

INFORMATION RISK

TRIAGE TOOL

V201901

Contents

[1. Triage Risk Assessment Tool 2](#_Toc357367)

[2. Aims 2](#_Toc357368)

[3. Scope 2](#_Toc357369)

[4. Questions 2](#_Toc357370)

[5. Background 3](#_Toc357371)

[6. About the data 4](#_Toc357372)

[7. About the solution 4](#_Toc357373)

[8. Information governance 6](#_Toc357374)

[9. Scores 8](#_Toc357375)

|  |
| --- |
|  |

# ****Triage Risk Assessment Tool****

The tool is based on Lime Survey, an open source platform whose instance has been installed by the Show team on a NSS web server. Access is only available from SWAN to authorised individuals. The tool is based on a set of questions whose answers provide the final risk score. The risk assessment tool is available on:

<https://www.yoursurvey.scot.nhs.uk/index.php?r=survey/index/sid/455432/newtest/Y/lang/en>

# Aims

The tool provides a high level risk assessment of information systems whose score highlights whether further and more detailed information such as Security System Policy is required. The main aims are described below:

* To help Boards achieve compliance with National Security Policy Framework
* To provide an efficient tool that follows a reliable and consistent algorithm to measure information system risk

# Scope

The survey tool could be deployed to all the 22 organisations which form NHS Scotland. At the moment is only a proof of concept which requires testing to make sure that the score is reliable and valid. The level of risk score could be entered in the asset register.

# Questions

The questions are divided into four categories that reflect the tables below: “background questions”, “about the data”, “about the solution” and “information governance”. The tables have the following columns:

* Question code in the questionnaire
* Description includes the question

# Background

|  |  |  |
| --- | --- | --- |
| **Question code** | **Question** |  |
| B1 | Your name  |  |
| B2 | Your email |  |
| B3 | Your contact number |  |
| B4 | Your role in the project in question |  |
| B5 | What is the name of the project/information system/data asset? |  |
| B6 | Approximate project budget | Table 7 "B6 - Approximate project budget values"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | less than GBP 10k |
| 2 | GBP 10k - 100k |
| 3 | GBP 100k - 250k |
| 4 | GBP 250k - 1m |
| 5 | more than GBP 1m |

 |
| B7 | Please describe how the solution is paid for (e.g. source of funding, who is paying?) |  |
| B8 | How would you describe the profile of the solution? | Table 9 "B8 - How would you describe the profile of the solution?"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | Low profile, limited exposure and visibility outside of local project team, internal to the health board |
| 3 | Moderate profile - visibility at SMT or exec level within the health board and/or partner organisations |
| 4 | High profile - some public engagement, key strategic deliverable for SG/NHSS/health board strategy |
| 5 | Very high profile - critical success project for the health board, high profile visibility in public/media, key to SG/NHSS/health board strategy |

 |
| B9 | When is it planned for the solution to go live? | Table 12 "B9 - When is it planned for the solution to go live?"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | Longer than 12 months |
| 2 | In the next 12 months |
| 3 | In the next 6 months |
| 4 | In the next 3 months |
| 5 | Solution is already live |

 |

# About the data

|  |  |  |
| --- | --- | --- |
| Question code | Description |  |
| D1 | Data in scope | Table 5 "D1 - Data in scope values"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | Green |
| 3 | Amber |
| 4 | Red |
| 5 | Extraordinarily sensitive |

 |
| D2 | Volume of personal records  |

|  |  |
| --- | --- |
| **Table 3** | **Value** |
| No personal record | 1 |
| between 0 and 1,000 | 2 |
| between 1,000 and 10,000 | 3 |
| between 10,000 and 100,000 | 4 |
| More than 100,000 | 5 |

 |

(\*) We are asking for how many times the app is predicted to be used in year (estimate gross figures)

# About the solution

|  |  |  |
| --- | --- | --- |
| Question code | Description |  |
| S1 | Which organisations will access the data? | Table 11 "S1 - Which organisations will access the data?"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | Internal to health board only |
| 3 | Internal to NHS only |
| 4 | NHS and partners on SWAN |
| 5 | Internet facing, public, external partners |

 |
| S2 | High level architecture of the system | Table 14 "S2 - If an information system will be implemented describe the high level architecture”

