GOOD BOOST

Technology Risk Case Report & Log (#GBP026)

Reviewed: 18th December 2023
Next review: 18th June 2024
Reviewed by: Alex Georgiou

Document Control

Organisation	Good Boost Wellbeing Ltd
Title	Technology Risk Case Report & Log – GBP026
Author	Alex Georgiou
Owner	Alex Georgiou – Chief Technical Officer (CTO) & Data Protection Officer (DPO)
Review date	18/12/2023

Document Approvals

This document requires the following approvals:

Sponsor Approval	**Name**	**Date**
CEO / CSO	Ben Wilkins	18/12/2023

Table of Contents

1.0 Introduction and Purpose

1.1 Good Boost's technology risk management plan provides the process that identifies information technology associated risk on an ongoing basis, documents identified risks and the response to them the organisation expects. A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's and/or organisations objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with technology will be identified, analysed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritising risks.

The Risk Management Plan is created by the Data Protection Officer (DPO) / Technology Director, is informed and updated by the Clinical Safety Officer (CSO) and is monitored by responsible technology and engineering team members. The intended audience of this document is the technology staff and the wider team for full awareness.

Good Boost's Technology Risk Management plan exists to identify risk within our technology infrastructure, architecture and operation and create plans, actions and protocol to mitigate risk. Furthermore, it is used to monitor and control risk in an effective manner.

The key risks include:

- User suitable technology design
- Clean Code (bug minimisation)
- Version Control
- Malware Attacks / Hacking
- Disaster Recovery

1.2 Process

The DPO / Technology Director and the CSO will ensure that risks are actively identified, analysed, and managed throughout the life of the IT resources. Risks will be identified as early as possible to minimize their impact. The steps for accomplishing this are outlined in the following sections. The IT manager responsible for a service will serve as the responsible party for addressing risk in their services

1.3 Risk Identification

Risk identification involves the technology leadership (DPO/CSO), appropriate stakeholders, and will include an evaluation of the risks related to the Good Boos technology infrastructure, architecture and operation. The identification effort will take place annually. A Risk Register will be generated and updated as needed and will be stored electronically by the DPO.

1.3.1 Three elements of Risk

Good Boost's technology and the processes to deploy them for customer use them are a vital part of the ongoing mission of the organisation and its business goals and objectives. The following describes these three elements in more detail:

Threats – threats can be both internal to the organisation and external, and come in many different forms. The common element is they work against the confidentiality, integrity, security and availability of technology, or compromise its function. Some possible threats would be the alteration of data or system, or release of protected information, whether intentional or unintentional. Others would be competitors, hackers and other cyber criminals, acts of terrorism, viruses and malware to names a few.

Vulnerabilities – Vulnerability are weaknesses or ‘holes’ in information and technology resources and processes which allow the potential for unauthorised or unintentional change or manipulation of resources which impacts the confidentiality, integrity, security and availability of these technology resources.

Impacts – Impacts are the costs associations with failure in protecting the confidentiality, integrity, security and availability of technology resources. These costs can be increased expenses or outflows (fines, work house, equipment replacements, legal fees etc) or decreased revenues due to inability to deliver organisational products and services or negative publicity.

The threats, vulnerabilities and impacts to information resources are not constant and will change over time. Because of this, the threats to vulnerability of the overall impact of every technology resources must be evaluated and re-evaluated on a regular basis to ensure the ongoing risks are continuously managed.

1.4 Quantitative Estimation of Technology Risk

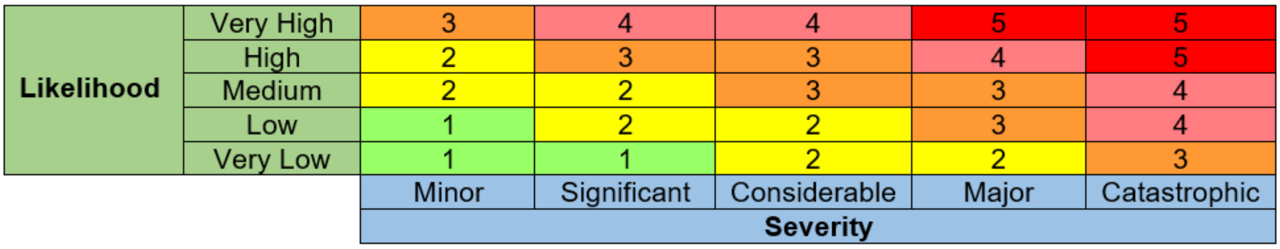
Estimation of technology risk uses criteria specified below that includes:

