to non-compliance. | Limited evidence of due diligence performed by IS/IT department in monitoring performance of third-party vendors, which resulting in contractual breach. Breach of contract may involve improper handling of patient data which may cause issue in non-compliance with Privacy Act, which potentially leads to imposed fines or suspension/cancellation of facility by regulatory body | High |
| NA13 | Low | Very High | Moderate | Inoperable facility, damage to or loss of information and physical assets, injury or loss of life, disruption of service and financial loss. | Very High | Risk of natural or man-made disaster at facility causing damage to or loss of information and physical assets, injury or loss of life, disruption of service and financial loss. | Non-adversarial fire incident at main or backup facility causes inoperable facility or destroys backups of data, software, configurations and/or logs, injury or loss of life, disruption of service and financial loss. | High |
| NA14 | High | High | High | Slow delivery of service, limited ability to perform business function, and ineffective employee performance. | Moderate | Risk in ineffective business function and employee performance due to lack of desirable functionalities in current system | The internal system is outdated and thus, lacks some functionalities that are desirable for more effective service delivery, such as sending automatic reminders to patient. Absence of such functionality may lead to slow delivery of service, limited ability to perform business function, and ineffective employee performance. | Moderate |
| NA15 | High | High | High | Disruption to service, extended waiting time to process data, thus may lead to customer dissatisfaction. | Moderate | Risk in ineffective business function, customer dissatisfaction, and reputational damage due to non-functional system. | IS/IT department or contracted third-party vendor for system maintenance perform constant system maintenance needed to ensure systems are running properly during peak business hours causes disruption to service, extended waiting time to process data, thus may lead to customer dissatisfaction. | Moderate |
| NA16 | High | High | High | Disruption in service delivery, which may result in customer dissatisfaction, damage to reputation and inefficient work performance of employees. | Moderate | Risk in ineffective business function, customer dissatisfaction, and reputational damage due to non-functional system. | Functional speed of internal systems is deteriorated due to over-development and over-capacity internal systems causing disruption in service delivery, which may result in customer dissatisfaction, damage to reputation and inefficient work performance of employees. | Moderate |
| NA17 | Moderate | High | Moderate | Data and identity theft if fail to the hand of adversary, damage to trust relationships with patients which causes damage to reputation, potential lawsuit by affected party which increase legal costs, and potential breach to the Privacy Act which may result in sanctions or business shutdown. | High | Risk in data/identity theft, damage to trust relationships/reputation, breach of compliance due to mishandling of data by improperly trained authorised employees. | Authorised users, e.g. employees, inadvertently expose critical/sensitive information due to lack of knowledge in handling data. For example, employee accidentally sends an email containing confidential information to a wrong recipient. Such incident may lead to data and identity theft if falls to the hand of adversary, damage to trust relationships with patients which causes damage to reputation, potential lawsuit by affected party which increase legal costs, and potential breach to the Privacy Act which may result in sanctions or business shutdown. | Moderate |
| NA18 | Moderate | High | Moderate | Data theft, damage to or loss of information assets, damage to trust relationships with patients which causes damage to reputation, potential lawsuit by affected party which increase legal costs, and potential breach to the Privacy Act which may result in sanctions/fines or business shutdown. | High | Risk in data theft/loss, reputational and financial damage, and non-compliance due to spill of sensitive information by improperly trained employee | Authorised employee erroneously contaminates information system, device or network by placing on it, or exposing sensitive/confidential information. The information is exposed to access by unauthorised individual and causing the device/network/system to become unavailable until the spill is investigated and mitigated. Such incident may result in data theft, damage to or loss of information assets, damage to trust relationships with patients which causes damage to reputation, potential lawsuit by affected party which increase legal costs, and potential breach to the Privacy Act which may result in sanctions/fines or business shutdown. | Moderate |
