GOVERNANCE DOCS

Legitimate Interests Assessment

Northfield Home Supplies (sample)

Personalised postal and email offers to existing loyalty card customers, based on their purchase history, across 60 stores and the online shop in the UK and Ireland.

ASSESSED	25 September 2026
METHOD	GDPR and UK GDPR Article 6(1)(f): the purpose, necessity and balancing tests, following EDPB Guidelines 1/2024 and ICO guidance
IN SCOPE	8 scope items, 13 risks
APPETITE	Medium and below (level 9 or less) accepted without treatment
PROFILE	Retail and e-commerce
PREPARED BY	Governance Docs

Confidential. Prepared for Northfield Home Supplies (sample). Contains details of a processing activity, its impact on the people concerned and the safeguards that address it; share on a need-to-know basis.
Based on a self-assessment using information supplied by the organization. Not independently verified by Governance Docs; see "Basis of this report and limitation of liability".

CONTENTS

Where the organization's risks stand

PROCESS SCORE

93 / 100

Level 4 · Managed

Owned, justified and accepted: ready for management review and audit.

Initial | Developing | Defined | **Managed**

The score measures how complete and defensible the assessment is, not how risky the organization is.

RISKS	ABOVE APPETITE	CRITICAL	ABOVE AFTER TREATMENT	FINDINGS
13	3	0	0	3

WHAT THIS ASSESSMENT TELLS YOU

- Legitimate interests assessment needed: Legitimate interests may be available. Complete the three-part test: the purpose, the necessity and the balance. Factors calling for extra care: 2 of seven, so weigh the balance carefully and consider whether a DPIA is also needed.
- No High or Critical impact on the people concerned remains once the planned safeguards are in place, so the balance can favour the processing on those terms.
- 3 of 12 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, special category data is used or inferred, at level 12 (High), owned by Marketing Manager.
- Planned treatment brings the number of risks above the line from 3 to 0.

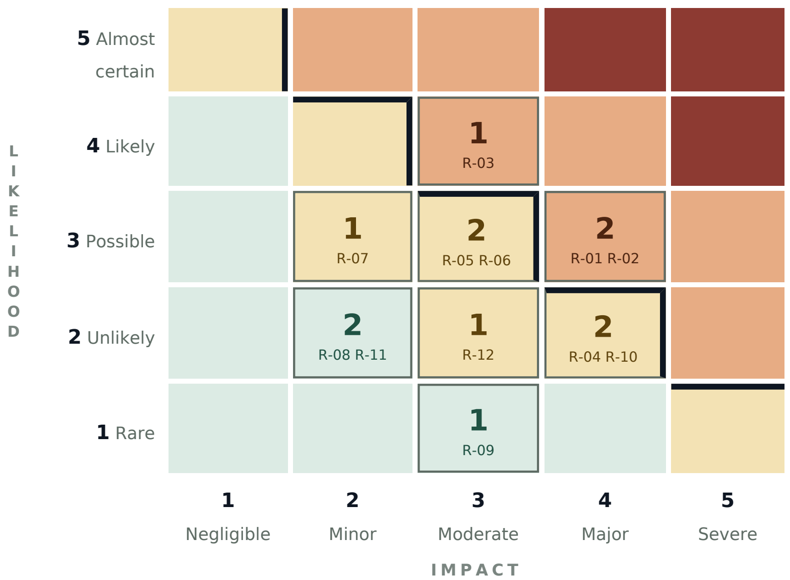
DO THESE FIRST

	SEVERITY	ACTION	RISKS	OWNER	DOCUMENT THAT CLOSES IT
1	MAJOR	**Not yet rated for likelihood and impact** Rate each one against the likelihood and impact scales in your criteria.	R-13	Marketing Manager	Risk assessment and treatment methodology
2	MAJOR	**Risk with no owner** Name an owner, by role, for each risk.	R-12	To assign	Risk assessment and treatment methodology
3	MAJOR	**Scope item with no risks identified** Link an existing risk to it, add a new one, or take it out of scope.	Customer contact details	To assign	Records of processing and LIA

