Credit Information Governance Body

Risk Policy

Version	Date	Owner	Author	Approved by	Document Location	Comments
1.0	September 2025	Legal Counsel			Sharepoint	
2.0	November 2025	Chair of ARC				

Risk Policy

1. Purpose

This Risk Policy outlines the framework and principles through which the Credit Information Governance Body UK (hereafter referred to as "the Body") identifies, assesses, manages, monitors, and reports risks related to the governance of credit information. It aims to ensure the integrity, accuracy, security, and appropriate use of credit data within the UK financial ecosystem.

2. Scope

This policy applies to all functions, systems, employees, third-party providers, and stakeholders involved in the handling, oversight, or regulation of credit information under the remit of the Body.

3. Regulatory Context

This policy aligns with:

- **UK GDPR** and **Data Use and Access Act 2025**
- **Financial Conduct Authority (FCA)** standards
- **Information Commissioner's Office (ICO)** guidance
- **Principles for Financial Market Infrastructures (PFMI)**

4. Risk Governance Structure

The Body adopts a **three lines of defence** model:

1. **First Line:** Operational teams responsible for data governance, compliance, and IT controls.
2. **Second Line:** Risk and compliance function independently monitoring and advising on risk management.
3. **Third Line:** Internal audit providing independent assurance on effectiveness of the risk management framework.

The Audit and **Risk Committee** reports to the Board and oversees all CIGB risks. The Chair of the Audit and Risk Committee is responsible for the maintenance and implementation of this policy.

Any incidents or breaches of this policy must be reported in writing, by email, to the Chair of the Audit and Risk Committee or CIGB General Manager and logged in the Incident and Breach register.

5. Risk Appetite

The Body maintains a **low tolerance** for risks that may compromise:

- Data privacy and protection
- Integrity and accuracy of credit data
- Stakeholder and subscriber rights and protections
- Reputational harm to CIGB
- Legal and regulatory compliance

Risk appetite statements are reviewed annually by the Board within this policy.

6. Key Risk Categories

6.1 Data Privacy and Security Risk

- Risk of unauthorised access, data breaches, or misuse of personal data.
- Managed through encryption, access controls, regular penetration testing, and data minimisation principles.

6.2 Operational Risk

- Failures in systems, processes, or human error leading to data errors or delays in reporting.
- Mitigated by strong internal controls, business continuity planning, and staff training.

6.3 Regulatory and Compliance Risk

- Risk of non-compliance with UK GDPR, FCA, or ICO requirements.
- Addressed through ongoing monitoring, policy updates, and regulatory engagement.

6.4 Third-Party Risk

- Risk from vendors or partners who handle credit data on behalf of the Body.
- Managed through due diligence, SLAs, and regular audits of third parties.

6.5 Reputational Risk

- Risk of public trust erosion due to failure in data stewardship or ethical breaches.
- Controlled via transparent governance, clear communication, and prompt incident management.

6.6 Technology and Cyber Risk

- Threats from cyberattacks, system obsolescence, or software vulnerabilities.
- Mitigated with secure IT architecture, threat monitoring, and cyber insurance.

6.7 Strategic and Emerging Risk

- Monitored through horizon scanning and participation in industry consultations.

7. Risk Assessment and Monitoring

- All risks are identified, assessed, and scored using a **Risk Matrix** (likelihood vs. impact).
- Regular risk assessments are conducted at entity, departmental, and project levels.
- A **Risk Register** is maintained and updated quarterly
- An Action Log is maintained in tandem with the Risk Register to monitor mitigating actions.

8. Incident Management

- All incidents must be reported within 24 hours.
- CIGB has an Incident and Breach register aligned with ICO requirements.
- Post-incident reviews are mandatory, with root cause analysis and remedial actions.

9. Reporting and Escalation

- Monthly risk reports to the Board as part of BAU MI.
- Immediate escalation of high/critical risks to the Board.

11. Policy Review

This Risk Policy is reviewed **annually** or following a major incident, regulatory update, or organisational change. Amendments must be approved by the Audit and Risk Committee and ratified by the Board.