BISHOPS' CONFERENCE OF SCOTLAND

INFORMATION AUDIT GUIDE

Table of Contents

1 Introduction ..... **Error! Bookmark not defined.**

2 Setting your objectives ..... **Error! Bookmark not defined.**

3 Identifying whgat informaion you have ..... **Error! Bookmark not defined.**

Document Control

Title	Basic Guide to Data Protection
Prepared by	Donna Maguire
Approved By	BCOS
Date of Approval	April 2018
Version Number	1.2
Review Frequency	Every 3 years
Next Review Date	Oct 2028

Status Control

Version	*Date*	*Status*	*Prepared by*	*Reason for Amendment*
1.2	11/2/2018	Complete	DMM	
1.3	01/10/2025	Review	DMM	

1 INTRODUCTION

The amount of information that the BCOS is creating and storing is continually increasing. We need to understand the nature and the purpose of this information so that we can utilise it fully in ways which are safe and compliant with legislation. This document outlines a practical process which will help you to understand, audit and document your information, making sure that it complies with the Data Protection laws, as well as supporting your day to day work.

Key questions:

- **How much information does your organisation/office hold?**
- **Who manages this information?**

1.1 What is the purpose of this Guidance?

The Guidance focusses on understanding and documenting the information you hold and should help you to:

- identify what information you hold
- understand your reasons for having the information

While undertaking an audit of the information you hold might seem a daunting task, it should result in significant benefits, including:

- better change management
- improved understanding of information risk
- identification of potential savings and efficiencies.

While this Guidance contributes to overall good Information Management (IM), one of its **KEY Objectives** is to support compliance with the new Data Protection Regulations.

An Information Audit will allow you to manage your digital and physical information, to ensure you comply with the new regulations, as well as ensuring that it meets your office/agency's needs. This will allow you to operate with accountability, in a legal, effective and efficient manner. It will help you to protect your reputation, make informed decisions, avoid and reduce costs, and deliver better services. The advent of GDPR makes it clear that, if you lose information because you haven't managed it properly, the consequences can be very serious.

Here we will provide you with practical information and support to help you complete your Information Audit by identifying information and documenting how it meets the requirements of your office/agency.

1.2 Who is this Guidance for?

The audience for this will vary depending on who is performing the Information Audit. Regardless of their role, the person leading the process is advised to consult other members of the organisation - for example, directors, Information controllers and processors, secretaries, and IT professionals - who may also find it useful to read this document to understand the background.

2 SETTING YOUR OBJECTIVES

You may be reacting to an incident, for example a loss of data, and you want to ensure that it does not happen again. Or you may want to prepare your office/agency for a specific change, such as the implementation of new data policies and you want to ensure that you have the necessary understanding to best protect your information.

While it is important to review all your information, trying to capture everything in detail at once is likely to be an overwhelming task. It is far better to prioritise key areas you want to look at initially.

You must as yourself questions such as:

- what you are trying to achieve and what are your priorities?
- what do you want to do with the information you are going to gather?
- what can you practically achieve?
- what risks do you need to mitigate?
- what benefits do you hope to achieve?
- what areas need the most urgent attention?

3 IDENTIFYING WHAT INFORMATION YOU HAVE

3.1 What is "information"?

To understand your information and how to manage and protect it, it is vital to first understand what we mean by the term "*information*".

"Information" is the term used for any data collected or held by your office/agency, either in physical or digital form. The key concept here is to group your individual pieces of information into manageable portions. If you had to individually assess every file, database entry or piece of data you hold, you would have a list of millions of items and an impossible task. By grouping items at a level to match your objectives, you can make the task more achievable.

3.2 How do you identify and group your information?

You should identify your information as above, considering the level of detail that is required to meet compliance with GDPR. The information must be defined to a level of description that allows its constituent parts to be managed usefully as a single unit i.e. all items relating to a project.

To perform this audit, you will need to talk to all staff within your office/agency to ensure you have covered all aspects of your business. You may already have resources you can use to help in this process, for example documentation of previous information audits, technical environment registers, configuration management databases or software lists. You should investigate these resources and re-use and adapt them wherever possible.

It is probably easiest to start with very broad definitions and then refining by splitting up the information groupings until they are of manageable sizes. To assess whether something is important, ask the following questions:

- Does it have a value to the organisation? Will it cost money to reacquire the information? Would there be legal, reputational or financial repercussions if you couldn't produce the information on request? Would it influence operational efficiency if you could not access the information easily? Would there be consequences of not having this information? Is there any risk associated with the information?

- Is there a risk of permanently losing the information? Any risk that the information is not accurate? Any risk that someone may try to tamper with it? Any risk arising from inappropriate disclosure?