Heat maps: today and after treatment

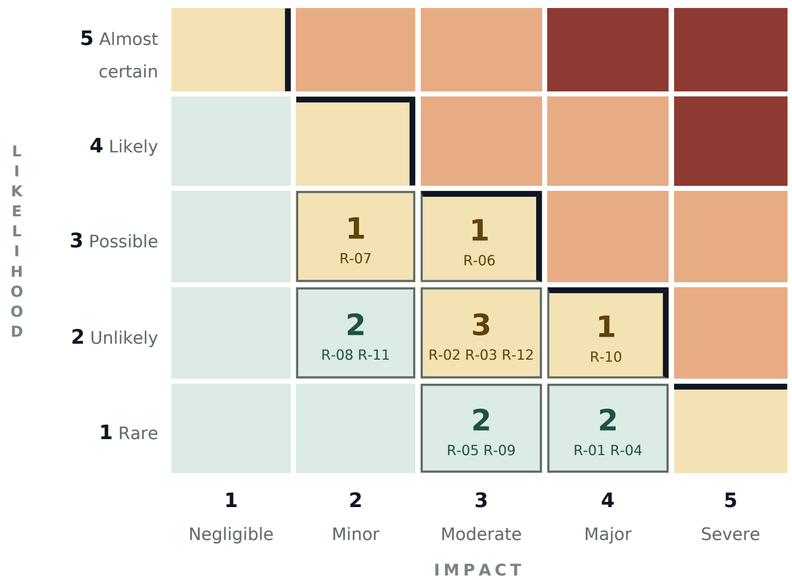
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

Current risk levels



12 of 13 risks rated.

Target levels after treatment



12 risks plotted; 0 removed by avoidance; risks above the line with no decision are not plotted.

Low 1–4 · Medium 5–9 · High 10–16 · Critical 17–25 · Appetite line

RISKS BY LEVEL

3 Low	6 Medium	3 High	1 Not rated

Analysis and priorities

IN ONE SENTENCE

Legitimate interests can support personalised offers once sensitive product ranges are excluded, history is cut to two years and the privacy notice explains the profiling.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our legitimate interests assessment confirms we can keep sending personalised offers to loyalty customers, provided we stop using health-related purchases, keep only two years of history and tell customers clearly how offers are chosen. These changes are due before the next campaign.

WHERE YOU STAND	The screening found that legitimate interests is available for personalised offers to loyalty customers, with two factors calling for extra care: profiling and direct marketing. You have recorded 13 impacts on customers across 8 scope items, and 12 are rated. Your process score is 93 out of 100, at the Managed level.
WHAT IT MEANS FOR THE ORGANIZATION	3 impacts sit above your appetite line, all of them High: offers that could reveal a health condition, a detailed profile built from five years of purchases, and a privacy notice that does not explain the profiling. Planned safeguards bring all three within appetite, so the balance can favour the processing on those terms.
WHERE TO FOCUS FIRST	Exclude the sensitive product ranges and update the privacy notice before the next campaign, since both are conditions of the DPO's advice. Then rate the pricing impact, name an owner for the combining risk and link the contact details to at least one impact.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Exclude health-related ranges from offers** R-01 Special category data is used or inferred	Offers based on mobility, continence or first aid purchases can reveal or suggest a customer's health.	Agree the excluded product list with the DPO and remove those ranges from the segment rules.	Legitimate Interest Assessment Form	30 DAYS
2	**Explain the profiling in the privacy notice** R-03 People are not told about the processing	Customers cannot judge whether to object to profiling they have not been told about.	Add a short section on how offers are chosen, the interest relied on and how to opt out.	Privacy Notice Procedure	30 DAYS
3	**Cut purchase history to two years** R-02 Profiling builds a detailed picture of people · R-05 Data is kept longer than the interest needs	Five years of item-level purchases builds a far more detailed picture than the offers need.	Set up the monthly deletion of older history and switch segments to product categories.	Retention Policy	60 DAYS
4	**Rate the effect of different offers by segment** R-13 People are disadvantaged financially · Not yet rated for likelihood and impact	Some customers may see better discounts than others, and an unrated impact cannot be weighed in the balance.	Compare offer values across segments from the last campaign and rate the impact.	Risk assessment and treatment methodology	30 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Exclude sensitive product ranges from segments.
- Publish the updated privacy notice.
- Send the suppression list to the printing house daily.

DAYS 31 TO 60

- Delete purchase history older than two years.
- Move to category-level segments.
- Rate the pricing impact and name an owner for the combining risk.

DAYS 61 TO 90

- Check complaints and opt-out rates after the first campaign.
- Review the excluded product list for the new season.

