logoInformation Security

IG Pack

Risk assessment approach

V201901

**Why I need an IG Pack and when I need it ?**

An IG Pack is a standard set of documents, some of which are based on templates. The documents help project and system managers of digital innovations, projects or systems, to ensure they have considered the digital and information risk of their projects/systems. These also provide evidence that they have done the appropriate due diligence should there be an investigation (e.g. those run by the Information Commissioner Office or the NIS Competent Authority).

The IG Pack is designed to help you navigate through the required assessments and documentation you should keep as part of your project/system as you proceed towards approval.

In particular, the current regulations require that approval is sought **PRIOR** to processing personal data. The Network and Information Systems (NIS) Regulations also require certain levels of resilience to be built into digital systems across health care organisations. Resilience is the ability of your system to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation, including cyber-attacks but also other common issues that may impact the performance of your system such us speed, access to data, etc.

Understanding and reasonably minimising the information security and privacy risks of your project/system is not only good practice but a legal requirement derived from Data Protection regulations (UK) and the Network and Information Systems (NIS) Regulations (UK) .

**What does it mean to you?**

If you are running a project or managing an information system that handles NHS data, you must ensure your project/systems have sufficient security measures in place and complies with current regulations (e.g. Data Protection and NIS regulations (UK)).

This paper has been designed to help you by providing guidance, support and resources to help you manage risk within of your project/system and follows the fundamental principles of proportionality. i.e. The higher the risk the more effort you have to put to manage the risk.

**Where can I find the templates and resources mentioned in this paper?**

All templates mentioned in this paper can be downloaded from <http://www.informationgovernance.scot.nhs.uk/> section (IS Toolkit > Resources)

**Practical Steps:**

# STEP 1 - Run a triage of the overall system/project risk

NHS Scotland has developed a quick risk triage tool that generates a report and estimates the level of risk based on your answers to a few questions and the recommended next steps to get information governance (IG) approval for your project.

Regardless what are the recommended next steps, keep the output of this triage as evidence of due diligence and to justify the reasons taking those steps. The approach is based on proportionality, which is a fundamental characteristic of modern information risk management.

greater information risk = more requirements

lower information risk = lighter requirements

The time and resources allocated to understand and manager the information risk in your project depends on the overall risk of your project in first instance

The aim is to provide sufficient information to help stakeholders make robust risk-informed decisions. Typical stakeholders will be: Senior Information Risk Owners and Information Asset Owners. In some cases (e.g. National projects) special panels (e.g. NHS Scotland Public Benefit and Privacy Panel) may have also delegated powers to make these decisions.

All information systems processing NHS Scotland data must implement appropriate security controls to mitigate risk and protect NHS data and services, following fundamental proportionality principles.

## How to use the risk assessment tool

Access the online risk assessment tool using the link below (note this is only accessible to users via SWAN).

<https://security.scot.nhs.uk/new-nhs-scotland-cyber-risk-triage-tool/>

\*note this tool is not only focused on “cyber” risks despite of its name, but the overall information security risk of projects that involve digital information systems.

If you don’t have access to this link, you can use a paper format version available in the IG Pack (“*IGPACK Template for DOC02a Risk Assessment Triage Tool*”).

If you don’t have access to this tool, contact the Information Security Officer in your Health Board, who should be able to run the triage tool for/with you and also assist with a realistic interpretation of the risk level. This interpretation should be done in tandem by people who understand information security and people who understand the project/system context to avoid raising the level of risk unnecessarily whilst estimating risk on the cautious side, but also to a reasonable and realistic level.

Print off the outcome/report generated by this tool, as this constitutes evidence of your assessments towards compliance with data protection regulations, such as Data Protection regulations (UK) (it is mandatory to keep evidence of these considerations).

Based on the outcome of the risk assessment complete the corresponding next steps (refer to the illustration on the next page).

