Risk Management

Information Security in Credit Unions.

It's time for Credit Unions to Embrace the Advantages of Implementing ISO 27001:2022

BACKGROUND

In the last decade, the risk and risk management agendas have moved centre stage in the credit union sector. Legislation and regulation require credit unions to address risk and particularly cyber risk in a comprehensive manner. Within the EU, The European Agency for Cybersecurity (ENISA) is the agency dedicated to achieving a common level of cybersecurity across the EU. In Ireland, the National Cyber Security Centre (NCSC) is responsible for advising and informing Government IT and Critical National Infrastructure providers of current threats and vulnerability associated with network information security.

Risk management frameworks standards utilised across the sector include, IT Infrastructure Library (ITIL), Control Objectives for IT (COBIT), National Institute of Standards & Technology (NIST), ISO/IEC 27001: 2022, etc. From an enterprise risk perspective, credit unions deal with a variety of risk specialisms, including Business Continuity Management, Incident & Crisis Management, Health & Safety Management, Security Risk Assessment, Financial Risk Management, Reputational Risk Management and Contract Risk Management. More recently, the credit union sector was challenged by the COVID 19 pandemic and was required to assess the associated risks and implement appropriate controls to safeguard members and staff. Furthermore, implementing ISO:27001:22 will address many of the requirements of the Central Bank 'Cross Industry Guidance on Operational Resilience e.g. BCM, Incident Management, Communications Plans, etc, and the EC's Digital Operational Resilience Act (DORA)

The Central Bank of Ireland in its publication 'Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks' noted: *'Based on our supervisory experience to date, firms are not implementing sufficiently robust systems and controls and must increase their efforts in developing resilience to IT failures, including cybersecurity incidents, so that they can minimise the potential impact on their business, reputations and wider financial system.'*

Furthermore, the Central Bank's publication on Cross Industry Guidance on Operational Resilience published in December 2021 requires credit unions to address key areas of their business, which are identified under three Pillars and cover such areas as Governance, Business Continuity Management, Incident Management,etc..

The Central Bank of Ireland of Ireland also states that it expects credit unions to develop, implement, maintain and communicate an appropriate ITRM (Information Technology Risk Management Framework).

This paper makes the case for the adoption, by credit unions, of an internationally recognised standard, ISO/IEC 27001: 2022. The standard, addresses, inter alia, expectations of the Central Bank of Ireland in a systematic and comprehensive manner and specifies the requirements for establishing, implementing and maintaining an **Information Security Management System.**

OVERVIEW OF THE STRUCTURE OF ISO: 27001:2022

ISO/ 27001: 2022, Information Technology-Security Techniques-Information Security Management Systems-Requirements, consists of two components. The main component of the standard consists of 11 clauses. Clauses 0-3 provide you with an introduction to the standard, defines the scope of the standard, normative references and terms & definitions.

Clauses 4-10 set out the requirements for information security and address the following areas: ***Leadership, Planning, Support, Operation, Performance Evaluation and Improvement.***

Annex A, the second component of the standard, Reference Control Objectives and Controls, provides a catalogue of 93 controls grouped into four sections. These sections cover the following areas: ***Organisational Controls (37), People Controls (8), Physical Controls (14) and Technological Controls (34).***

INFORMATION SECURTY MANAGEMENT SYSTEM

Information security is a core objective of all credit unions and needs to be **comprehensively addressed**. Information Security Management System ISMS is a systematic approach for managing and protecting the credit union's information. Implementing an ISMS ensures that the risks associated with information security are identified and controlled, thus ensuring its confidentiality, integrity and availability. The System consists of organisational controls; including policies and procedures that set the information security rules in the credit union as well as technical and other controls.

BENEFITS OF ISO: 27001:2022 IMPLEMENTATION

There are a number of key benefits to implementing ISO: 27001:2022.

COMPLIANCE

ISO/IEC 27001: 2022 provides your credit union with the framework that helps the credit union to comply with regulations regarding data protection, privacy and IT governance. It also addresses the various contractual obligations, e.g., clauses in SLA's.