Can legitimate interests be used? The screening

Legitimate interests assessment needed

Legitimate interests may be available. Complete the three-part test: the purpose, the necessity and the balance. Factors calling for extra care: 2 of seven, so weigh the balance carefully and consider whether a DPIA is also needed.

Screening note: Northfield is a private company, so legitimate interests is available. Offers are not necessary for the loyalty contract, and no law requires them. Emails go only to customers who bought from us and did not opt out when asked (the soft opt-in under PECR and the Irish ePrivacy rules); postal offers need no consent. Consent was considered and not chosen because customers already expect offers from the loyalty scheme. Profiling and direct marketing call for care in the balance.

Whether legitimate interests is available: any "yes" points elsewhere	Met
You are a public authority, and the processing is part of performing your official tasks	No
Other rules require consent for this activity	No
Another lawful basis clearly fits better	No
UK only: the purpose is a recognised legitimate interest in Annex 1 of the UK GDPR	No

Factors that call for extra care in the balance	Met
It involves special category or criminal offence data	No
It involves children's data	No
People may not reasonably expect it	No
It involves profiling, tracking or monitoring	**Yes**
The data comes from third parties, or the processing is invisible to people	No
It is for direct marketing	**Yes**
There is an imbalance of power between you and the people concerned	No

The purpose test

What the processing is for, the interest it serves, whose interest it is, and why it is legitimate. The data, systems, people and suppliers involved are listed with the register.

The purpose of the processing	Send loyalty card customers up to two postal and four email offers a month, chosen from the product ranges they have bought from before.
The legitimate interest, and whose it is	Northfield's commercial interest in direct marketing to its own customers (Recital 47 recognises direct marketing as a possible legitimate interest). Customers also benefit from offers on products they actually buy.
The benefit, and what happens without the processing	Targeted offers are redeemed about three times as often as untargeted mailings, and halve the paper sent to customers. Without segmentation, every customer would get the full catalogue each month.
Why the interest is lawful, clear and real	Direct marketing to existing customers is lawful when the ePrivacy rules are met and people can object. The interest is specific (offers from our own ranges) and present, not speculative. The scheme follows the Data and Marketing Association code.
The personal data and where it comes from	Name, postal address, email address, loyalty card number, and items bought in store and online over the last five years. All collected directly from customers through the loyalty scheme.
The people concerned and your relationship with them	About 410,000 loyalty card customers aged 18 or over. They signed up for the scheme, which offers points and member offers, and most shop with us several times a year.
Who receives the data	Email service provider and direct mail printing house (both processors). No data is sold or shared for others' marketing.
How long the data is kept	Purchase history kept for segmentation for two years (reduced from five); contact details until the customer leaves the scheme.

The necessity and balancing tests

The necessity test asks whether the processing is needed for the purpose, or whether a less intrusive way would do. The balancing test asks whether the interests, rights and freedoms of the people concerned override yours. Every "partly" or "no" says what is missing.

Question	Answer	Explanation or evidence
Necessity: the processing actually helps achieve the purpose	Yes	Segmented offers redeemed at 4.1% against 1.3% for the full catalogue in a 2025 test.
Necessity: it is a reasonable and proportionate way to achieve it	Yes	A monthly frequency cap keeps contact within what members signed up for.
Necessity: there is no less intrusive way to achieve the same result	Partly	Category-level segments were considered; they work almost as well with less detail, and will replace item-level segments for sensitive ranges.
Necessity: only the personal data the purpose needs is used	Partly	All five years of history were used; reduced to two years from the next campaign.
Balance: people would reasonably expect the processing, given your relationship with them	Yes	The scheme sign-up page says members receive offers based on what they buy.
Balance: people are told about the processing and the interest in your privacy notice	Partly	The privacy notice covers marketing but does not explain the profiling or name the interest; being updated.
Balance: people can object easily, and an objection to direct marketing always stops it	Yes	Unsubscribe link in every email and a freepost or online opt-out for post; one suppression list applied to both channels.
Balance: children's interests are protected, or no children are involved	Yes	Scheme membership is for adults only; date of birth checked at sign-up.
Balance: safeguards limit the impact on people (minimisation, retention, security, opt-outs)	Partly	Sensitive product ranges to be excluded from segments; access to the CRM limited to the marketing team.
Balance: any imbalance of power is taken into account, and people are not pressured	Yes	Customers can shop without the card; there is no pressure to join or stay.

