NS&I Risk Management Framework

Status:	**Final**
Version:	**4.2**
Date:	03.09.2025
Amended by:	Neil Edwards
Next Review	03.09.26

Scope

The NS&I Risk Management Framework (RMF) applies to both the corporate centre of NS&I, NS&I programmes, and outsourced services.

Our strategic suppliers — Atos, IBM, and Sopra Steria — must follow the RMF. They're expected to show they have strong risk controls and governance, as outlined in government standards (and the HMT Orange Book).

The data they provide on risks and controls is essential. It helps NS&I track risk across all outsourced services, especially where they interact with customers. These suppliers must also oversee risk within their own supply chains, with NS&I's Commercial Team keeping oversight.

Other (non-strategic) suppliers aren't part of this framework but must still prove they have solid internal controls. This is checked during procurement, onboarding, and contract reviews.

Risk Culture

At NS&I, managing risk is part of how we work every day. Our culture — backed by leadership and the Board — supports responsible decision-making and doing the right thing.

We take a balanced approach: encouraging innovation, but only within clear risk boundaries. Everyone at NS&I is expected to manage risks as part of their role.

We aim for a positive risk culture where issues are identified early, understood, and handled properly — so we can keep delivering safely and responsibly.

Risk Management Framework: Objectives

NS&I's Risk Management Framework (RMF) sets out how we manage risk across the organisation. Its main goals are to:

- Help the CEO (Accounting Officer) meet government standards, including the Orange Book, by ensuring we have clear policies and processes for identifying, assessing, and managing risk.
- Provide clear principles that both NS&I and its suppliers can use to ensure a sound system of risk management, in support of our 'You're in safe hands' customer principle.
- Define and communicate the Board's risk appetite so that decisions — whether to take or avoid risk — are informed and aligned.
- Maintain a Risk Universe: a list of NS&I's key risks (Operational, Strategic, and Transformation), each owned by an Executive Committee member and regularly reviewed.
- Ensure we collect, collate and analyse reliable risk and control data from both inside NS&I and our suppliers, so we can monitor key risks and act when needed.
- Ensure that when a risk goes beyond our appetite, action is taken — either by NS&I or through supplier oversight — to bring it back within acceptable limits.
- Provide regular risk reports to senior committees (ERC, ARC and Board) on our principal risks and how they're being managed.

HMT Orange Book

The Orange Book sets out the government's official principles for managing risk. NS&I's RMF and risk management system are aligned to the Orange Book (with one deviation, the use of the term vulnerabilities instead of event within the construct of a risk). The Orange Book states:

- Risk management must be part of leadership and governance at every level.
- It should support decision-making and be built into day-to-day activities.
- It must be collaborative and based on solid evidence.
- Risk processes must cover:
  - Identifying and assessing risks
  - Choosing how to manage them
  - Monitoring progress
  - Reporting in a clear and timely way
- Organisations must keep learning and improving how they manage risk. NS&I follows these principles by putting them into action through our RMF.

Government Functional Standards

NS&I's RMF reflects and builds upon risk management and audit good practice outlined in two key government functional standards.

06: Finance

This standard, created by the Government Finance Function, outlines best practices for risk management in government.

09: Audit

This standard, created by the Government Internal Audit Agency (GIAA), outlines best practices for internal auditing in government.

GIAA is NS&I's internal auditor. Each year, they assess how well they follow this standard and report any areas that need improvement as part of their annual audit opinion.

Roles & Responsibilities

Who owns the Risk Framework?

The Risk Director is responsible for designing and maintaining NS&I's Risk Management Framework (RMF), so it meets government standards. The CEO (Accounting Officer) remains ultimately accountable for risk management.

The framework is reviewed each year by the Executive Risk Committee to make sure it's still effective. Internal audits are also carried out regularly.

What does the Risk Team do?