| NA19 | Moderate | High | Moderate | Data loss and disruption of service | Moderate | Risk in data loss and disruption of service due to employee negligence | Employees accidentally damage hardware, equipment, component parts or other physical assets that are used to manage organizational data, causing data loss and disruption of service. | Moderate |
| NA20 | Moderate | High | Moderate | Increased network architecture exposure to cyber adversary activities which may result in disclosure of confidential information, data theft, damage to or loss in information assets, reputational and financial damage, non-compliance in handling data, imposed fines by regulatory body, and potential suspension or cancellation to facility due to non-compliance. | Moderate | Risk of cyberattacks to systems due to unauthorised download and/or install of non-approved software in company's devices | No evidence of IS/IT governance on use of company's devices resulting in employees to download and install non-approved software/applications, causing increased network architecture exposure to cyber adversary activities. Once infected, it may cause disclosure of confidential information, data theft, damage to or loss in information assets, reputational and financial damage, non-compliance in handling data, imposed fines by regulatory body potential suspension or sanctions or suspension/cancellation of facility. | Moderate |
| NA21 | Moderate | High | Moderate | Data and identity theft if falls to the hand of adversary, damage to trust relationships with patients which causes damage to reputation, potential lawsuit by affected party which increase legal costs, and potential breach to the Privacy Act which may result in imposed fines or suspension/cancellation of facility by regulatory body. | High | Risk in data/identity theft, damage to trust relationships/reputation, breach of compliance due to mishandling of data by improperly trained authorised employees of third parties. | Authorised users of third-party, e.g. employees, inadvertently expose critical/sensitive information due to lack of knowledge in handling data. Such incident may lead to data and identity theft if falls to the hand of adversary, damage to trust relationships with patients which causes damage to reputation, potential lawsuit by affected party which increase legal costs, and potential breach to the Privacy Act which may result in sanctions or suspension/cancellation of facility. | Moderate |
| NA22 | Moderate | Moderate | Moderate | Increased exposure of internal information systems to cyberattacks | Moderate | Risk in increasing exposure to cyberattacks due to inherent vulnerabilities into software products | Inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into the commonly used off-the-shelves software products which are used by the organization to perform business functions. Due to this, software products can increase exposure of internal information systems to cyberattacks. | Moderate |
| NA23 | Moderate | Moderate | Moderate | Misdiagnosis that can be fatal to patient's health and well-being, lawsuit from affected patient that cause damage to reputation and financial loss. | Moderate | Risk in misdiagnosis of sample, business loss and reputational damage due to error in equipment. | Non-adversary incorrect patient sample analysis report due to defect in the functionality of the Haematology Analyser System. Incident may lead to misdiagnosis that can be fatal to patient's health and well-being, potential lawsuit from affected patient may cause damage to reputation and financial loss., damage to trust relationship with client. | Moderate |
| NA24 | Moderate | Moderate | Moderate | Misdiagnosis of laboratory results, missing patient data which may lead to damage to trust relationships with client, damage business reputation, and financial loss. | Moderate | Risk in business loss and reputational damage due to manual process in handling data | Non-adversarial human error during manual labelling process of samples causing incorrect labelling of sample container. That may result in inaccurate diagnosis of laboratory results, missing patient data which may lead to damage to trust relationships with client, damage business reputation, and financial loss. | Moderate |
| NA25 | Moderate | Moderate | Moderate | Misdiagnosis that can be fatal to patient's health and well-being, lawsuit from affected patient that cause damage to reputation and financial loss. | Moderate | Risk in business loss and reputational damage due to manual process in handling data | Non-adversarial human error in manual laboratory report production resulting in accurate report/laboratory results, which may lead to misdiagnosis that can be fatal to patient's health and well-being, potential lawsuit from affected patient may cause damage to reputation and financial loss., damage to trust relationship with client. | Moderate |