- Does the information have a specific content e.g. personal or sensitive data? Do you understand what it is and what it is for? Does it include all the context associated with the information?

- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Note:

- Pieces of information should be grouped dependant on their significance to your office/agency, not on their technological requirements, i.e. database on a computer or paper files in filing cabinet. Each piece of information may contain individual items that require different solutions to be addressed at the same need.

- While it may be that a piece of information could logically belong to two different groups, this can lead to conflicts of ownership and control. So ideally each piece of information should only be included within a single group and must not be duplicated. However, while information can reference (point to) other information, care must be taken to manage these potentially complex relationships.

- Information can also contain other Information. As you introduce more and more detail in sub levels, it may be useful to retain the sense of the high-level information. Your office/agency must define clear rules about how the management and retention schedules of these groups of information operate at these different levels.

- The groupings of information may change over time. For example, you may have an information group which contains all the items archived into long term storage, therefore other pieces of information will be added into this group over time.

While such an audit can be a complicated process, done properly, it can be of real, lasting benefit to your office/agency. There is no right or wrong way to group your assets. The key point to remember is that you should do all of this within the scope defined by your organisation's objectives.

Key questions:

- **What kinds of information does your organisation/office hold?**
- **What main groupings of information will you use?**

4 IDENTIFING HOW YOU NEED TO USE INFORMATION

Once you have identified your information, you must determine how you need to use it. This covers everything from how you find it, through how you access it, to what you do with it. You must also consider any surrounding or supporting information which is important. There are five relevant questions here:

i. How will you find the information?

ii. Who has access to the information and how?

iii. How do you use the information?

iv. What do you need to be able to understand the information?

v. To what extent do you need to trust that the information is what it claims to be?

For each of these questions you must consider what your requirements are now, and how they might change over time. This will have implications for the retention schedules imposed on your information.

If you lose the ability to find, open, work with, understand and trust your information in the way that you need, it is for all intents and purposes LOST.

Note: it is possible that, in defining these requirements, you may need to go back and re-define your information groups; this may well be an iterative process. If the contents of a group now have dramatically different requirements in any of these areas, you may need to further subdivide it.

4.1 How will you find your information?

The detail and depth of any search required will depend on the type of information; it may be as simple as physically looking in a filing cabinet or it may involve finding the information digitally by searching within the information groups for files or searching within those files to find specific pieces of data.

Examples of requirements to meet GDPR:

- It must be possible to find generic information from your filing system without referencing specific names, to meet privacy requirements.
- It must be possible to search within the information to find files created within a specific date range.
- Any requests for information about your IT should be passed to your IT provider.

It is important to consider these requirements because they impact upon how you store your information and any aids/technology used for searching and indexing it.

Examples of requirements needed to comply with GDPR:

- Are the individual files inside an information group private, requiring only the person that created the file to be able to access the information?
- Is everything within the information group protectively marked allowing only those with the right clearance to access them?
- Can the information within the information group be published openly?

- Will you be able to release individual items inside the information group within 20 working days of a request?

The benefits of ensuring your information is kept secure are obvious. However, by considering the examples detailed above, you will be well placed, not only to meet your targets under the Data Protection Regulation on transparency, but improving the efficiency of storage, and potentially even reducing the likelihood of any duplication of work.

4.3 How do you need to be able to work with the information?

This is where you define the functionality that you require from your information, how you use it and what you need from your it.

Examples of requirements which you might consider:

- Does the information require to be editable? (This may involve using original source files.)
- Should the information be available to disabled users in formats suitable for screen and non-screen users, for example, brail or audio formats?
- While the creator of the document must have full read/write access, does everyone else only require read-only access, when working digitally?
- How will any formulae and functions inside the information be maintained so that they can be updated? It is not sufficient to only be able to access the resulting data.

Answers to such questions will determine the functionality that your technology must provide. So, by understanding these features, you may be able to streamline your software.

4.4 What do you need to be able to understand about the information?

This is about understanding the content and context of your information. This additional information is not necessarily included within the audit itself but is vital to making the information usable. This additional information may be stored digitally as metadata, but it may also be specific knowledge held by individuals, which may involve training or handover procedures when staff change.

Examples of requirements:

- Does the information within this group contain references and links to the content of other named information elsewhere?
- Is the information a large collection of files which must be kept within the current structure? Any restructuring would confuse the meaning of the collection of files?
- Was the information created under a specific set of circumstances which also must be recorded?
- Is there a complex version history which must be maintained so that it will be possible to access the information as it was at any specified date?
- Is the filing system holding the information complex, undocumented, and requiring those filing and retrieving information from within it to be trained in how to use it?

Answers to such questions will help you to understand how your information interacts and allows you to ensure that it continues to be usable over time.