- Severity of the hazard
- Likelihood of the hazard
- The resulting clinical risk

To estimate the technology risk a Technical Risk Matrix has been applied to quantify the total risk and the risk acceptability definitions suitably evaluate and respond to each risk.

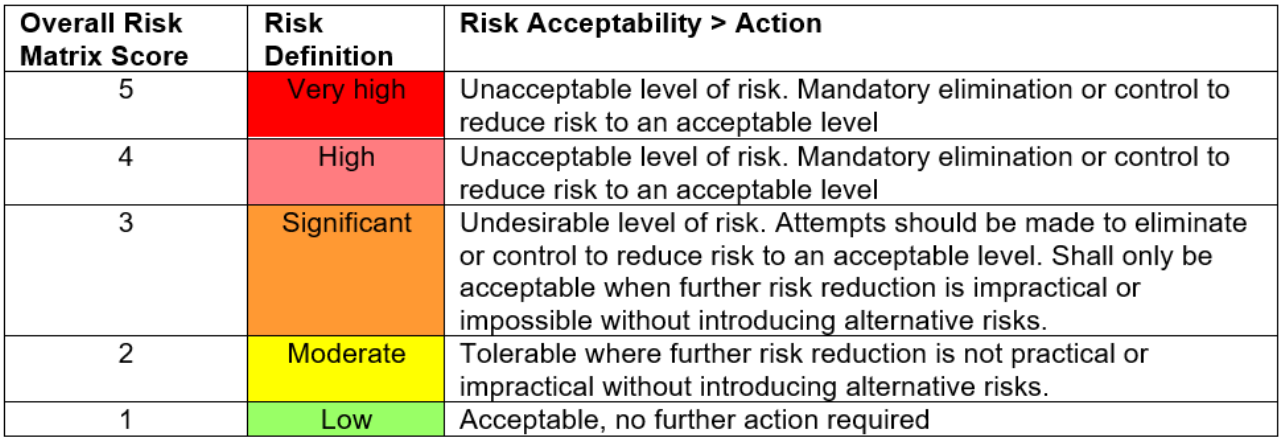
The Technology Risk Matrix and scoring criteria are displayed below

Technology Risk Matrix



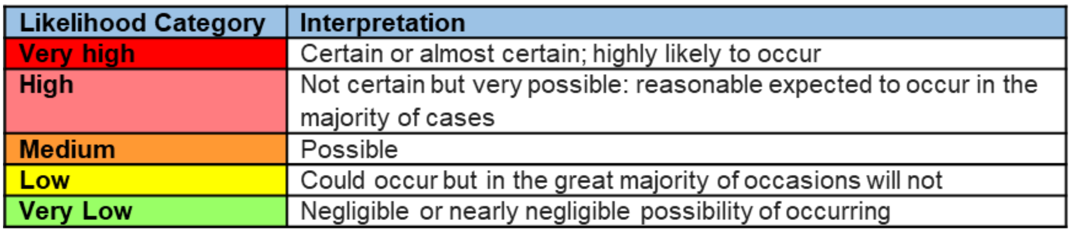
Likelihood	Very High	3	4	4	5	5
	High	2	3	3	4	5
	Medium	2	2	3	3	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3
		Minor	Significant	Considerable	Major	Catastrophic
		Severity				