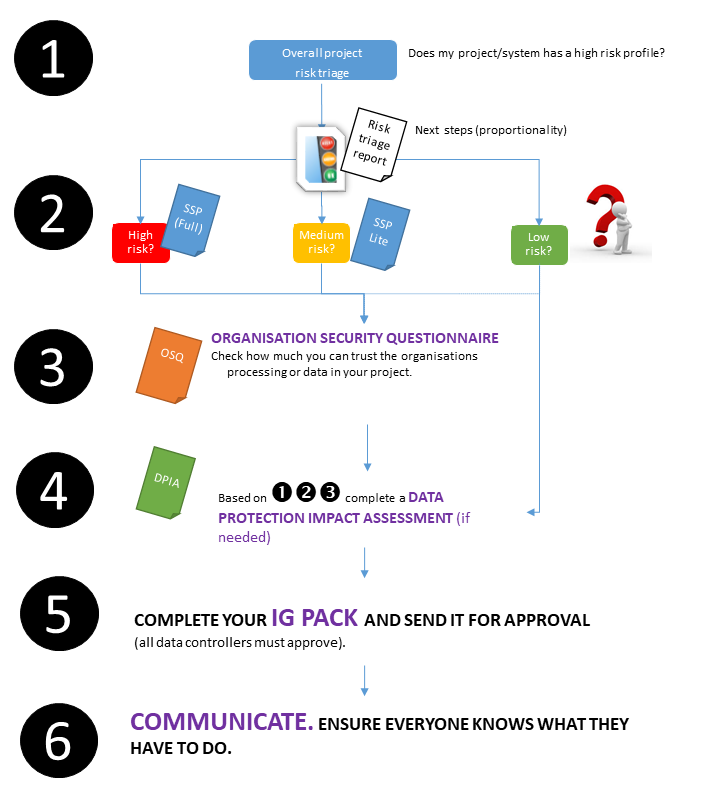


Figure 1 Getting approval for your project. Next steps - a risk based approach.

# STEP 2 – Understanding the technical security of your project/system

You need to understand how secure the system/service needs to be from a technical perspective. For this, you may need to engage with other people, such us the Information Security Officer of your health board, who will be able to advise you on who else should be contacted depending on the complexity of your project. For example, if your project involves subcontractors hosting servers on your behalf or providing web applications as a service, infrastructure as a service, etc. you may need to engage with them in order to ascertain how secure their provided services or their digital infrastructure is.

The NHS Scotland provides 2 templates in order to document and describe the security of a system:

* SSP – System Security Policy, required for high profile/risk projects
* SSP Lite – System Security Policy Lite version, required for medium profile/risk projects and recommended as a minimum for any system as good practice.

If you are working with 3rd parties/suppliers for the whole or parts of your digital solution, you may have to ask them to provide equivalent information in their own format. However providing them with the template is a good idea in order to ensure they provide all the information that is required by your Health Board Information Security Officer, otherwise he/she may not be able to scrutinise the technical security aspects of your project/system.

This information will be required in Step 4 in order to assess the adequacy of the security measures, and the level of risk to the organisation and the privacy of individual (if personal identifiable data is handled in the project/system).

Step 2 tells you about the technical security of your system.

# STEP 3 – Understanding the organisational security of your project/system

Similar to step 2, at this point you need to ensure that not only the system but also the organisation that manages the system can be trusted.

The following information is required for ALL organisations handling data in your project/system, regardless of type, this includes ALL, commercial companies,, charities, private subcontractors, central or local government agencies, departments, or other public bodies, including other NHS health boards.

This can be done in various ways:

* **ISO27001 Certified organisations.**

Ask the organisation(s) involved in processing your project’s data (manually or electronically) if they are ISO27001 certified. If so, you want to ask them to provide copy of the certification, the scope of the certification and a statement of applicability that identifies what controls are in scope. You cannot assume that an organisation is skilled at managing information just because they say they are ISO27001 certified, you need to understand the extent of their certification. Your Information Security Officer (ISO) can help you making sense of this information but you must always ask all organisation(s) engaged in the handling data in the project/system to provide this information to you or your ISO.

* Organisation who are **not ISO27001 certified** but are assessed against the **NHS IG Toolkit** **(England)** or its replacement, the **NHS Digital ‘**[**Data Security and Protection Toolkit’**](https://www.igt.hscic.gov.uk/)**.**

For organisation who can provide a recent assessment under the NHS IG Toolkit, you can ask for their organisation code (you can run a search by organisation name as well) and access their last report from [here](https://www.igt.hscic.gov.uk/ReportsOrganisationChooser.aspx?tk=434235743453262&lnv=3&cb=4bdea560-430d-4e9b-99a9-074f5a095929&reptypeid=1) (link to the NHS Information Governance Toolkit).

The IG Toolkit has been replaced by the Data Security and Protection Toolkit, but the IG Toolkit remains available to access historic submissions which still may be relevant for the remaining part of the year. Be cautious however because an organisation may have been rated as Level 3 in the IG Toolkit (this is good), but it doesn’t mean the organisation still operates at the same level of security today due to changes in the organisation’s systems, work practices, processes and procedures. The IG Toolkit offers attainment levels on a scale of 0 to 3, where 0 in insufficient and 3 the best possible outcome. The organisation is scored for each control, and the report produced indicates the percentage of attainment. Put simply the higher the percentage the better the organisation is at managing its security.