The Risk Team makes sure NS&I has strong, practical risk management in place. Their job includes:

- Keeping our list of key risks (Risk Universe) up to date.
- Making sure NS&I and suppliers share the right data to manage risk properly.
- Checking that outsourced suppliers follow their risk obligations.
- Managing NS&I's risk tool and helping others use it.
- Supporting and challenging teams and suppliers to ensure risks are tracked, understood, and managed well.
- Providing the risk owners with data about risk policy adherence, risk exposures, breaches of appetite, the status of the control environments which they oversee, and horizon scanning for emerging and distant exposures.
- Provision of legal and regulatory compliance advice; ownership of security, fraud and financial crime, legal and regulatory risk.

What do Executive Committee (ExCo) members do?

Each ExCo member is a Key Risk Area (KRA) Owner. They must make sure their teams follow the RMF and manage risk effectively. ExCo own risk policies associated with their area of responsibility and assure internal and external adherence to relevant risk policies. They are responsible for the effective management of the risk they own, including ensuring mitigations and action plans are being delivered on time and to cost. Furthermore, they are responsible for the oversight of the internal and external control environments associated with the risks they own and manage. Each year, they confirm this by submitting a statement to the Accounting Officer.

What does a Risk Owner do?

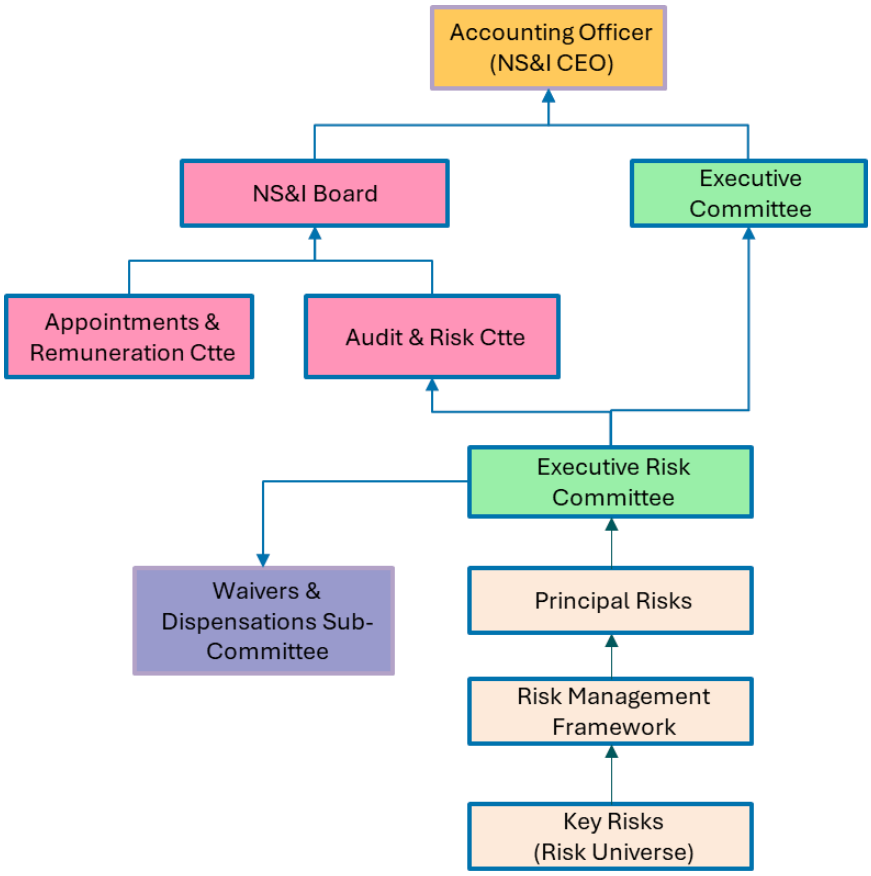
Risk Owners (may be delegated by ExCo but must be a Head of) manage specific risks. Their key tasks are:

- Document how each risk will be monitored and controlled.