The ways the processing could affect the people concerned follow in the register, rated for them and not for the organization, with the safeguards that tip the balance and the GDPR articles they help meet.

What was in scope

The personal data, people concerned, processing step, system or technology, processor or recipient and location or transfer the assessment covered, with their owners.

Type	Scope item	Owner	Risks
Personal data	**Purchase history**	Marketing Manager	4
Personal data	**Customer contact details**	Marketing Manager	**0**
People concerned	**Loyalty card customers**	Chief Customer Officer	2
Processing step	**Customer segmentation**	Marketing Manager	3
Processing step	**Postal and email offers**	Marketing Manager	3
System or technology	**CRM and marketing platform**	IT Manager	2
Processor or recipient	**Email service provider**	Procurement Manager	1
Processor or recipient	**Direct mail printing house**	Procurement Manager	2

Risk register

Every risk, highest level first. Level = likelihood x impact, rated with the controls already in place. The rationale is the organization's own reason for the rating. The full scenario for each risk (threat, weakness and consequence) is in the workbook.

#	Ref	Risk scenario	Scope items	Harm to people	Owner	Existing controls	L	I	Level	Rationale
1	R-01	**Special category data is used or inferred** Weakness: No Article 9 condition identified alongside legitimate interests	Purchase history, Customer segmentation	Confidentiality lost, Loss of control, Physical or emotional harm	Marketing Manager		3	4	12 · High	Mobility, continence and first aid products are in the catalogue and feed the segments, so an offer can reveal or suggest a health condition.
2	R-02	**Profiling builds a detailed picture of people** Weakness: Profiles go further than the purpose needs, with no opt-out	Purchase history, Customer segmentation	Loss of control, Discrimination, Surveillance	Marketing Manager	Segments limited to product ranges	3	4	12 · High	Five years of item-level purchases build a detailed picture of each household.
3	R-03	**People are not told about the processing** Weakness: The notice does not name the purpose or the legitimate interest relied on	Loyalty card customers	Loss of control, Rights obstructed	Data Protection Officer	Privacy notice covers marketing	4	3	12 · High	The notice does not mention profiling or the interest relied on, so customers cannot judge whether to object.
4	R-05	**Data is kept longer than the interest needs** Weakness: No retention period tied to the legitimate interest	Purchase history, CRM and marketing platform	Confidentiality lost, Loss of control	Marketing Manager		3	3	9 · Medium	Purchase history has been kept since the scheme started in 2019 with no deletion.

5	R-06	**Contact or disclosure causes distress** Weakness: No thought given to how the contact lands for the person	Postal and email offers	Confidentiality lost, Physical or emotional harm	Marketing Manager	Complaints handled by customer services	3	3	9 · Medium	Three complaints in 2025 about offers linked to items bought for a relative who had since died.
6	R-04	**Direct marketing continues after someone objects** Weakness: Suppression lists not shared or not applied	Postal and email offers, Direct mail printing house	Loss of control, Rights obstructed, Physical or emotional harm	Marketing Manager	Unsubscribe link and suppression list	2	4	8 · Medium	The printing house receives the suppression list weekly, so a postal offer can still arrive after an objection.
7	R-10	**The data is exposed in a breach** Weakness: Security not matched to the data and its volume	CRM and marketing platform	Confidentiality lost, Financial loss, Physical or emotional harm	IT Manager	Encryption, role-based access, access logging	2	4	8 · Medium	Large customer file; access limited to 14 marketing staff.
8	R-12	**Datasets are combined in ways people would not expect** Weakness: The combined effect on people was never assessed	Customer segmentation	Loss of control, Discrimination, Surveillance	**None**		2	3	6 · Medium	Online and in-store purchases are joined through the card number.
9	R-07	**More personal data is used than the purpose needs** Weakness: No review of which data the purpose actually needs	Purchase history	Confidentiality lost, Loss of control	Marketing Manager		3	2	6 · Medium	Store and time of purchase are held but not needed for offers.
10	R-08	**Objecting or opting out is difficult** Weakness: No simple opt-out; the route is hidden or needs an account	Postal and email offers	Loss of control, Rights obstructed	Marketing Manager	Freepost opt-out	2	2	4 · Low	Postal opt-out takes up to 28 days to apply.
11	R-11	**People would not reasonably expect this use of their data** Weakness: Nobody checked what people expect, and the use is not obvious from the context	Loyalty card customers	Loss of control, Rights obstructed	Chief Customer Officer	Scheme terms mention member offers	2	2	4 · Low	Members sign up for offers; panel feedback confirms they expect them.

