

Data Security and Protection Toolkit 2021/2022

IT System Risk Assessment

- It is a Data Protection requirement that all Information Assets (systems) have a risk assessment carried out which must cover both the risk of the system being unavailable, along with any privacy risks to the data held in the system.
- Risk assessments are the responsibility of the Information Asset Owner (responsible system owner)
- Risk assessments must be reviewed at least annually.
- Any (Divisional) actual or perceived risk must be discussed at divisional level and considered for inclusion on the Divisional Trust Risk Register (DATIX)
- This template has been provided to assist in this process, it is not compulsory to use this template or this format, however your assessment must meet the standards set down in the Trusts Risk Policy.
- This template includes some examples to consider any additional risks identified should be added.
- This template has been created in line with the Trusts RM01 Risk Management Policy and Strategy. The impact, likelihood and scoring are based on the Matrix taken from RM01 and added in the appendix of this document for reference.
- Examples of INFORMATION SECURITY risks to be considered when completing this assessment can be accessed [here](#)

System Name

Completed by

IAO:

Site:

Division:


 

Directorate:


Excluded
this point.

If an exclusion is authorised by the DSP team there is no need to complete beyond this point.

Date Completed

Review Due

Is this system business critical to your department? Yes No

Is this system business critical to the Trust? Yes No

Data Flows

Does this system store or transfer data out side the UK YES NO

If yes provide details of data items and locations below

If Yes what risk mitigation is in place?

Business Continuity -

Following any failure how robust was the business continuity plan in place for this system. Please detail below:

Have changes had to made to the business continuity plan in the past year? Please detail below:

Do you keep a manual (paper) copy of your business continuity plan or processes?
YES NO

If so where are they stored? Please detail below:

Appendix

Impact Matrix

Impact Domains	Impact Score and Examples of Descriptions				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Impact on the safety of patients, staff or	Minimal injury requiring no/minimal intervention or	Minor injury or illness, requiring minor intervention Requiring time off	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days	Incident leading to death Multiple permanent injuries or

public (physical / psychological harm)	treatment. No time off work	work for >3 days Increase in length of hospital stay by 1-3 days	hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	irreversible health effects An event which impacts on a large number of patients
Quality / Equality / Complaints / Audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
Human Resources / Organisational Development / Staffing / Competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory Duty / Inspections / PFI Contracting	No or minimal impact or breach of guidance/ statutory duty	Breach of statutory legislation Reduced performance rating if unresolved	Single breach in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breaches in statutory duty Improvement notices Low performance rating Critical report	Multiple breaches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse Publicity / Reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business Objectives / Projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including Claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service / Business	Loss/interruption of >1 hour Minimal or no impact	Loss/interruption of >8 hours Minor impact on	Loss/interruption of >1 day Moderate impact on	Loss/interruption of >1 week	Permanent loss of service or facility Catastrophic impact on

Interruption / Environmental Impact	on the environment No impact on other services	environment Impact on other services within the Division	environment Impact on services within other Divisions	Major impact on environment Impact on all Divisions	environment Impact on services external to the organisation
Information Security / Data Protection	Potential breach of confidentiality with less than 5 people affected Encrypted files	Serious potential breach of confidentiality with 6 – 20 people affected Unencrypted clinical records lost	Serious breach of confidentiality with 21 – 100 people affected Inadequately protected PCs, laptops and remote device	Serious breach of confidentiality with 101 – 1000 people affected Particularly sensitive details (i.e. sexual health)	Serious breach of confidentiality with over 1001 people affected Potential for ID theft

Likelihood Matrix

SECTION 2 – LIKELIHOOD OF OCCURENCE

Risk Score		Probability
1.	RARE	The event may only occur in exceptional circumstances.
2.	UNLIKELY	Unlikely to occur.
3.	POSSIBLE	Reasonable chance of occurring.
4.	LIKELY	The event will occur in most circumstances.
5.	ALMOST CERTAIN	Most likely to occur than not.

Risk Scoring Matrix

SECTION 3 – RISK SCORING MATRIX

		Consequence/Impact Score				
		1	2	3	4	5
Likelihood	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Recorded 2018/2019 review status

Recorded 2019/2020 review status


Recorded 2020 / 2021 review status

I Agree that the 2021/2022 review of this document is Complete

Name



Date



Submit