



# INFORMATION ASSET REGISTER AND RISK ASSESSMENT POLICY

**BADGER GROUP**  
Badger House  
121 Glover Street  
Birmingham, B9 4EY

Please Destroy All Previous Issues

This document is the property of Badger and must not be reproduced, published or used by any third party without prior written authorisation from Badger.

Author	Issue Date	Version	Document Ref	Approved By	Approval Date	Next Review	Page i
IG Lead	Sept 2023	V3.4	IG-15	IGSG	Sept 2023	Sept 2025	

# Contents

- 1 INTRODUCTION.....1
- 1.1 Information Assets (IAs).....1
- 2 Information Asset Register.....1
- 3 INFORMATION RISK MANAGEMENT AND ASSESSMENT .....2
- 3.1 Key definitions: .....2
- 3.2 Risk Assessment Process .....2
- 3.3 Scoring Matrix.....3
- 4 ASSESSMENT PROCESS AND RESULTS .....3
- 4.1 Methodology .....3
- 4.2 Results.....3
- 4.3 Recommendations Arising.....4
- 5 APPENDIX 1 – INFORMATION ASSET REGISTER AND RISK ASSESSMENT .....5
- 6 APPENDIX II - IT INFRASTRUCTURE RISK ASSESSMENT .....6

# DOCUMENT CONTROL

## Document Storage

Location: P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IG Soc - GDPR Policies\IG-15 - Information Asset Register Risk Assessment Policy V3.4.docx

## Version Control Log (Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V3.2	Sept 2019	S Barnes	Reviewed, minor change
V3.3	Apr 2022	A Savage	Reviewed, no changes
V3.4	Sept 2023	J Carey	Reviewed

## Approval

Version	Name	Position	Signature	Approved Date
V2.6	Badger Executive	Executive Team		11 Dec 2014
V3.0	IGSG	IG Steering Group		09 March 2017
V3.1	Badger Executive	Executive Team		25 July 2019

## Glossary

Term	Description
SIRO	Senior Information Risk Manager
IAO	Information Asset officer
ISO	Information Security Office
IGSG	Information Governance Steering Group

## 1 INTRODUCTION

Information Governance requires the recording and regular review and risk assessment of both Information and physical assets. These assets are documented within their respective databases and will be reviewed twice yearly and updated following any change.

### 1.1 Information Assets (IAs)

Information Assets are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. Information Assets will likely include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data, though Information Assets should not be seen as simply technical. There are many categories of Information Asset including:

- Information. Databases, system documents and procedures, archive media/data, paper records etc.
- Software. Application programs, system, development tools and utilities.
- Physical. Infrastructure, equipment, furniture and accommodation used for data processing.
- Services. Computing and communications, heating, lighting, power, air-conditioning used for data processing.
- People. Their qualifications, skills and experience in use of information systems.
- Intangibles. For example, public confidence in the organisation's ability to ensure the confidentiality, integrity and availability of personal data.

As these categories suggest, Information Assets are not necessarily tangible objects; business processes and activities, applications and data should all be considered as Information Assets, however, their degree of importance to the organisation may vary.

## 2 INFORMATION ASSET REGISTER

Badger will undertake a programme of activity to ensure that all Information Assets are identified and assigned to an Information Asset Owner (or equivalent).

Badger's Senior Information Risk Owner will oversee a review of the organisation's information asset register to ensure it is complete and robust.

All information assets will be identified and included in this information asset register. The information asset register will also record business criticality, risk level, the risk owner, the information asset owner (or equivalent), and details of all risk assessments carried out.

The information asset register will be organised by service, rather than location. This information asset register links all the categories listed above and makes good risk management sense to group all of the components that relate to the same information asset or business process together. For example, IT system, its system documentation, its physical location, the data held within it and the skills of staff who administer it into one information asset category.