4.5 To what extent do you need to trust that your information is what it claims to be?

The level of trust required of information will vary considerably. Most of your information may well not require any additional validation as it will speak for itself. However, for some, you may have to prove it has not been tampered with, or to certify it has been created on the date specified.

Examples of requirements:

- Do you need to record all access to the contents of the information?
- Do you need to be able to verify the integrity of a dataset, that nothing has been altered?
- Do all previous versions of the contents of the information need to be maintained as accessible?

Such requirements are particularly important because they cover your legal obligations and there may be serious repercussions if they are not fully understood and implemented.

Key questions:

- **How easy/difficult is it to find particular information in your office/agency?**
- **Do all office/agency colleagues organise the information in the same way?**
- **Do you need to track who has accessed any of your information?**

5 INFORMATION AUDIT (USING THE EXCEL SPREADSHEET)

The key purpose of the Information Audit is to document the links between your information and your GDPR compliance requirements.

In addition to details of how each information group supports your office/agency, there are several interesting and useful fields which can be recorded for each information group. How many of these you complete depends on your objectives.

The way that you build the Information Audit will depend on the scale of your objectives and the resources you have available. But, for this guide, please refer to the spreadsheet provided.

Explanation of Fields to be completed in the Information Audit Register

Name of Information Group	-Name of Information Group -How do you identify the information? (This could be a project, a collection, an event etc.)
What does it do	-Brief description of what the information is -More detail on what the components of the information are -Whose information
Location	-Where is the information located? -What is the file-path? -Local hard drive, external drive, shared network drive? -Where is its physical location, i.e. filing cabinet, building, safe, etc.
Owner	-Who created the information, or where does the information come from? -Who is the Information Owner? -Which department holds responsibility for the information? -Who are the stakeholders?
Volume/Size	-What is the size of the information? i.e. filing cabinet drawers; paper file boxes; digital files kb/Mb; etc.
Personal data	-Does the asset include sensitive personal data? N.B. This is very important for Data Protection.
Access	-What part of the office/agency does this asset support? -Who is at risk from the information -How will you find the information? -Who can open the information and how? -How do you need to be able to work with the information? -What do you need to be able to understand about your information? -To what extent do you trust your information is what it claims to be?
Shared	-Who is the information shared with? (Is it shared with other agencies out with the BCOS)? Under what agreement is the information shared?
Format/Media	-What format is the information saved in? i.e. digital file format; paper format; audio; video; etc…
Retention	-How long should it be kept in immediate access? -What should happen to it when it no longer needs immediate access? -What are the disposal requirements?
Password/Encryption	-is your information password protected? – who has the password? -is your information encrypted? – who has the encryption key?
Risks / impact	-What are the risks to the information? -What are the risks to the office/agency from the information (for example from its loss, corruption or inappropriate access)?
Key Information	-What is the value to the office/agency? -What would be the cost of replacing the information?
Backups	-is your data backed up? -where is it backed up? (off site etc.); how is it backed up?

5.2 Identify owners of information assets

One of the key fields on the Information Audit form is the **Owner** of the information who is responsible for making sure that the information is meeting its requirements, and that risks and opportunities are monitored. The owner need not be the creator, or even the primary user, of the information, but they

must have a good understanding of what the office/agency needs from the Information, and how the information needs to be able to fulfil those requirements.

5.3 Password, Encryption and Backups

It is important to record how your information is protected. Is it by password or encryption or both. Who has the passwords and encryption keys? Is your digital data backed up both on and off site? How do you backup and where do you store your physical data (i.e. paper files; audio & visual material; compact disks; etc.) Are the backup locations safe & secure & catastrophe proof (would not be the case if they were all in the same room/building and there is a fire)?

Key questions:

- **Is your information password protected? if so, who has the password?**
- **Is information encrypted? Who has the key?**
- **How & where is it backed up?**
- **Who has access to the backups?**

6 TAKING NEXT STEPS

The Information Audit provides you with a comprehensive list of the Information that is important to your office/agency. It may be a list of a hundred information groups covering your entire office/agency, or it may be just a few information groups that will be affected by the new Data Protection Regulations. Each entry on the register will have all the additional information about the information that is required to understand how it should be managed so that it delivers the use that your office/agency requires from it.

There are several ways you can use this Register to identify risks, capitalise on opportunities and manage change. You should return to your original objectives and take the corresponding next steps.

6.1 Mapping to technology dependencies

For each information group it is now possible to assess what technology is required to meet your needs. This will also allow you to understand the potential impact of change on your assets, and to make informed decisions about where to prioritise investment in ensuring the continued usability of your information. It should also highlight where savings can be made by not maintaining technical support unnecessarily.