| NA26 | Moderate | Moderate | Moderate | Misdiagnosis that can be fatal to patient's health and well-being, lawsuit from affected patient that cause damage to reputation, increased legal costs, and loss of business. | Moderate | Risk in business loss and reputational damage due to manual process in handling data | Non-adversarial human error in during sample processing causing mishandle of patient information by inputting patient data into the system incorrectly. Such incident may result in misdiagnosis of laboratory results, missing patient data which may lead to damage to trust relationships with client, damage business reputation, and financial loss. | Moderate |
| NA27 | Low | High | Moderate | Data loss and disruption of service | Moderate | Risk in data loss and disruption of service due to employee negligence | Employees accidentally damage hardware, equipment, component parts or other physical assets at third-party facilities that are used to manage organizational data, causing data loss and disruption of service. | Moderate |
| NA28 | Low | High | Moderate | Non-compliant business operations, penalties imposed by regulatory body, business shutdown | High | Risk in non-compliance due to mishandling of compliance data requirements | There is no evidence that the company is exercising its due diligence in making sure interchange and interconnectivity with government systems are always in compliant with the standards and regulations. Non-compliance may result in penalties or suspension or cancelation of facility. | Moderate |
| NA29 | Moderate | High | Moderate | Damage to or loss of information technology or equipment, damage or loss of information assets if data on the hardware is not backed up in time, inability to perform business functions in a sufficiently timely manner, and service disruption which may cause damage to reputation. | Low | Risk in hardware failure during operations due to lack of governance in hardware maintenance causing damage on equipment, loss of data and disruption of service | Hardware, such as servers, analyser systems, individual desktops, are not regularly maintained as there is no evidence on IS/IT governance on hardware maintenance. Irregular maintenance of hardware leads to devices operating ineffectively or fail to operate during operations resulting in inability to perform business functions in a sufficiently timely manner, and service disruption which may cause damage to reputation. | Low |
| NA30 | Moderate | Moderate | Moderate | Damage to or loss of information assets. | Low | Risk in damage or loss of information assets due to disk error | Corrupted storage due to disk error of aged or depleted computing hardware, causing damage to or loss of information assets. | Low |
| NA31 | Low | High | Moderate | Disruption of service which may lead to data loss, customer dissatisfaction, damage to organizational reputation, increase financial costs in fixing the system, and loss in business. | Low | Risk in data loss and disruption of service due to system failure | Due to frequent use, the Haematology Analyser System fails to function during peak business hours. System failure causes disruption of service and may lead to data loss, customer dissatisfaction, damage to organizational reputation, increase financial costs in fixing the system, and loss in business. | Low |
| NA32 | Moderate | High | Moderate | Delay in operations and service delivery that may affect negatively on customer satisfaction. | Low | Risk of delay in operations and service delivery and low customer satisfaction due to interruption of internet connection. | Non-adversarial activities by contracted Internet Service Provider causing disruption to system connectivity to the cloud thus disabling access to the internal systems. This causes delay in operations and service delivery that may affect negatively on customer satisfaction. | Low |
| NA33 | Low | High | Moderate | Disruption to service, inability to perform current business functions (data processing). | Low | Risk of service disruption due to hardware failure at third-party facility | There is no evidence that regular hardware maintenance is performed by third-party organizations, which may result in hardware failure that impacts service delivery and data processing ability of Banksia's operations. | Low |
| NA34 | Low | Moderate | Low | Injury, delayed operations, loss of patient information, lengthy investigation process, increase in insurance premiums | Moderate | Risk of road incidents causing loss of data and delay in laboratory report production | Non-adversarial road incident during sample transfer leading to injury of driver, loss of collected samples causing delay in data processing or laboratory report production and lengthy investigation process. | Low |
| NA35 | Low | High | Moderate | Non-adversarial unauthorised access and disclosure of data to unauthorised users. | Low | Risk of unauthorised access or disclosure of data due to error in privilege settings | Authorised privileged administrator or user inadvertently assigns a user exceptional settings or set privilege requirements on a resource low, causing non-adversarial unauthorised access and disclosure of data to unauthorised users. | Low |