Risk Matrix Score Acceptability Definition



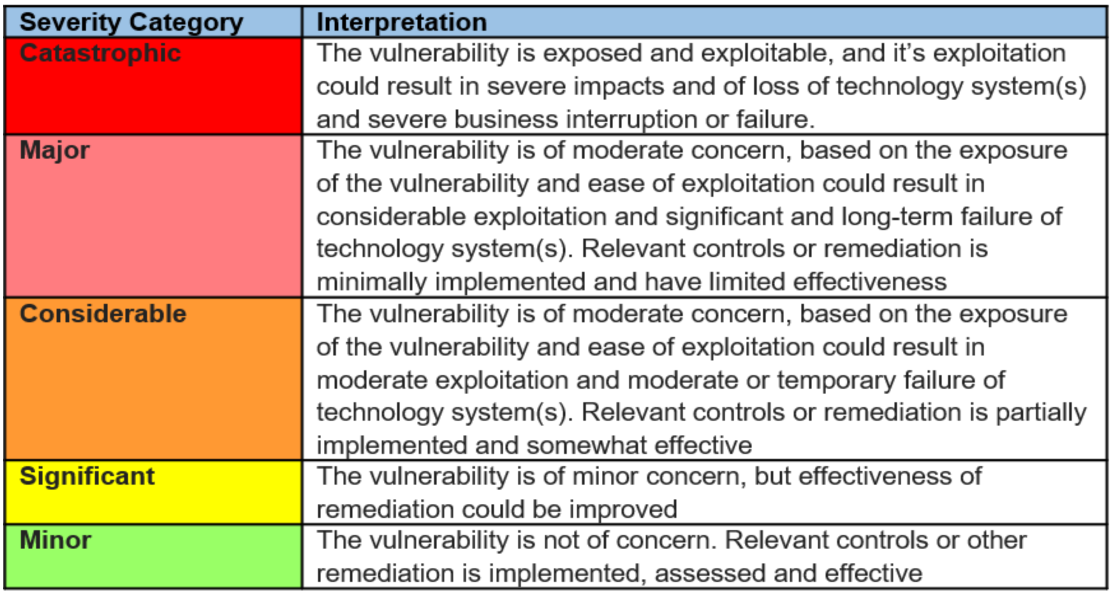
Overall Risk Matrix Score	Risk Definition	Risk Acceptability > Action
5	Very high	Unacceptable level of risk. Mandatory elimination or control to reduce risk to an acceptable level
4	High	Unacceptable level of risk. Mandatory elimination or control to reduce risk to an acceptable level
3	Significant	Undesirable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternative risks.
2	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
1	Low	Acceptable, no further action required

Likelihood Classification



Likelihood Category	Interpretation
Very high	Certain or almost certain; highly likely to occur
High	Not certain but very possible: reasonable expected to occur in the majority of cases
Medium	Possible
Low	Could occur but in the great majority of occasions will not
Very Low	Negligible or nearly negligible possibility of occurring

Severity Classification



Severity Category	Interpretation
Catastrophic	The vulnerability is exposed and exploitable, and it's exploitation could result in severe impacts and of loss of technology system(s) and severe business interruption or failure.
Major	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation could result in considerable exploitation and significant and long-term failure of technology system(s). Relevant controls or remediation is minimally implemented and have limited effectiveness
Considerable	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation could result in moderate exploitation and moderate or temporary failure of technology system(s). Relevant controls or remediation is partially implemented and somewhat effective
Significant	The vulnerability is of minor concern, but effectiveness of remediation could be improved
Minor	The vulnerability is not of concern. Relevant controls or other remediation is implemented, assessed and effective

2. Risk Identification

In accordance with the technology risk management process a technology risk identification has been undertaken to understand the risks associated with use of Good Boost's digital exercise app and wider technology system. Section 2 described the process and methodology in identifying and analysing risks alongside the estimation of the relative risk to users.

2.1 Risk Identification process and Estimation of Technology Risk

Possible risks are explored and identified by the DPO and CSO on an annual basis. This incudes reviewing all systems and potential risks to the infrastructure, architecture and operation of Good Boost's technology. The process is a shared activity to list all possible risks and the number of possible contributing causes. The risk rating of likelihood, severity and overall risk is the pre-mitigation risk analysis. Post-mitigation analysis will be complete following application of controls and mitigation actions.