12	R-09	**A supplier uses the data for its own purposes** Weakness: Terms not reviewed before the data is shared	Email service provider, Direct mail printing house	Confidentiality lost, Loss of control	Procurement Manager	Processor contracts reviewed in 2025	1	3	**3 · Low**	Both contracts forbid use of the data for the supplier's own purposes.
13	R-13	**People are disadvantaged financially** Weakness: Effects on different groups not tested	**None linked**	Discrimination, Financial loss	Marketing Manager		–	–	**Not rated**	

What will be done, by whom and by when

Every risk with a treatment decision, earliest due date first. The data protection safeguards listed are the ones the treatment relies on; they carry into the lia safeguards plan. Acceptance is the risk owner's approval of the plan and of the risk that remains.

Ref	Risk	Decision	Planned actions	Data protection safeguards	Owner and due date	Current to target	Accepted
R-01	**Special category data is used or inferred** Marketing Manager	**Modify**	Exclude sensitive product ranges from segmentation and from offer selection; review the excluded list each season.	DP.9 Special category condition documented (Art 9, 10) DP.20 Privacy by design and by default (Art 25) DP.1 Data minimisation (Art 5(1)(c))	Marketing Manager 31 Oct 2026	12 · High → 4 · Low	Chief Customer Officer 22 Sep 2026
R-03	**People are not told about the processing** Data Protection Officer	**Modify**	Update the privacy notice and the scheme sign-up page to explain the segmentation, the interest and how to object.	DP.6 Privacy notice and transparency (Art 12 to 14) DP.13 Right to object and opt-out (Art 21)	Data Protection Officer 31 Oct 2026	12 · High → 6 · Medium	Chief Customer Officer 22 Sep 2026
R-04	**Direct marketing continues after someone objects** Marketing Manager	**Modify**	Send the suppression list to the printing house daily and check it before every print run.	DP.13 Right to object and opt-out (Art 21) DP.14 Processor contract and due diligence (Art 28)	Marketing Manager 31 Oct 2026	8 · Medium → 4 · Low	Chief Customer Officer 22 Sep 2026
R-02	**Profiling builds a detailed picture of people** Marketing Manager	**Modify**	Limit history to two years and move to category-level segments.	DP.1 Data minimisation (Art 5(1)(c)) DP.23 Purpose limitation controls (Art 5(1)(b))	Marketing Manager 30 Nov 2026	12 · High → 6 · Medium	Chief Customer Officer 22 Sep 2026
R-05	**Data is kept longer than the interest needs** Marketing Manager	**Modify**	Delete item-level history older than two years each month.	DP.5 Retention schedule and deletion (Art 5(1)(e))	IT Manager 31 Dec 2026	9 · Medium → 3 · Low	**Not recorded**

7 risks are within appetite (Medium and below) and need no treatment; 1 are not yet rated.

Where the assessment falls short

Each finding is a gap between the assessment as recorded and what GDPR Article 6(1)(f) ask for, with the risks it applies to and the document that closes it.

Severity	Finding	Applies to	What it means	To fix	Document that closes it
MAJOR	**Not yet rated for likelihood and impact**	R-13	Without both ratings a risk has no level, so it cannot be compared with the appetite line or placed in priority order.	Rate each one against the likelihood and impact scales in your criteria.	Risk assessment and treatment methodology
MAJOR	**Risk with no owner**	R-12	Each impact needs an owner who can put the safeguards in place. Without one, the LIA records an impact nobody will reduce.	Name an owner, by role, for each risk.	Risk assessment and treatment methodology
MAJOR	**Scope item with no risks identified**	`Customer contact details`	Something you put in scope has no risk attached to it. Either it faces no credible risk, which is rare, or the identification step missed it.	Link an existing risk to it, add a new one, or take it out of scope.	Records of processing and LIA