- Use data (including from suppliers) to track risk levels and performance.
- Act when controls are weak or something goes wrong.
- Use the risk tool to record risks and actions taken.
- Work with the Risk Team for extra guidance and challenge.
- Report key updates to the Executive Risk Committee.

NS&I Governance Structure

The diagram below outlines the governance structure within NS&I.



Accounting Officer & Board

NS&I's Accounting Officer (the CEO) is responsible to HM Treasury and Parliament for how NS&I is run. This includes setting our risk appetite, creating a strong risk culture, and ensuring we have the resources to manage risk effectively.

The Board supports and advises the executive team but doesn't manage day-to-day operations. It ensures good governance, including having strong internal audit arrangements and a sound system of risk management in place.

Some of the Board's responsibilities around risk are delegated to the **Audit and Risk Committee (ARC)**.

Audit and Risk Committee

ARC meets quarterly and is led by an independent non-executive director. It checks whether risks are being managed in line with the Board-approved risk appetite.

If things go off track, ARC reviews how management responds and challenges decisions as needed. After each meeting, the Chair reports back to the Board. ARC can also escalate serious risk issues directly.

ARC operates in line with government internal audit standards (Functional Standard 09).

Executive Risk Committee

ERC is responsible for day-to-day risk oversight and meets every quarter. Chaired by the Risk Director, it includes the Accounting Officer, senior managers, and supplier representatives.

ERC reviews overall risk exposure focuses on our principal risks, and tracks actions being taken to manage them. Experts may be invited to provide further insights or updates.

Waivers & Dispensations Sub-Committee

WDSC, a sub-group of ERC, reviews and approves requests to either permanently or temporarily step outside of a risk policy and/or remove or reduce contractual obligations. It meets every two months and is chaired by the Risk Director.

Three Lines of Defence

NS&I uses the "Three Lines of Defence" model to manage risk:

1. **First Line** – Teams that manage risks day-to-day
2. **Second Line** – Risk teams that advise, support, and challenge
3. **Third Line** – Independent internal audit for objective assurance

1St Line of Defence *(Risk & Control owners)*	2nd Line of Defence *(Risk & Control advise & oversight)*	3rd Line of Defence *(Independent Assurance)*
• Identify, assess, own and manage risks • Design, implement and maintain effective internal control measures Supervise • execution and monitor adherence.	• Set the boundaries for delivery through the definition of standards, policies, procedures and guidance • Assist management in developing controls in line with good practice	• Provide an objective evaluation of the adequacy and effectiveness of the framework of governance, risk management and control

		• Monitor compliance and effectiveness • Agree any waivers and dispensation where requirements cannot be met • Identify and alert ERC & ARC to emerging issues and changing risk scenarios.		• Provide proactive evaluation of controls proposed by management • Advise on potential control strategies and the design of controls.

Risk Appetite

Risk appetite is the amount of risk NS&I is willing to take to achieve its goals. By clearly setting this out, we help teams understand what risks are acceptable — and where to draw the line.

These risk appetite statements guide decision-making and ensure that we stay aligned with our values and priorities. Our suppliers are required to follow these same expectations.

How it works:

- Risk appetite statements cover different types of impact (e.g. financial, operational, reputational).
- They are reviewed and agreed by the Executive Committee (ExCo) and the Board.
- Each Key Risk Area (KRA) Owner sets measures and thresholds to track performance against appetite, using a traffic light (RAG) system.
- These measures are reviewed at least once a year, or sooner if NS&I's business or structure changes.

The current set of Risk Appetite statements are:

Area	Appetite	2025-26 Risk Appetite Statements
Business Interruption having an impact on customers	Minimal Averse	NS&I has minimal appetite for unplanned loss of customer-facing services, or our ability to maintain net-financing management, for more than 48-hours.
Viability of FBC for Transformation	Minimal	NS&I is averse to any activity which may necessitate the need to seek additional funds from HMT and/or cause significant delay to the delivery of key programme milestones.