I.D.	Describe risk and nature of impact	Likelihood	Severity	Overall Risk
R1	Poorly designed and unusable technology for users • Inability for users to access and utilise Good Boost technology	Medium	Major	Medium
R2	Failure of user facing technology due to overloading • Inability for users to access and utilise Good Boost technology	Low	Major	Medium
R3	Unauthorised access and use of user personal data • Data protection compromise; breach of sensitive data	Medium	Catastrophic	High
R4	Errors in data storage and writing to databases • Inability for users to access and utilise Good Boost technology • Potential error in exercise recommendation function	Medium	Major	Medium
R5	Deployment of non-functioning technology due to poor code review • Inability for users to access and utilise Good Boost technology • Incorrect functioning that could lead to data errors of functional errors of exercise recommendation	Medium	Major	Medium
R6	Malware / Hacking of technology and data • Loss of company intellectual property • Non-functioning of technology • Data protection compromise; breach of sensitive data	Medium	Catastrophic	High
R7	Loss of data due to employee actions • Loss of company intellectual property • Data protection compromise; breach	Medium	Catastrophic	High

	of sensitive data			
R8	Loss of data due to 3rd parties and contractors • Loss of company intellectual property • Data protection compromise; breach of sensitive data	Medium	Catastrophic	High
R9	Failure of database and cloud storage systems • Loss of company intellectual property • Non-functioning of technology • Data protection compromise; breach of sensitive data	Medium	Catastrophic	High
R10	Failure of Clinical Technology systems (such as exercise recommendation errors) • Incorrect functioning that could lead to data errors of functional errors of exercise recommendation	Medium	Catastrophic	High

2.2 Technology Risk Evaluation

I.D.	**Describe risk and nature of impact**	**Overall Risk**	**Action**
R1	Poorly designed and unusable technology for users	Medium	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R2	Failure of user facing technology due to overloading	Medium	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R3	Unauthorised access and use of user personal data	High	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R4	Errors in data storage and writing to databases	Medium	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R5	Deployment of non-functioning technology due	Medium	Unacceptable level of risk. Attempts should be made to eliminate or control

	to poor code review		to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R6	Malware / Hacking of technology and data	High	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R7	Loss of data due to employee actions	High	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R8	Loss of data due to 3rd parties and contractors	High	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R9	Failure of database and cloud storage systems	High	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks
R10	Failure of Clinical Technology systems (such as exercise recommendation errors)	High	Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks

2.3 Single and Multiple Contributors to Risks

I.D.	Describe risk and nature of impact	Contributors
R1	Poorly designed and unusable technology for users	• No user-led design / co-design • No internal testing & review • No user-led testing / piloting
R2	Failure of user facing technology due to overloading	• No load testing • Use of systems and servers with limited bandwidth
R3	Unauthorised access and use of user personal data	• Failure of Access controls • Cyber attack (hacking)
R4	Errors in data storage and writing to databases	• No internal testing & review • Poor database architecture
R5	Deployment of non-functioning technology due to poor code review	• Poor code framework and protocol • Poor code review process • No internal testing / piloting • No user-led testing / piloting
R6	Malware / Hacking of technology and data	• No penetration testing • Poor/exposed staff operations (i.e. passwords, equipment, network access, training)
R7	Loss of data due to employee actions	• Poor/exposed staff operations (i.e. passwords, equipment, network access, training) • Failure of Access controls
R8	Loss of data due to 3rd parties and contractors	• Poor procurement process • Failure of Access controls
R9	Failure of database and cloud storage systems	• Poor procurement process • Poor database architecture • No penetration testing
R10	Failure of Clinical Technology systems (such as exercise recommendation errors)	• Failure of Clinical Risk Management

3. Risk Mitigation and Control Planning

Each major risk (those falling in Medium (orange), High (bronze) and Very High (Red) zones on the Risk Matrix) will be assigned to a responsible IT Manager for monitoring purposes to mitigate and reduce risk to a tolerable level. For each major risk, and the single or multiple contributing factors, one of the following approaches will be selected to address it:

- Avoid – eliminate the threat by eliminating the cause
- Mitigate – Identify ways to reduce the probability or the impact of the risk
- Accept – Nothing will be done
- Transfer – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each major risk (medium or higher) that will be mitigated, the ultimate accountability is with the Technical Director / DPO to identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include redesign, redevelopment, additional access controls, non-technical administrative controls, new or changed processes, etc.