PROCESS SCORE IN DETAIL

Criteria defined Every likelihood and impact level has a definition, and the appetite line is set.	**100%**	11 of 11	weight 10
Scope covered Every scope item has at least one risk linked to it.	**88%**	7 of 8	weight 10
Risk owners named Every risk has an owner accountable for it.	**92%**	12 of 13	weight 15
Risks rated Every risk has a likelihood and an impact, so it has a level.	**92%**	12 of 13	weight 15
Ratings explained Existing controls and a rationale are recorded for each risk.	**77%**	20 of 26	weight 10
Treatment decided Every risk above the appetite line has a treatment option chosen.	**100%**	3 of 3	weight 15
Targets within appetite Treatments bring each risk to a target at or below the line.	**100%**	3 of 3	weight 10
Treatments scheduled Each treatment has an owner and a due date.	**100%**	3 of 3	weight 5
Residual risk accepted Risk owners have accepted what remains after treatment, by name and date.	**100%**	3 of 3	weight 10
LIA record complete Screening, the purpose test, the necessity and balancing tests, data protection advice, the conclusion and the review date are all recorded.	**90%**	19 of 21	weight 25

Findings by severity

1 · Initial (0+)
A start on a register, not yet an assessment that decisions can rest on.

2 · Developing (40+)
The risks are identified, but gaps in rating or treatment would not survive an audit.

3 · Defined (60+)
A complete, repeatable assessment with a treatment plan behind it.

4 · Managed (80+)
Owned, justified and accepted: ready for management review and audit.

Can you rely on legitimate interests?

RESIDUAL IMPACT: DOES THE BALANCE FAVOUR THE PROCESSING?

No High or Critical impact on the people concerned remains once the planned safeguards are in place, so the balance can favour the processing on those terms.

DATA PROTECTION ADVICE

Who advised	A DPO is designated and gave advice
Advice	DPO: legitimate interests can apply if mobility, continence and first aid ranges are excluded from segments, purchase history is limited to two years, and the privacy notice explains the profiling and the right to object before the next campaign.
Followed	Yes

VIEWS OF THE PEOPLE CONCERNED

Views	Sought, and summarised below
Summary or reason	Customer panel of 30 loyalty members: most expected offers based on what they buy and valued them; several objected to offers based on health-related products, which the exclusions address.

OUTCOME AND APPROVAL

Outcome	**Legitimate interests applies once the planned safeguards are in place**
Approved by	Chief Customer Officer
Approved on	22 Sep 2026
Next review by	30 Sep 2027

Keep the LIA with your records of processing and name the interest in your privacy notice. Review it if the purpose, the data, the people or the context changes. If the people's interests override yours, legitimate interests is not available: change the processing, use another lawful basis or stop. If the processing is likely to be high risk, a DPIA is needed as well.

Criteria used and basis of this report

The balancing test asks whether the interests or fundamental rights and freedoms of the people concerned override the legitimate interest, so likelihood and severity are rated for them, not for the organization. This is the record of the criteria every rating in this report was made against.

LIKELIHOOD SCALE

Value	Label	Definition
1	**Rare**	Not expected in the next 5 years; no known case here or in the sector
2	**Unlikely**	Could happen once in 2 to 5 years; has happened in the sector
3	**Possible**	Could happen about once a year
4	**Likely**	Expected several times a year
5	**Almost certain**	Expected monthly or more often, or already happening

IMPACT SCALE

Value	Label	Definition
1	**Negligible**	Negligible: people are not affected, or only trivially
2	**Minor**	Minimal: minor inconvenience people overcome without difficulty
3	**Moderate**	Significant: real inconvenience, distress or cost people can overcome with some difficulty
4	**Major**	Serious: significant consequences such as discrimination, fraud, financial loss or damage to reputation
5	**Severe**	Severe: serious, lasting or irreversible harm, such as to health, livelihood or safety

RISK LEVELS AND ACCEPTANCE

Band	Levels	Treatment
Low	1–4	Accepted without treatment
Medium	5–9	Accepted without treatment
High	10–16	Needs a treatment decision
Critical	17–25	Needs a treatment decision

Level = likelihood x impact. A risk above the appetite line may still be retained, but only with the risk owner's recorded acceptance.

Process score. Ten dimensions: nine for the register, each the share of risks (or of risks above the line) that meet it, and one for the completeness of the LIA record. Each is multiplied by its weight and the total is scaled to 100. A dimension with nothing in scope counts in full. Any critical finding holds the level at Developing, whatever the score.

Your workbook. The Excel workbook that comes with this report is the register as a working file. Change a likelihood or impact on the Risk register sheet and every level, the heat maps on the Dashboard and the process score recalculate. It also holds the treatment plan and a list of the data protection safeguards your treatments rely on.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The risks, ratings, risk levels, treatment decisions, findings, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.