6.2 Understanding your information management requirements

Alongside having the right technical tools to support your information requirements, there are likely to be information management processes which need to support the delivery of your requirements. This may mean introducing, updating and enforcing metadata or security policies, or providing relevant training and guidance on how and where to store files.

6.3 Identifying and mitigating risks

The risks associated with managing information include: loss of data, having it fall into the wrong hands; getting it corrupted. By considering such risks, you will be able to mitigate against them and form

contingency plans. You may need to escalate these risks to appear on departmental or corporate risk registers.

6.4 Identifying opportunities for disposal, exploitation, savings and efficiencies

In assessing the business requirements for your information assets, you may have uncovered information which is no longer actually required, and action should be taken to dispose of this. You may also have found that some information is only needed very rarely and could therefore be moved to cheaper long-term storage which is not instantly accessible.

If you have identified information that can, or should be shared, you can begin the process of allowing and promoting this access.

6.5 Managing change

When you have a comprehensive assessment of your current information and your requirements for it, you will be in a much better place to assess how any change may affect it. These changes could be to the information itself; how it's managed; any upgrades to the technology supporting it; or your office/agency's requirements that created it.

For specific changes you will be able to build impact and risk assessments allowing you to take mitigating action and to plan contingencies. You can also use this information to improve your change management process to make all future change-planning better. It is important to remember that you must embed the management of the Information Audit itself within your change processes. If the Information Audit is not kept up to date, through change it will become redundant and misleading.

Appendix 1 – Some scenarios which show examples of Information Management processes

1. Managing risks and improving governance; managing retention and disposal

A small government organisation has business information stored across several shared drives, standalone databases, and an Electronic Document and Records Management System (EDRMS). Current data protection risks are not well managed, partly because of a corporate lack of understanding about where information is and how long it has been there. At the same time the organisation is looking to reduce its IM and IT costs by getting rid of information it doesn't need.

The organisation decides it should initially map all its information at a high level. Each department is asked to describe on a spreadsheet the different types of information it creates and uses. The decision about how to describe each type of information is devolved to departments to ensure descriptions are relevant and useful at the business level. Departments are also asked to say how long they need to keep each information type for business, legal or archival purposes, whether there are sensitivity issues with any type, where the information is stored, whether the information type is a key asset, whether any information type is no longer needed for any purpose, and the size of the data.

Completed spreadsheets could look like this:

Information Type	How long to keep	Sensitivity	Where stored	Key Corporate asset	Can be destroyed now	Data size
Strategic planning	Long term	FOIA exemptions	EDRMS	Yes	No	Small
Public complaints	Medium term	DPA	Standalone Database	No	No	Small
Building plans	Long term	No	Paper files	Yes	No	Small
Project X	Short term	No	Shared drive	No	No	Small
Weblog files	Short term	DPA	Server Z	No	Yes	Large

The Information Management team collates every spreadsheet into a single workbook. This forms the nucleus of the organisation's Information Audit Register. The information management team are then able to:

- identify information types which need protection, e.g. personal data, and to review whether the arrangements are adequate
- identify with the IT team which information/data can be immediately destroyed
- allocate retention schedules to the information types
- analyse the location patterns of information and decide, for instance, whether some information types should be transferred from shared drives to the EDRMS
- identify key corporate information groups and assess whether these are being utilised sufficiently.

After this exercise, the IT and IM teams have decided to expand the Information Audit to include fields about technical issues, e.g. suitability of systems for the information type, and file format obsolescence, and technical and business change issues which might impact information, to ensure digital continuity can be assured.

2. Managing change

An organisation uses an EDRMS to store and access all their digital files. The organisation has decided to migrate to a new system for several business reasons, including cost and license terms. The information stored within the system covers everything from financial data with access restrictions and legal requirements for storage, through to trivial documents which have no further use to the organisation.

As a first step, the change managers perform a high-level audit of the information within the system, grouping the information into manageable groups defined by the different business divisions within the organisation. Each information group is assigned an Information Officer in that business division who is then given the responsibility of filling out a form to establish the usability required by that asset.

The Information Officers are encouraged to take this opportunity to review the information they have stored, deleting files which are no longer of use, tidying filing structures and improving the metadata associated with each file. Once the Information Officers have completed their forms, the change managers can compile the information into a centralised list of the information groups and their requirements. They can then use this list to make sure the requirements are met by the new system and that the assets can be transferred without losing any information. Test plans can be written, based on the list, to assure that everything has been transferred successfully.

If this kind of change was undertaken without a thorough audit first, no one would fully understand what functionality was required from the new system, which could lead to too little, or even too much, expensive functionality in the system. Technology changes are a key threat to digital continuity, as it is very easy to lose necessary usability information during transfer.