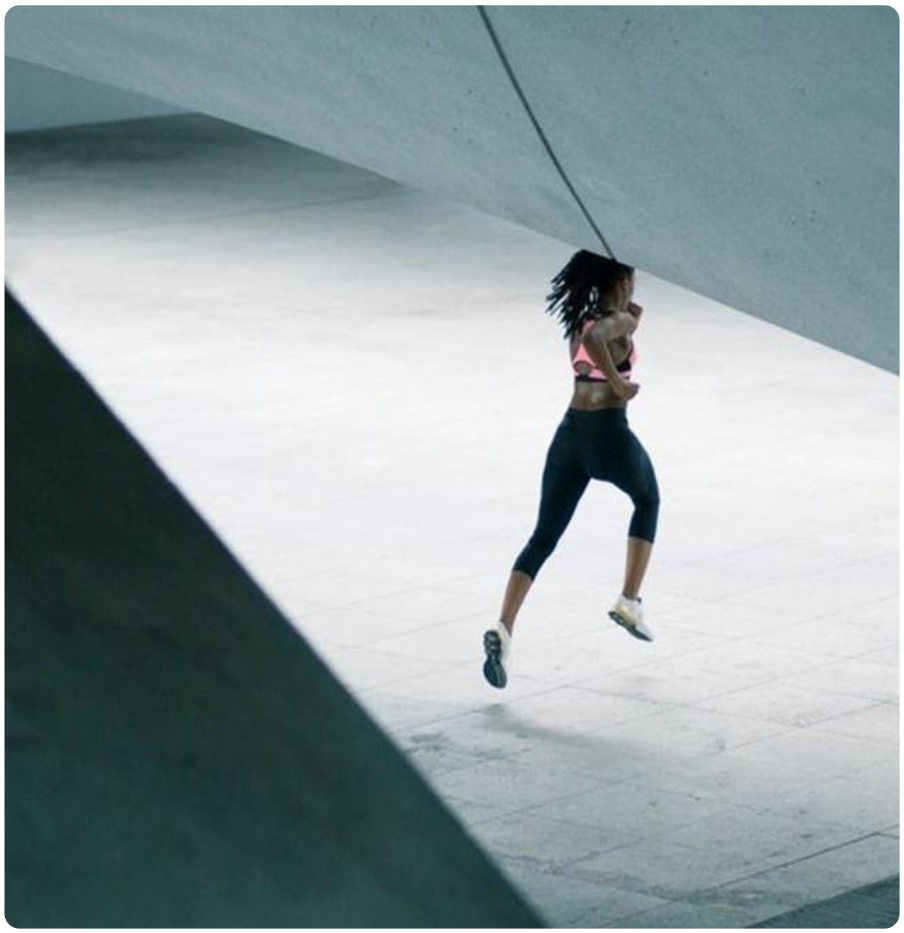

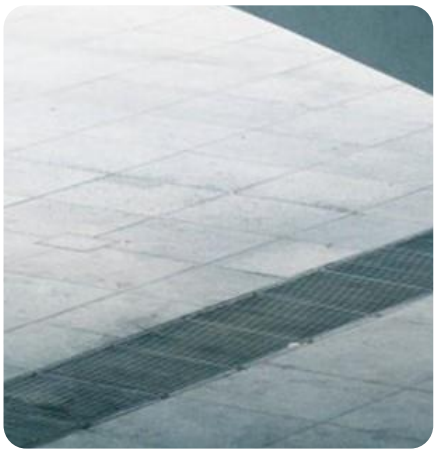

Executive summary report covering a review of the data management, protection, and oversight measures within the operations of the Central Credit Register service

26 September 2024

1 Executive Summary for the CCR service independent review

1.1 Background

The Central Bank of Ireland (CBI) issued a public statement on 21st August 2023 after identifying the cause of an **archiving error that affected the retention period** of certain borrower information held on the Central Credit Register (CCR). The issue was first brought to the Central Bank of Ireland's attention by a member of the public. As a result of this error, some **borrower information was retained on the register for an additional three months and included in credit reports**. This error caused data to be retained for longer than permitted under the Credit Reporting Act 2013 and constituted a data breach under data protection legislation.

The CBI stated that **no borrower data was compromised or accessed by any unauthorised third parties because of the error.**

Following the incident, the **CBI initiated a targeted independent, point in time, review of the end-to-end CCR service, focusing on the adequacy and the effectiveness of data management and data protection control measures** and **oversight mechanisms** for the CCR service**. The review was conducted from May to July 2024.**

This report summarises the key findings, and the recommendations from the independent review that was outlined in a **detailed technical report finalised in September 2024.**

1.2 What is the Central Credit Register service?

The **Central Bank of Ireland** is responsible for the operation of the **Irish Central Credit Register (CCR)** under the Credit Reporting Act 2013. The CCR is a database that **stores personal and credit information** for loans of **€500** or more. Following a public procurement process, the Central Bank of Ireland contracted with a third party to operate the Central Credit Register on its behalf.

The CCR provides credit reports to **borrowers and lenders, and supports the Central Bank's obligations and functions**, including consumer protection, supervising the financial sector, and ensuring financial stability. The Central Bank owns the information held on the Central Credit Register and is a **data controller under the Data Protection Acts**.

1.3 What is the scope of the independent review?

The **independent review** covered an assessment of the data protection safeguards and data management measures in place as well as a review of controls and oversight measures in place for risk management and monitoring.

Overall, this included a review of the **monitoring of compliance with documented requirements** focusing on **data management and data protection** as well as risk assessment frameworks and controls. Additionally, it included reviewing adequacy of the control measures and the roles and responsibilities in place. **Oversight mechanisms** were also reviewed focusing on data protection and **data management for the end-to-end CCR service**.