### 3 INFORMATION RISK MANAGEMENT AND ASSESSMENT

#### 3.1 Key definitions:

- **Risk:** The chance of something happening, which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.
- **Consequence:** The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Likelihood:** A qualitative description or synonym for probability or frequency.
- **Risk Assessment:** The overall process of risk analysis and risk evaluation.
- **Risk Management:** The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment:** Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
  - a. Avoid the risk
  - b. Reduce the likelihood of occurrence
  - c. Reduce the consequences of occurrence
  - d. Transfer the risk
  - e. Retain/accept the risk
- **Risk Management Process** The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

#### 3.2 Risk Assessment Process

The Badger risk management process as defined in IG-02 Badger Risk Management Strategy consists of the following stages:

- **Identifying risks**  
Identify the risks using formal tools such as brainstorming, or informal methods, or as feedback from visitors, staff or partners. If possible, ascertain contributory factors and the consequences.
- **Evaluating risks**  
Each risk will be assessed (scored) in terms of it's likelihood of occurrence (probability) and it's potential impact on Badger if it occurs (impact) in accordance with the scoring matrix and scoring definitions.
- **Controlling risks**  
Develop action plan(s) to mitigate each risk. Identify ownership for risk, target for completion of actions and frequency of progress report
- **Monitoring and review** on regular basis.

### 3.3 Scoring Matrix

The risk level used in the Asset Register is derived from this table.

		Rank	IMPACT				
			Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
<b>LIKELIHOOD</b>	<b>Certain</b> • Inevitable • No influence/control over event occurring	5	5 LOW	10 MODERATE	15 HIGH	20 VERY HIGH	25 VERY HIGH
	<b>Likely</b> • Regular occurrences frequently encountered Daily/weekly/ monthly • Risk is current almost certain to happen within next 12 months • More than 75% chance of occurrence	4	4 LOW	8 LOW	12 MODERATE	16 HIGH	20 VERY HIGH
	<b>Possible</b> • May occur occasionally, once or twice an year • Reasonable possibility it will happen within the next 3 years • 31% - 50% • Has happened in the past	3	3 VERY LOW	6 LOW	9 MODERATE	12 MODERATE	15 HIGH
	<b>Unlikely</b> • Occurs infrequently, but remains a possibility	2	2 VERY LOW	4 LOW	6 LOW	8 LOW	10 MODERATE
	<b>Rare</b> • Has happened rarely/never before • Less than 10% chance of occurrence	1	1 VERY LOW	2 VERY LOW	3 VERY LOW	4 LOW	5 LOW

## 4 ASSESSMENT PROCESS AND RESULTS

### 4.1 Methodology

Assessments will be carried out by a group nominated by the IGSG and typically including the SIRO, IG Lead, IAO and the members of the technical team.

- All systems, storage and information flows. will be identified, along with the current arrangements.
- Any system or security incidents since the last review will be reviewed.
- All aspect of information flow, storage, access and security will be discussed in detail, and the risk assessed using the scoring matrix.

### 4.2 Results

A proforma of how results will be collated can be found at Appendix I. The results will be produced in a report containing a narrative summary of findings including any resulting actions and risk reduction necessary to safeguard the business. A concurrent IT infrastructure physical asset register assessment will be undertaken to ensure that all facets of asset management (information and physical) are considered as part of the risk assessment and audit of assets.