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | No information system (e.g. Only paper records, or access using existing desktop/office e.g. Word, Excel) |
| 3 | Web based application - accessed using browser, no special software required |
| 4 | Thick client application - software must be installed on end user device |
| 5 | Mobile application - app installed via Google Play, Apple Store or another app store |

 |
| S3 | Location of the data hosted | Table 13 "S3 - Where will any parts of the solution or data be hosted?"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | All internal to health board |
| 3 | Utilising private contracted hosting in the UK |
| 4 | Utilising shared/cloud hosting in the UK |
| 5 | Utilising shared/cloud hosting outside of the UK or not sure |

 |
| S4 | How many users will access the data? | Table 8 "S4 - Approximately how many users will access the system/data?"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | Less than 100 |
| 3 | Between 100 and 1,000 |
| 4 | Between 1,000 and 10,000 |
| 5 | More than 10,000 |

 |
| S5 | Are any aspects of the solution covered by independent security certification? |  |

# Information governance

|  |  |  |
| --- | --- | --- |
| Question code | Description |  |
| IG1 | Will personal data be shared with another organisation? | If “yes” then data sharing agreement is required |
| IG2 | Controls in place | Table 10 "IG2\_6 - Patching policy in place to ensure all infrastructure kept up to date (all critical and security patches applied within 4 weeks of release)?"

|  |  |
| --- | --- |
| **Value** | **Answer option** |
| 1 | Yes |
| 5 | No |

 |
| IG3 | Concerns about the project |  |
| IG5 | Will data be processed by third party? | If “yes” then data processing agreement is required |
| IG6 PIA | IF any of the PIA questions is YES, a DPIA is required (refer to NHSScotland IG Pack, DPIA template) |

| **IG6** | **PIA triage questions** | **YES/NO**  |
| --- | --- | --- |
| 1. | The work involves carrying out a ***systematic and extensive evaluation*** of people’s personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing. Includes: Profiling and predicting, especially when using aspects about people’s work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movementsProcessing with effects on people such as exclusion or discrimination Excludes:Processing with little or no effect on people | Y |
| 2. | The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.*** Includes:* Racial or ethnic origin data
* Political opinions data
* Religious or philosophical beliefs data
* Trade Union membership data
* Genetic data
* Biometric data for the purpose of uniquely identifying a person
* Health data
* Sex life or sexual orientation data
* Data which may generally be regarded as increasing risks to people’s rights and freedoms e.g. location data, financial data
* Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive

To decide whether processing is ***large scale*** you must consider:* The number of people affected by the processing, either as a specific number or as a proportion of the relevant population
* The volume of data and/or the range of different data items being processed
* The duration or permanence of the processing
* The geographical extent of the processing activity
 | Y |
| 3.  | The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people. | N |
| 4.  | The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.  | N |
| 5. | The work involves processing personal data about ***vulnerable groups.***  This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.  | NO. May happen but not targeted  |
| 6. | The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new “Internet of Things” applications. | Y |
| 7. | The work involves transferring personal data across borders ***outside the*** countries listed in the [ICO website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/) ? * EEA countries
* Countries with an ‘Adequacy decision’ . You can view an up to date list of the countries which have an adequacy finding on [the European Commission's data protection website](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).
* covered by the EU-US Privacy Shield framework. check on the [Privacy Shield list](https://www.privacyshield.gov/list) to see whether the organisation has a current certification; or
* Covered by Canada’s PIPEDA
 | N |
| 8. | The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.  | N |

# Scores

|  |  |  |  |
| --- | --- | --- | --- |
| IMPACT | Score | LIKELIHOOD | Score |
| D1 | 4 | IG2 | 1 |
| D2 | 2 | S1 | 1 |
| B6 | 2 | S2 | 5 |
| B8 | 3 | S3 | 4 |
| S4 | 1 | B9 | 3 |
| TOTAL IMPACT SCORE | **12** | TOTAL LIKELIHOOD SCORE | 14 |
| Impact score normalised | [A] = (Impact score / 25) \* 5[A ] = 12/25\*5 = 2.4  | Likelihood score normalised | [B] = (Impact score / 25) \* 5 [B] = 14/25\*5 = 2.8 |

 **RISK = Likelihood \* impact = [A] \* [B] = 2.4 \* 2.8 = 6.72 rounded: 7**

Based on the outcome of the risk assessment complete the corresponding next steps.



**If any of the IG6 (PIA) answers are YES, a DPIA is required** (refer to NHS Scotland IG Pack, DPIA template)