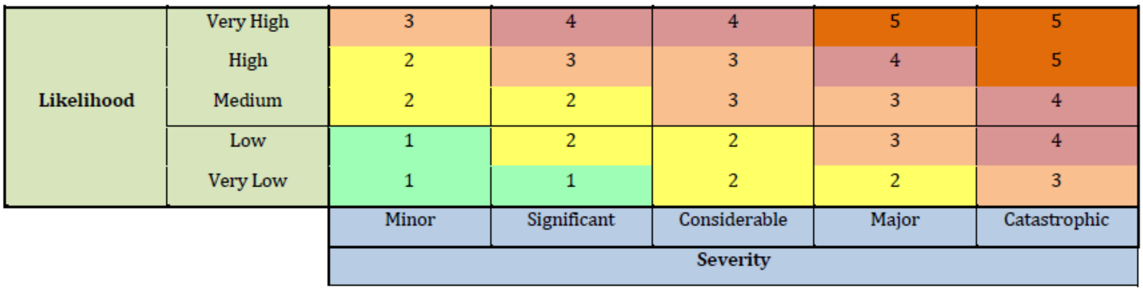
For each major risk (medium or higher) that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialise in order to minimise its impact.

4. Risk Mitigation Actions

I.D.	Describe risk and nature of impact (Rx)	Contributors (Cx)
R1	Poorly designed and unusable technology for users	
C1	**No user-led design / co-design** **Action** – focus groups with key stakeholder and anticipated users of the technology to co-design the functionality of the technology and ensure technology is inclusive and accessible. Outcomes of focus groups are to be integrated into the iterative design, development and deployment of technology.	
C2	**No internal testing & review** **Action** –New releases of the Good Boost app is reviewed by an appointed quality assessor (QA) to systematically check for functioning of technology. Any failures are reported to appropriate teams (technology/clinical) to resolve the failure.	
C3	**No user-led testing / piloting** **Action** – New apps and features are tested by primary user groups (i.e. adults with MSK condition) with feedback loops on functionality and satisfaction. Feedback is reported to relevant teams (technical/clinical) for iterative improvements ahead of final sign off and release of any app, new version or feature.	
R2	Failure of user facing technology due to overloading	
C1	**No load testing** **Action** – Monthly load testing the app and systems that have public facing users to a minimum of double estimated maximum usage (users/end-point calls)	
C2	**Use of systems and servers with limited bandwidth** **Action** – Procurement of code bases and servers with bandwidth that is sufficient to offer a minimum of double the estimated maximum usage (users/end-point calls)	