Supplier failure	Minimal	
		NS&I has a minimal appetite for protracted service disruption because of one or more suppliers failing.
	Averse	
Failure to meet Net Financing SDM		
	Cautious	NS&I has a minimal appetite for any result outside of this range and takes necessary action to remain within the end of year parameters or within any adjustments agreed with DRM during the year.
Cyber & Data Security		
		NS&I has an averse appetite for a prolonged loss of IT and/or digital services (internally and customer-facing); suffering interference with or loss of, or denial of access to data; and a breach of confidentiality.
IT Recovery		
		Due to investment constraints, we have a cautious appetite for our inability to recover systems, applications, services and data within 48 hours (period aligned to our business interruption risk and impact tolerances).
Fraud		
		NS&I is averse to any loss to customers resulting from fraud and seeks to make good any such loss. NS&I expects all parties to cooperate to recover any fraudulent payments that have been made and to adjust the control environment to prevent future instances of a similar nature.
Data Migration	Averse	
		NS&I are averse to the loss, misuse, or mismanagement of customer data. We will operate within the boundaries of UK GDPR and require third parties and outsourcing partners who access and/or store our data to adopt the same appetite. Where data is stored and transmitted in digital form, we recognise its vulnerability to cyber interference, and we will ensure and assure its protection in line with our cyber security risk appetite.
	Averse	

Risk Classification and Risk Universe

Risk Classification

NS&I manages four levels of risk:

1. **Non-Key Risks** – These are low-level, expected risks managed within teams or by suppliers. If they grow in impact, they must be escalated. Local tools (like Excel) can be used to track them, but proper data must be available if the risk becomes more serious.

2. **Key Risks** – These are more serious, unexpected risks that could significantly affect NS&I, its customers, or strategic goals. They are tracked in our live **Risk Universe**, which is regularly updated.
3. **Principal Risks** – These are the highest-priority Key Risks — those rated as high impact and high likelihood. They are the focus of reports to the Executive and Audit & Risk Committees.
4. **Crisis Scenarios (Tail Risks)** – These are rare, extreme events (e.g. pandemics, major cyber-attacks) that require a government-wide response. NS&I includes relevant scenarios in its crisis planning.

Even though the Risk Directorate doesn't track Non-Key Risks daily, they must still be managed using the same risk principles and are subject to periodic review.

Each risk in NS&I includes:

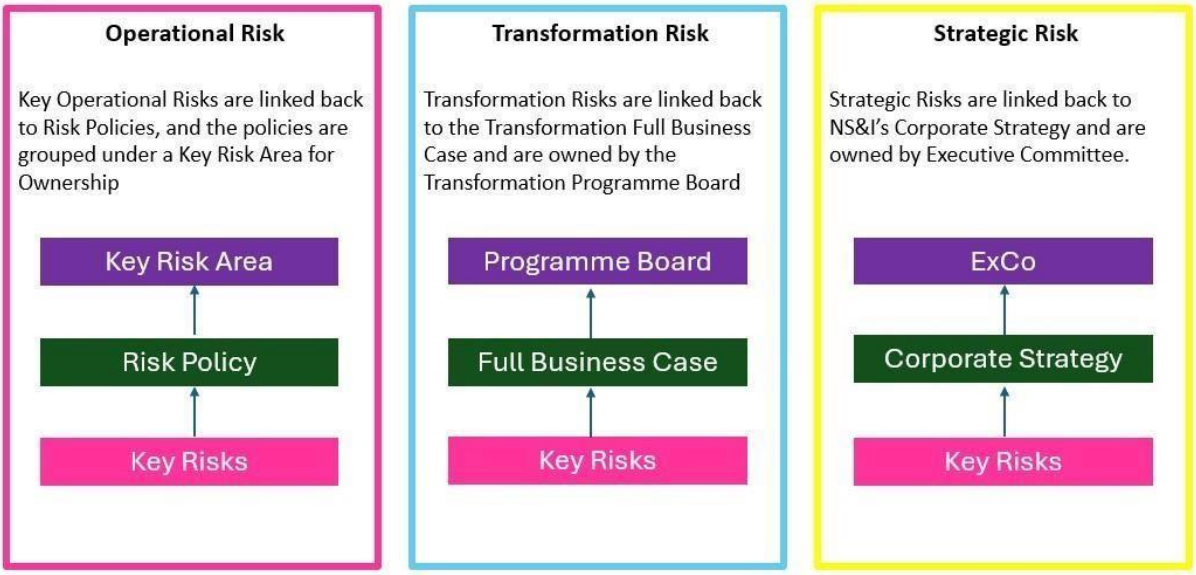
- **Description** – what the risk is
- **Vulnerabilities** – weaknesses that could lead to adverse consequences
- **Triggers** – events that could expose those weaknesses
- **Consequences** – potential impact on customers or the business