The review was **limited to an examination of the documentation provided and interviews** with relevant stakeholders involved in the CCR service.

1.4 What was the approach for the independent review leading to findings and recommendations?

The independent review involved a **four-stage process** to guide the identification of findings and recommendations.

Firstly, a data privacy and third-party risk management assessment was applied which is based on **regulatory requirements and good practice**, which enables **focus areas of the CCR service to be benchmarked.** It was also used to validate findings, benchmark documentation quality expectations, and guide the scope of the interview questions.

Secondly, a desk-based review of policies and procedures was completed. This included technical manuals, organisational policies and database management related procedures covering requirements of **data protection, risk management and business operations management.** The aim was to identify where the appropriate **documentation was in place** and to assess the **quality** of the documentation.

Thirdly, **stakeholder interviews** with individuals and teams involved in the day-to-day delivery and operational management of the end-to-end CCR service were conducted to obtain further information and to validate observations. Interview questions were focused on **data protection, third-party risk management and the steps taken for maintaining resilience** of the overall CCR service operations.

Finally, the data privacy and third-party risk management assessment was used to map outputs from the documentation review and the interviews to identify key findings and recommendations.

1.5 What good practices were identified as part of the independent review?

Throughout the review, several instances of good practice were identified. For example, when evaluating the **monitoring and compliance with contractual requirements for data management and data protection**, the findings highlighted a robust process for managing service performance. Additionally, there is a **proactive approach to risk monitoring**, with effective mechanisms in place to regularly test the performance of the database systems.

When looking at security systems, it was found that access to databases is tightly managed based on **role requirements and appropriate restrictions are applied**. Examples of good practice included the use of regular security scanning to fix bugs.

When reviewing the **control measures** in place to support data protection**,** it was found that there is proactive development of **information security policies, regular security testing, and a thorough data protection governance framework** to ensure that data is managed securely.

Service management processes are well-established, ensuring that the CCR service operates smoothly, with **changes tracked and tested to maintain its functionality**. Data protection is a key priority, with a comprehensive governance framework to **handle data requests** and manage data breaches in line with best practices relating to the CCR service.

In assessing the oversight measures for data management and data protection, the review identified a **proactive approach to risk management.** This included a specialist risk stakeholders forum focusing on **data protection, information security, business continuity** and wider operational risks. Additionally, compliance with contractual obligations and service level performance targets for the CCR service are discussed in **supplier relationship management meetings** which is a positive step towards supporting overall **accountability** for the **CCR service** operations.

1.6 What findings and recommendations were identified for the management and monitoring of the CCR service?

The findings of the review identified three overarching recommendations to enhance the effectiveness of management and oversight of data protection and third-party risks within the end-to-end CCR service.

Evolution of the operating model and organisational alignment for the CCR service

Firstly, the operating model supporting the end-to-end CCR service across CBI and involved parties is not fully aligned. It is recommended to evolve the **operating model for the CCR service** by completing a comprehensive review of its capabilities covering **processes, people, systems, data, controls**, and **governance** to ensure alignment at each stage of the end-to-end CCR service. Given that the current **operating model was implemented in 2017**, a review offers the opportunity for enhancing the overall effectiveness of the service.

Increasing the ability of stakeholders to support changes in service provision **will enhance the management and monitoring** of third-party risks by ensuring necessary adjustments can be effectively implemented. Enhancing current processes will further aid in **effective management, monitoring, and reporting within the CCR service**, including solutions for **overseeing data protection, information security, and third-party risk management.**

Strengthen risk management capabilities for the CCR service

Secondly, it was identified that there are opportunities to improve the ongoing oversight of third-party risks and control effectiveness across the delivery of the end-to-end CCR service.

There are benefits in **strengthening the risk management capability by** enhancing **first-line oversight** within CBI.[1] This involves bolstering risk management capabilities in relation to the third-party service provider to support ongoing oversight of the CCR service. Maintaining this on an ongoing basis, entails building on existing progress being made by embedding CBI's **Third-Party Risk Management (TPRM) policy and framework within the CCR service,** by ensuring that the **necessary resources and processes** are in place to support effective oversight and management of third-party risks and controls.

Embedding a culture of ongoing risk management relating to the third-party service for the CCR service

Lastly, third party risk management is not fully embedded in an integrated way across CBI and involved parties.

Embedding a culture of **ongoing third-party risk management**[2] means, identifying appropriate controls and addressing potential risks associated with outsourcing services to third parties. Improving ownership and accountability can be achieved by fostering an environment that **emphasises the continuous identification, management, monitoring, and reporting of third-party risks**.

This can be partly facilitated through targeted, **role-specific third-party risk management training** across CBI and all parties involved in the delivery of the CCR service. Enhancing the engagement of Data Protection Officers by increasing their involvement in direct data protection status reporting for the CCR service is also recommended.

[1] "First-line" refers to the business units and management that are responsible for managing and owning risks.
[2] The process of identifying, managing and monitoring controls in place to manage potential risks and assessing the effectiveness of the controls in place for managing the risks when working with external suppliers.

Conclusion

In combination with the good practices, the review identified focus areas for **enhancing organisational alignment, strengthening risk management capabilities, and cultivating a proactive approach to third-party risk management** across all parties involved in the CCR service. This will enhance the management and monitoring, ensuring the CCR service operates effectively.

By evolving the operating model and strengthening the **comprehensive management and monitoring of third-party risks and identification of appropriate controls**, the CCR service can **minimise the impact and likelihood of disruptions and incidents**. Enhancing oversight and management of **parties involved in the CCR service,** reinforces the CBI's commitment to excellence and integrity in its operations. Proactively **identifying, managing, monitoring, and reporting** third-party risks at **every stage** of the CCR service will improve accountability and foster stronger collaboration among all parties.