R3	Unauthorised access and use of user personal data
C1	**Failure of Access controls** **Action –** Access control policy and protocol to minimise staff access to personal data. Two-factor authentication for personal data access. Additional agreements and justification with authorised personnel to have access to this data.
C2	**Cyber attack (hacking)** **Action –** Penetration testing to identify system exposure. Any weaknesses are identified and resolved **Action –** Policies and protocols on employee equipment security, passwords, network access, confidentiality agreements to minimise risk of system access compromise
R4	Errors in data storage and writing to databases
C1	**No internal testing & review** **Action –**New releases of the Good Boost app is reviewed by an appointed quality assessor (QA) to systematically check for functioning of technology. Any failures are reported to appropriate teams (technology/clinical) to resolve the failure.
C2	**Poor database architecture** **Action –** Databases designed to be easy to navigate with data dictionaries to define and explain data stored in databases. **Action –** Routine data accuracy testing to ensure that data entered through front-end apps are accurately recorded in the database
R5	Deployment of non-functioning technology due to poor code review
C1	**Poor code framework and protocol** **Action –** Follow guidance and framework for clean and maintainable code. All code is subject to review and approval by two developers.
C2	**Poor code review process** **Action** - All code is subject to review and approval by two developers and unit testing
C3	**No internal testing / piloting** **Action –**New releases of the Good Boost app is reviewed by an appointed quality assessor (QA) to systematically check for functioning of technology. Any failures are reported to appropriate teams (technology/clinical) to resolve the failure.
C4	**No user-led testing / piloting** **Action –** New apps and features are tested by primary user groups (i.e. adults with MSK condition) with feedback loops on functionality and satisfaction. Feedback is reported to relevant teams (technical/clinical) for iterative improvements ahead of final sign off and release of any app, new version or feature
R6	Malware / Hacking of technology and data
C1	**No penetration testing** **Action –** Quarterly penetration testing. Any exposures and weaknesses are identified and resolved within 5 business days.
C2	**Poor/exposed staff operations (i.e. passwords, equipment, network access, training)** **Action –** Implementation of policies and protocol of provision of secure digital equipment and devices, working from home policies, password policies, data protection policies and training to minimise everyday activities of personnel that could compromise exposer and create weaknesses
R7	Loss of data due to employee actions
C1	**Poor/exposed staff operations (i.e. passwords, equipment, network access, training)** **Action –** Implementation of policies and protocol of provision of secure digital equipment and devices, working from home policies, password policies, data protection policies and training to minimise everyday activities of personnel that could compromise exposer and create weaknesses
C2	**Failure of Access controls** **Action –** Access control policy and protocol to minimise staff access to personal data. Two-factor authentication for personal data access. Additional agreements and justification with authorised personnel to have access to this data.

R8	**Loss of data due to 3rd parties and contractors**
C1	**Poor procurement process**
	Action – all 3rd parties must have evidence of acceptable security standards that comply with revenant regulatory standards and practices in place before procurement. All contracts include confidentiality, data sharing agreements and IP/source code ownership
	Action – all sub-contractors agree contracts with clauses of confidentiality and IP ownership. Sub-contractors are provided with Good Boost emails so all communication is centralised and controlled
C2	**Failure of Access controls**
	Action – Access control policy and protocol to minimise staff access to personal data. Two-factor authentication for personal data access. Additional agreements and justification with authorised personnel to have access to this data. Any access of data provided to 3rd parties must follow GDPR requirements and have a minimum sign off of two authorised persons.
R9	**Failure of database and cloud storage systems**
C1	**Poor procurement process**
	Action – All digital system must be purchased from a reputable source/organisation
	Action – All digital systems must demonstrate evidence of acceptable standards that comply with revenant regulatory standards and practices.
C2	**Poor database architecture**
	Action – Databases designed to be easy to navigate with data dictionaries to define and explain data stored in databases.
	Action – Routine data accuracy testing to ensure that data entered through front-end apps are accurately recorded in the database
C3	**No penetration testing**
	Action – Quarterly penetration testing. Any exposures and weaknesses are identified and resolved within 5 business days.
R10	**Failure of Clinical Technology systems (such as exercise recommendation errors)**
C1	**Failure of Clinical Risk Management**
	Action – complete and implement Clinical Risk Management plan



Likelihood	Very High	3	4	4	5	5
	High	2	3	3	4	5
	Medium	2	2	3	3	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3
		Minor	Significant	Considerable	Major	Catastrophic
		Severity				