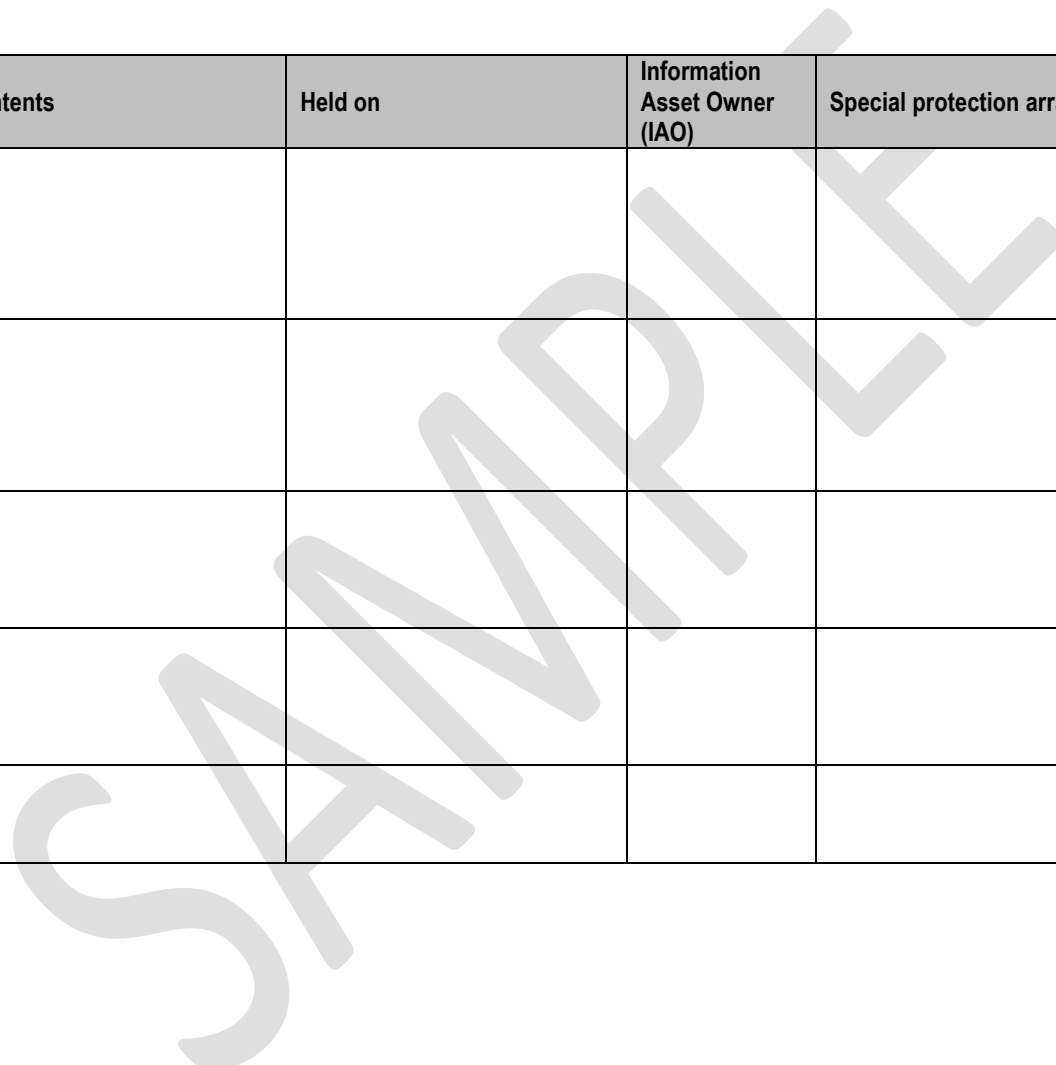
The IT Infrastructure physical risk assessment proforma can be found at Appendix II.

### 4.3 Recommendations Arising

Badger will document all recommendations, and this will be underpinned by an action plan with assigned owners that will be tracked monthly at the IGSG and reported on quarterly to the Badger Executive and Badger Board.

**5 APPENDIX 1 – INFORMATION ASSET REGISTER AND RISK ASSESSMENT**

No	Information	Responsible Department	Contents	Held on	Information Asset Owner (IAO)	Special protection arrangements	Date last reviewed	Risk Level	By





**6 APPENDIX II - IT INFRASTRUCTURE RISK ASSESSMENT**

Server Name	Description	Age Of Kit / Warranty expires	Risk Impact Score	If loss occurred what would be the consequences	Downtime actions/ Controls

Low Risk



Medium Risk



High Risk



Probability

VH	1	2	3	3	3
H	1	2	3	3	3
M	1	1	2	3	3
L	1	1	2	3	3
VL	1	1	1	2	3
	VL	L	M	H	VH

**Impact**