| NA36 | Low | Low | Low | Disruption to operations, damage to hardware | High | Risk of inoperable hardware due to infrastructure failure/outage causing disruption to operations | Electricity outage at main or backup facility causing operational disruption of hardware which rely on electricity to function normally (e.g. servers, desktops, analyser system) in processing data. Outage may result in inoperable hardware, inoperable facility and damage to physical assets. | Low |
| NA37 | Very Low | High | Low | Inoperable facility, damage to or loss of information and physical assets, personnel injury, disruption of service and financial loss. | High | Risk of natural or man-made disaster at facility causing inoperable facility, damage to or loss of information and physical assets, personnel injury, disruption of service and financial loss. | Non-adversarial flood incident at main and backup facility causes inoperable facility or destroys backups of data, software, configuration and/or logs, causing disruption to operations, personnel injury, damage to or loss of physical assets and financial loss. | Low |
| NA38 | Very Low | Very High | Low | Inability to perform current mission/business functions, injury or loss of life, damage to or loss of physical facilities and equipment, and financial loss. | Very High | Risk of natural disaster affecting one or more facilities causing service disruption, injury or loss of life, damage to physical equipment and financial loss | Earthquake at a large magnitude affect the laboratories causing inability to perform current mission/business functions, injury or loss of life, damage to or loss of physical facilities and equipment, and financial loss. | Low |

## Appendix F Control Implementation

Table F.1. Cost Benefit Analysis and Imp

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat | Control | Cost of exposure | Cost of Control | Who's Responsible for implementing the control | Time Frame within which the control should be implemented |
| Adversarial Cyber Attack | Setup a VPN so that only authorized users can access the system | High | Low | Networking Specialist | Immediate |
| Adversarial Cyber Attack | Setup access control and monitor employee activity | High | Low | System Administrator | Immediate |
| Adversarial Cyber Attack | Train employees regularly with best security practices | High | Medium | Training Provider | Within few weeks |
| Adversarial Cyber Attack | Encrypt all the data that is backed up | High | Low | Data Backup Provider | Immediate |
| Adversarial Cyber Attack | Hire a team to monitor all the data that goes in and comes out of the system | High | High | IT Manager | 1 to 2 months |
| Adversarial Cyber Attack | Hire an individual after security clearance to handle the system from client side | High | High | IT Manager | 1 to 2 months |
| Performance Degradation and Data Loss due to legacy system | Upgrade the system with current technology and requirements | High | High | Software Development Company | 1 to 3 months |
| Performance Degradation and Data Loss due to legacy system | Upgrade the hardware of the system to improve the performance | High | Low | IT Manager | 1 months |
| Performance Degradation and Data Loss due to legacy system | Increase the frequency of backup | High | Low | Data Backup Provider | Immediate |
| Performance Degradation and Data Loss due to legacy system | Use modernized approaches which keeps the legacy architecture to upgrade the system | High | Medium | Software Development Company | 1 to 3 months |
| System and data breach on irregularly maintained system | Communicating and share knowledge regarding the information security | High | Low | IT Manager | Immediate |
| System and data breach on irregularly maintained system | 24/7 IRP (Incident Response Plan) | High | Low | Software Developer, IT Help Desk | Immediate |
| System and data breach on irregularly maintained system | Disaster Recovery Plan (DRP) | High | Low | IT Manager | Immediate |
| System and data breach on irregularly maintained system | Data warehouse | High | Medium | Data Warehouse Developer | 2-4 Weeks |
| System and data breach on irregularly maintained system | Create own backup as well instead of just inside the cloud | High | Medium | Banksia IS/IT department | Every two weeks |
| System and data breach on irregularly maintained system | Audit on how the provider will receive, validate and report the data back to Banksia | High | Low | IT Manager | Immediate |
| System and data breach on irregularly maintained system | Contractual Agreement with Third Party | High | Low | Senior Executive | Immediate |
| System and data breach on irregularly maintained system | Employee access control to prevent employee from other departments access other information that is not appropriate for the job function | High | Low | IT Officer | Immediate |