4.1 Post-Mitigation Risk Analysis

I.D.	Describe risk and nature of impact	Likeli-hood	Severity	Overall Risk	Mitigation Actions	Likeli-hood	Severity	Overall Risk
R1	Poorly designed and unusable technology for users	Medium	Major	High	C1 User-led design / co-design C2 Internal testing & review C3 User-led testing / piloting	Very Low	Considerable	Moderate
R2	Failure of user facing technology due to overloading	Low	Major	High	C1 Load testing C2 Use of systems and servers with suitable bandwidth	Low	Significant	Moderate
R3	Unauthorised access and use of user personal data	Medium	Catastrophic	High	C1 Access controls C2 Cyber attack (hacking) mitigation	Very Low	Major	Moderate
R4	Errors in data storage and writing to databases	Medium	Major	High	C1 Internal testing & review C2 Suitable database architecture	Very Low	Significant	Low
R5	Deployment of non-functioning technology due to poor code review	Medium	Major	Significant	C1 Suitable code framework and C2 Suitable code review process C3 Internal testing / piloting C4 User-led testing / piloting	Very Low	Significant	Low
R6	Malware / Hacking of technology and data	Medium	Catastrophic	High	C1 Penetration testing C2 Suitable staff operations (i.e. passwords, equipment, network access, training)	Very Low	Major	Moderate
R7	Loss of data due to employee actions	Medium	Catastrophic	High	C1 Suitable staff operations (i.e. passwords, equipment, network access, training) C2 Access controls	Low	Considerable	Moderate
R8	Loss of data due to 3rd parties and contractors	Medium	Catastrophic	High	C1 Suitable procurement process C2 Access Controls	Low	Considerable	Moderate
R9	Failure of database and cloud storage systems	Medium	Catastrophic	High	C1 Suitable procurement process C2 Access Controls C3 Penetration Testing	Very Low	Major	Moderate
R10	Failure of Clinical Technology systems (such as exercise recommendation errors)	Medium	Catastrophic	High	C1 Suitable Clinical Risk Management	Very Low	Major	Moderate

4.2 Implementation of Technology Mitigation and Control Measures

The technology risk mitigation actions identified in section 4 must be implemented except where these are to be implemented by another. Every technology risk control measure implemented must be verified and documented by a senior member of each team (technical, clinical, operations).

Every technology risk control measure implemented must have the effectiveness of each measure verified.

4.2 Post-Mitigation & Control Technology Risk Evaluation

I.D.	Describe risk and nature of impact	Overall Risk	Action
R1	Poorly designed and unusable technology for users	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R2	Failure of user facing technology due to overloading	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R3	Unauthorised access and use of user personal data	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R4	Errors in data storage and writing to databases	Low	Acceptable, no further action required
R5	Deployment of non-functioning technology due to poor code review	Low	Acceptable, no further action required
R6	Malware / Hacking of technology and data	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R7	Loss of data due to employee actions	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R8	Loss of data due to 3rd parties and contractors	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R9	Failure of database and cloud storage systems	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.
R10	Failure of Clinical Technology systems (such as exercise recommendation errors)	Moderate	Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.

5. Risk Monitoring, Controlling & Reporting

Good Boost must establish, document and maintain a process to collect and review reported risk concerns and safety incidence for the technology system following it’s deployment.

Good Boost must assess the impact of any such information on the on-going validity of the technology risk management plan.

Where any such evidence is assessed to compromise and expose the technology system(s), Good Boost must take appropriate corrective action in accordance with the Technology Risk Management Plan and document it in the Technology Risk Case Report.

Good Boost must ensure security and exposure related incidents are reported and resolved in a timely manner of 5-business days. If this is not possible, there must be adequate justification for timescale of resolution.

A record of any security incidents, compromise and exposure, including their resolution, must be maintained by Good Boost in the Technology Risk Case Report Log.

6. DPO Sign-off

Item	Name/position/date	Notes
Measures approved by:	**Alex Georgiou**	**Integrate actions back into project plan, with date and responsibility for completion**
Residual risks approved by:	**Ben Wilkins**	**If accepting any residual high risk, consult the ICO before going ahead**
DPO advice provided:	**No further comments**	**DPO should advise on compliance, step 6 measures and whether processing can proceed**
Summary of DPO advice:		
DPO advice accepted or overruled by:	**Accepted**	**If overruled, you must explain your reasons**
Comments:		
Consultation responses reviewed by:	**Ben Wilkins**	**If your decision departs from individuals' views, you must explain your reasons**
Comments:		
This Technology Risk Management Plan will kept under review by:	**Alex Georgiou - DPO**	**The DPO should also review ongoing compliance with TRMP**

Signed: Alex Georgiou

Alex Georgiou – CTO & DPO
18th December 2023