The [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/) has replaced (2018) the Information Governance Toolkit. The DSP Toolkit allow organisations to measure themselves against the NDG Data Security Standards and provides help for organisations by providing a tool to measure Data Protection regulations (UK) compliance. Since NHS Digital (England) requires all organisations that process NHS England’s health and care data to complete a Data Security and Protection Toolkit, this is also a useful reference for assessing NHS Scotland suppliers, as they may have completed a DSP Toolkit for their dealings with England. If they have one completed, this may give you a helpful indication of the level of security of the organisation.

* **Any other organisations**.

If the organisation you need to scrutinise doesn’t have any security certification or the NHS IG Toolkit (England) or the DSP Toolkit (England), you may want to ask if they hold any other relevant information security certifications (e.g. Cyber Essentials+) and to provide details of these certifications, their scope and their certification results.

They must also complete the OSQ (Organisational Security Questionnaire) for which the NHS Scotland has developed a standard template.

# STEP 4 – Data protection legal requirements

You must also check if the proposed system/project meets any of the data protection conditions in pages 3 and 4 (triage table) of the NHS Scotland DPIA template – if that’s the case you must document a Data Protection Impact assessment (required by law) using the NHSS National template available for download from here:

<http://www.informationgovernance.scot.nhs.uk/>

Keep in mind that the aim of a DPIA is not only about identifying the data, data flows and security measures, but in particular to ensure that the risk for both: the individuals whom data is being processed and the organisation is addressed reasonably and with proportionality.

You will need any documents obtained in steps ➊➋➌ in order to be able to complete a DPIA, as it must include technical and organisational risks and ensure that sufficient measures are in place to reduce the risk to the point where it’s acceptable for the organisation and is compliant with current legislation.

The NHS Scotland DPIA template suggests who should be involved and consulted when conducting a DPIA, as any identified risks must be acceptable to those who own the data (Information Asset Owner, IAO) and your organisation’s SIRO (Senior Information Risk Owner), otherwise, the project/systems may be required to have further countermeasures (technical or organisational).

IAO’s and SIRO’s must require the advice of a qualified DPO (Data Protection Officer). Caldicott Guardians may also be required to provide advice, along with the opinion of others, such as the Information Security Officer (ISO), **prior** to making any decision to approve. Some SIRO’s have delegated decision powers to Caldicott Guardians, but this is not always the case in every organisation.

For National or Multi-Board projects the assessment is made by the PBPP (Public Benefit and Privacy Panel) on behalf of the NHS Scotland Health Boards.

Refer to the illustration on the next page which shows the typical approval process for different types of projects (e.g. research, telehealth/telecare innovation, etc.)

# Complete your IG Pack and send it for approval.

Approval needs to be given by all relevant data controllers. Check with your data controllers what is the best route.

For national NHS Scotland projects, the best route is PBPP (Public Benefit and Privacy Panel) as they have delegated powers to scrutinise your application and approve on behalf of all NHS Health Boards (refer to Figure 2).

If your project involves other data controllers (e.g. Scottish Government, Local Authorities or even GPs), you may need to think how are you going to gather approval from all this parties, for which you may need to contact key information sharing advisory services across these parties.

The Digital Health and Social Care Division (former eHealth Information Assurance Team) at Scottish Government can provide advice on best routes for complex national projects.

Local Data Protection Officers and IG Leads can also provide similar advisory services.