Risk Universe

The Risk Universe is NS&I's central list of Key Risks, grouped into three categories:

- **Operational Risks** – from day-to-day work by NS&I and its suppliers
- **Transformation Risks** – from change or improvement projects
- **Strategic Risks** – from challenges to achieving long-term goals

Each risk is clearly owned and tracked within this structured framework.



Risk Types

Operational Risk

Operational risks come from people, processes, technology, or external events. NS&I's biggest exposure to these risks is through our outsourced suppliers — though NS&I always remains responsible. We split operational risks into:

- **Corporate risks** – managed by NS&I
- **Outsourced risks** – managed by suppliers, but overseen by NS&I, and subject to NS&I Operational Risk

Policies

Each senior leader (Key Risk Area Owner) is responsible for identifying and managing the key risks in their area, with support from the Risk Directorate.

Key Risk Areas

NS&I has six broad areas where operational risks are managed:

1. **Enterprise Services** (IT and supplier operations)
2. **Business Delivery & Change Projects**
3. **Retail Operations**
4. **People & Finance**
5. **Regulation, Compliance & Cybersecurity**
6. **Communications & Strategy**

KRA Owners must identify, assess, monitor, and respond to risks in their area. They also oversee supplier risk and write **Operational Risk Policies** that explain how their key risks are managed. These are reviewed every year by the Executive Risk Committee.

What is an Operational Risk Policy?

Each operational risk policy describes:

- **Risk appetite** – how much risk we're willing to take
- **Losses** – what a failure or issue would look like
- **Key Risk Indicators (KRIs)** – warning signs to monitor
- **Control objectives** – what controls should be in place

Adherence to policies is achieved through Risk Owners evidencing effective controls are in place to meet control objectives, regularly accessing control test data, reviewing loss data and managing defects in the control environment incurred through waivers and dispensations.

Semi automation of operational risk management: Risk Tool: ServiceNow IRM

NS&I is rolling out a new risk tool (ServiceNow IRM) to help collect data from suppliers, track controls, and monitor actions through dashboards.

Transformation Risk

These risks come from major change or improvement projects. They're identified and managed by the Transformation Programme Risk Team and mapped to broader transformation risks in our Risk Universe. Redrated risks become principal risks by definition and are reported to and tracked by the Executive Risk Committee. Transformation risks extend beyond programme, cost and time to include operational risks to the business by failure to deliver and exposures to the business through the associated change activity.

Strategic Risk

These are high-level risks that could stop NS&I from achieving its business goals. They are reviewed each year during strategic planning by senior leadership and updated only if there's a major shift in strategy.