Implementing ISO/IEC 27001: 2022 will ensure that your credit union is adhering to best practice and thereby complying with Central Bank of Ireland requirements.

The Central Bank of Ireland in its document 'Cross Industry Guidance in respect of Information Technology and Cybersecurity Risk' (2016) referenced ISO/IEC 27001: as a relevant best practice and internationally recognised framework. Other standards mentioned include ITIL, COBIT and NIST. They also note that these industry standards, inter alia, will inform the Central Bank of Ireland's supervisory and inspections approach to IT and IT Risk (Information Security / Cybersecurity) Management.

In the more recent Central Bank of Ireland roadshows, the issue of risk management was again highlighted and its approach to engagement with credit unions on this matter.

MARKETING EDGE

ISO/IEC 27001: 2022 will provide the credit union with the ability to differentiate from other credit unions and financial services organisations. Handling members sensitive information in a secure manner is paramount to maintaining credibility and ensuring high standards are maintained throughout the organisation.

LOWERING EXPENSES CAUSED BY INCIDENTS:

At the end of the day, implementing ISO/IEC 27001: 2022 helps the credit union to better organise its business by defining responsibilities and procedures. ISO: 27001: 2022 provides the credit union with a framework within which responsibility and accountability are clearly identified. It will force the credit union to define very precisely, both responsibilities and the processes and thereby strengthen your internal organisation.

BETTER ORGANISED BUSINESS:

At the end of the day, implementing ISO: 27001: 2022 helps the credit union to better organise its business by defining responsibilities and procedures. ISO: 27001: 2022 provides the credit union with a framework within which responsibility and accountability are clearly identified. It will force the credit to define very precisely, both responsibilities and the processes and thereby strengthen your internal organisation.

CULTURE

The adoption and implementation of ISO: 27001: 2022 creates a continual improvement culture built on theinitial improvements derived from process integration. Employees are engaged as their roles are identified and integrated into the ISMS.

IMPLEMENTING ISO: 27001:2022 AS A PROJECT

Implementing ISO:27001: 2022 in your credit union is a project. A good practice for effective implementation is to form a project team and to assign concrete roles to team members. The basic roles are usually: Project Manager, Project Team, Information Security Officer /Risk Manager, Compliance and Management.

The timeframe for implementing ISO:27001: 2022 will depend on several factors including, resources and their availability, skillset and the size of the credit union. As a general rule, six to nine months should be sufficient to complete the project.

THE PROCESS OF CERTIFICATION

Once the credit union has implemented ISO/IEC 27001: 2022, it has the option to go for certification. This involves engaging with one of the Certification Bodies who will visit the credit union and audit all aspects of ISO/IEC 27001: 2022. After completion of a successful audit, the credit union is required to maintain the standard on an annual basis. This involves annual interim audits and an in-depth audit every three years.

Further information: Purchase a copy of SO/IEC 27001: 2022 which is available from NSAI (National Standards Authority of Ireland), Central Bank of Ireland-Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks, NIST-National Institute of Standards & Technology, ENISA-European Union Agency for Cybersecurity, NCSC-National Cyber Security (Centre Ireland), GDPR-General Data Protection Regulations / Data Protection Commissioner.

This article was written by: Michael McHugh, Managing Director, CU-ISO SOLUTIONS Ltd.
Qualifications: Michael McHugh, B.Ed. Hons, LCOI, Dip. in Op. Risk (UCD) QFA, CUA, CUG, Certified ISO:27001: implementer and external auditor.

Industry Experience

- Decades of experience in the credit union sector.
- Founder member of Comhar Linn INTO Credit Union Ltd.-served as CEO for over thirty years. (Retired 2019)
- CEO of Rathmore & District Credit Union Ltd. Until 2021. (Interim appointment.)
- Founder member of PAYAC.
- **Further Information:**
- CU-ISO SOLUTIONS LTD. was set up to assist credit unions and financial service businesses who wishto implement ISO/IEC 27001: 2022 and associated standards.
- Website details: Website: www.cuisosolutions.ie
- Email: michael.mchugh@cuisosolutions.ie Mobile: +353(0)872434847