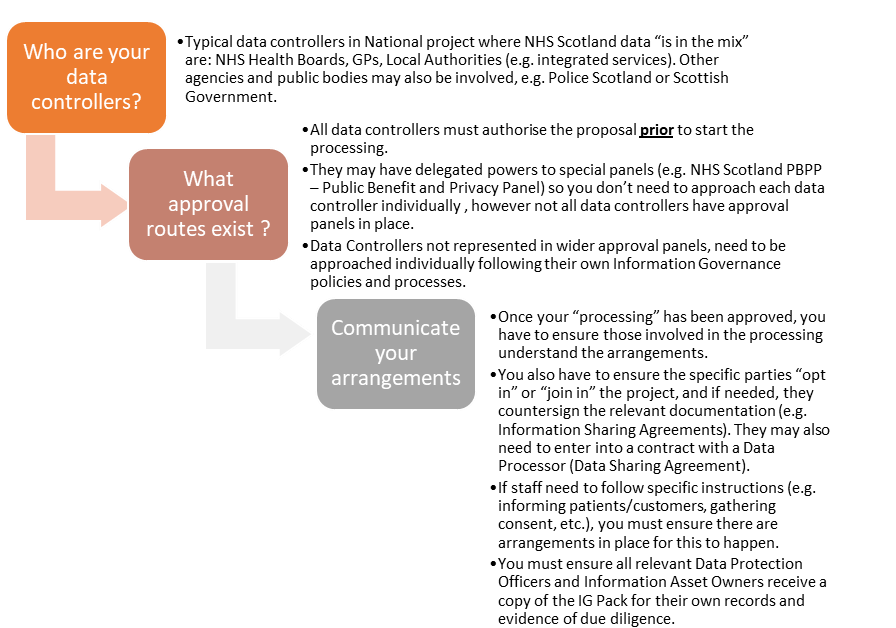


Figure 2 Getting the right approval.

Approval process from NHS Scotland data controllers (where NHS Scotland data is in the mix).

**What is in the IG Pack.**

The IG Pack is a set of documents that are necessary in order to inform stakeholders (data controllers) on the proposed processing, the arrangements put in place and any remaining risks to be taken into account, so they can make an informed decision and also instruct their teams/managers to act accordingly.

Most IG Packs include a combination of the following documents, depending on the particulars of each project:

* IG Pack checklist (this document)
* Executive letter
* A copy of the full PBPP application
* PBPP approval letter (with conditions if apply)
* Overall project/proposal risk triage
* DPIA – Data Protection Impact Assessment (signed off by data controllers or approved as part of a PBPP submission on behalf of NHS Scotland).
* CHIAG approval (if use of CHI is involved in the proposal) or indication in the PBPP application that it was sent to CHIAG and what meeting (CHIAG date minutes) was approved – generally it is included in the PBPP application and the DPIA – just ensure this is stated in these documents.
* Data Processor Agreements to be used (DPA) (if a subcontractor is used)
* Information Sharing Agreements (ISA) applicable (if data is shared with other parties that are also or will become data controllers for the data in this proposal)
* Opt-in / Opt-out / Sign off templates as applicable (e.g. when a large number of organisations can join an Information Sharing Agreement)
* Official mandate (e.g. Ministerial mandate or Scottish Government Executive Letter as applicable) – if existent this letter should be used to address the IG Pack to the Data Protection Officer of each relevant data controller (e.g. health boards, GPs, etc. as applicable)
* IA Registration Form Summary (or amend the information about this proposed processing in the IA Register if the IA is already registered)
* Privacy notices (existent or new)
* Evidence of relevant data protection training for all staff involved in the processing

For complex projects or if high risks are identified (privacy or security) in the “Overall project/proposal risk triage”, you must complete:

* Full Information Asset Risk Assessment
* ICO feedback (if consulted, e.g. when high privacy impact is foreseen)

If electronic/digital systems are involved (e.g. data captured, sent or accessed via digital means), you also need some sort of documentation of this system’s security. The level of detail depends on the outcome of the “Overall project/proposal risk triage”

* Security policy and risk assessment of each system involved (full, lite or as per instructions of a relevant Information Security Officer)
* Security questionnaire of the organisation(s) involved in the management and use of the system (and copies of any relevant Certification, e.g. ISO27001)- (full, lite or as per instructions of a relevant Information Security Officer)

## What if I have to share data with other organisations?

If you need to share data with a subcontractor (data processor) you need to have a contract with them with the right “Data Protection regulations (UK) ” (data protection) clauses.

The NHS Scotland Legal Office has provided a template you can download from the <https://www.informationgovernance.scot.nhs.uk/> website (IS-Toolkit > Resources)

If you need to share data with other data controllers (other organisations who will make decisions on the purposes and manner the data is processed, either independently or jointly with your organisation), then you need to have an Information Sharing Agreement (ISA) in place. You should check with a Data Protection Officer within these organisations if they already have an ISA that covers what you want to do in your project/system. If there is not ISA in place for that purpose (or it’s too obsolete), you must complete one using the Scottish Information Sharing Toolkit

<https://www.informationgovernance.scot.nhs.uk/is-toolkit/>

# COMMUNICATE.

**ENSURE EVERYONE KNOWS WHAT THEY HAVE TO DO.**

Once you have completed you IG Pack and you have obtained approval from the relevant Data Controllers. You have to ensure those teams involved in the processing understand what they have to do. This may require:

* explaining local Data Protection Officers and IG people the content of the IG Pack
* ensuring all Information Asset Owners are aware of the IG Pack and have registered the Information Asset in their local registry (or updated accordingly)
* project leads, managers, etc. understand what are the arrangements and any instructions they must follow.
* ensure any local data processor agreements and ISAs are signed off.