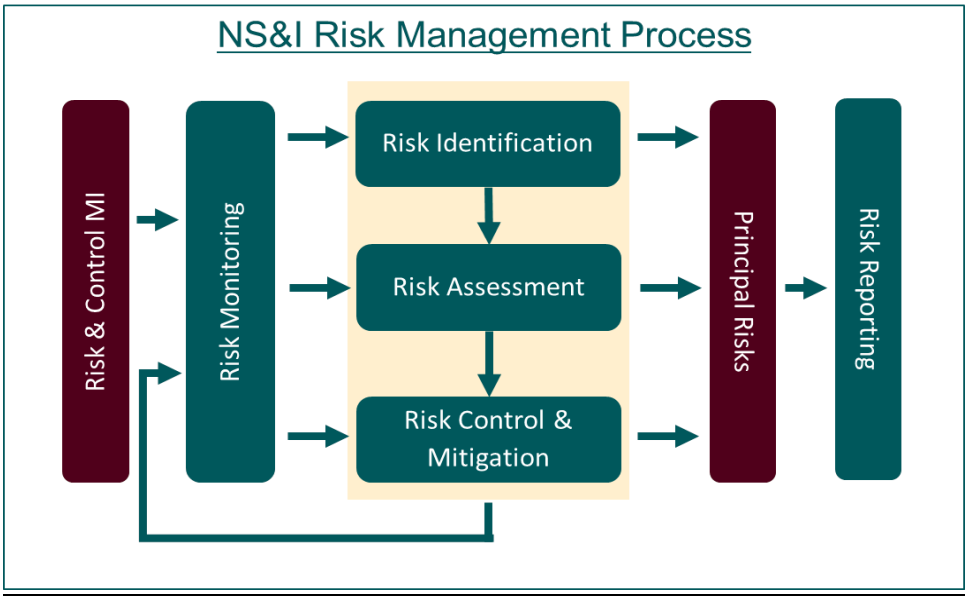
The Risk Management Process

NS&I follows a five-step cycle for managing risk:

1. **Identify** the risk
2. **Assess** how serious it is
3. **Control and Mitigate** it

4. **Monitor** ongoing risk levels
5. **Report** the status

This process is based on government and international best practice.



Risk Identification

At NS&I, a **risk** is anything uncertain that could stop us from meeting our goals or serving our customers. Identifying risks isn't a one-time task — it's an ongoing process. We look ahead to spot new or emerging risks early. Tools like **Bowtie Analysis** help break risks down into causes, weaknesses, and possible impacts. **Risk Assessment**

Once a risk is identified, we assess how serious it is. This helps us decide whether action is needed — and which risks are important enough to track in our Risk Universe.

We use a **5x5 Risk Matrix** to score risks based on **impact** and **likelihood** (both rated 1–5).

Types of Risk Ratings

- **Inherent Risk** – What the risk would look like with *no* controls in place.
- **Residual Risk** – What the risk looks like *now*, with current controls.
- **Projected Risk** – What the risk would look like *after* planned actions are completed.

What We Do About Risks?

Once a risk is assessed, we choose how to respond:

- **Treat** – Put in controls or actions to reduce the risk
- **Transfer** – Shift the risk to someone else (e.g. through a contract)
- **Tolerate** – Accept the risk if it's within safe limits
- **Terminate** – Stop the activity if the risk is too high and can't be reduced

We review these ratings and responses regularly to make sure risks stay within our acceptable limits. If a Key Risk is rated **Red** for Residual Risk, it becomes a **Principal Risk** and is formally reported to the ERC.

Risk Control & Mitigation

Controls are regular steps we take to reduce risk. There are four types:

1. **Preventative** – Stop the risk from happening

2. **Detective** – Spot issues early
3. **Directive** – Guide staff to follow the right process
4. **Corrective** – Fix problems when they occur

We track how well these controls are working using data (MI) linked to our Risk Policies.

Mitigating activities are one-time actions to reduce a risk or its impact. Risk Owners are responsible for planning and tracking these actions.

Strategic and transformation risks usually need mitigating actions, not regular controls.

Risk Monitoring

We only formally track **Key Risks** using our **Risk Tool**, which helps NS&I and our suppliers monitor risks and controls.

- **Risk Owners** must work with the Risk Team to make sure the right data (MI) is collected and added to the tool.
- For internal (corporate) risks, NS&I enters the data.
- For outsourced risks, suppliers provide most of the data, as required by their contracts.

What We Monitor and Why:

Data Type	Why It Matters	What to Do
Key Risk Indicators	Show if a risk is rising or falling.	Investigate trends and take action if performance is worsening.
Key Control Indicators	Show if controls are working.	Check supplier evidence, sample test if needed ("trust but verify").
Losses	Reveal when a risk has occurred (e.g. fraud, complaints).	Spot trends and justify fixing weak areas.
Risk Events	Incidents or breaches that expose control failures.	Make sure root causes are identified, and fixes are properly delivered.
Waivers/Dispensations	Show where a risk policy isn't being followed.	Monitor and ensure any related actions are completed.
Audit Outcomes	Show if internal audits have found weaknesses.	Track that audit actions are completed.

The **Risk Team** regularly checks in with Risk Owners to review progress and identify issues.

Risk Reporting

We report risks **every quarter** to the **Executive Risk Committee (ERC)** and the **Audit & Risk Committee (ARC)** — but only **Principal Risks** (those rated red).

- Risk Owners must write a **Principal Risk Report** using a standard template.
- The **Risk Team** supports this and gives an independent view on how well the risk is being managed.
- ERC can also request a detailed "deep dive" if needed.

Assurance Mapping

Assurance mapping helps us check that all key risks are being properly managed without any gaps or overlap. At NS&I, we use two key tools for this:

- **Risk Universe**: A list of the biggest risks we face which we regularly monitor.
- **Control Universe**: A list of the key actions (control objectives) we use to manage those risks. These are tracked using our risk tool, and the results of audits are linked to these controls.

Together, they help us see where assurance is strong or where we need to improve, guiding our yearly planning.

Supplier Risk Management Obligations

NS&I's main suppliers must follow risk management rules as part of their contracts. Here's what they need to do:

- **Risk Framework**: Have their own risk system (aligned to ours), reviewed each year, with a skilled risk lead managing it.
- **Risk and Control Self-Assessment (RCSA)**: Regular checks to ensure key controls are working well, and that they meet NS&I's expectations.
- **Risk Data**: Share regular risk and control data with NS&I so we can oversee performance.
- **Reporting**: Provide reports for NS&I's quarterly risk meetings when requested.
- **Evidence** the effectiveness of the control environment around NS&I data and services.
- **Submit** to audit by NS&I and/or by GIAA when required.

Other Risk Procedures

Waivers & Dispensations Procedure

- **Waiver**: A permanent exception when we can't meet a control (but not for legal or regulatory rules).
- **Dispensation**: A short-term exception (usually under 12 months) while fixes are being put in place.

Both must be approved and must show who's responsible if something goes wrong.

Risk Event Root Cause Analysis (RCA)

- When a serious risk turns into a real issue (like a major failure, loss, or legal breach), we need to investigate why it happened.
- This process looks at what failed, why, and what needs fixing to stop it happening again.
- RCAs are usually done by our suppliers, with NS&I oversight, and results are linked back to our risk tracking tools.

Appendix 1: Risk Policy template

XXX Risk Policy					
Policy Owner	xxxx	Date of last review:	xxxx	Date of next review:	xxxx
Policy Statement	Provide a short description of the policy including: Scope; including to whom it applies. Legal, regulatory or relevant standards within which the policy is designed to operate. Links to associated rules and protocols that staff can access. Where breaches of policy should be reported to.				

Key Risk	Risk Title: xxxxx Risk Description: xxxxx Vulnerabilities: • Xx • Xx • Xx Triggers: • Xx • Xx • Xx Consequences: • Xx • Xx • xx			
Definition of losses	Describe what losses are in relation to your risks – these can be financial and non-financial events.			
Risk Appetite				
Key Risk Indicator(s)	KRI Name	Red	Amber	Green

Control objectives	Control Objective description	How will this be monitored?		

Appendix 2: Risk Matrix: Operational & Transformation Risk

[Redacted. Please see accompanying document]