Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

IT Risk in Credit Unions
- Thematic Review Findings

January 2018

Table of Contents

1. Executive Summary

1.1 Purpose

This report (the "Report") sets out the key observations and expectations of the Central Bank of Ireland (the "Central Bank") in relation to information technology ("IT") governance and risk management arising from a thematic review of certain IT Risks. The findings set out in this report should be considered by credit unions in the context of assessing the adequacy of their own risk management framework and determining appropriate actions to mitigate risks identified.

The IT risk profile of most credit unions is increasing due to growing complexity of IT risk factors, including those driven by the types and number of systems used, expanding branch networks and increased connectivity to external IT networks. The Central Bank expects that the Boards and management of credit unions fully recognise their responsibilities in relation to IT governance and risk management and accordingly prioritise within their risk management framework.

The Central Bank carried out a thematic inspection of a number of credit unions with regard to their management of IT Outsourcing, Business Continuity Management and IT Security. The Central Bank also met with five IT suppliers and one credit union user group to gain a more comprehensive understanding of the nature of the IT risks within the sector. This report sets out key observations and examples of good practice and poor practice observed during the course of the thematic review.

This report sets out the Central Bank's expectations regarding good practices that credit unions should consider adopting when reviewing the effectiveness of their existing IT governance and risk management frameworks. It is important to note that this report does not address all aspects of the management of IT risk but rather focuses on those key areas that were within the scope of the thematic inspection.

Credit unions should examine the practices outlined within this report and review their alignment with them. Where there are gaps, credit unions should address these on a proportionate basis that is reflective of the scale and complexity of their business dependency on IT.

The Central Bank published a policy paper on *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks* in September 2016, which was circulated to all credit unions, setting out guidance in relation to IT governance and IT risk management. This report reinforces the expectations articulated in that paper on the areas covered in this IT Thematic review.

1.2 Background

The IT landscape of the credit unions inspected involve a range of specialist IT service providers and technologies to support their business processes. It was noted during the inspections that the quality of IT governance and ownership varied across the credit unions and is not necessarily proportionate to membership size, branch structure or asset levels. In the course of our review, it was clear that the primary focus by most credit unions on IT is on the shares and loans systems, which records all customers' shares and loans as opposed to the full end-to-end IT infrastructure and services used. Over recent years, there have been a large number of transfer of engagements which resulted in many credit unions now having a branch network requiring real time connectivity to a central shares and loans system, file shares and email. The need to have high speed, always available communications links between credit unions and their branches has increased the IT risk profiles of credit unions and broadened the number of critical IT components and suppliers for the credit unions. These critical components include IT support, IT telecommunications, phone systems, Wide Area Network (WAN) solutions and third party software.

As credit unions engagement with IT increases both in the expansion of their own internal networks and their offering of greater online services to members, there is an increasing requirement for credit unions to proactively monitor and manage their changing IT risk profile.

1.3 Methodology

In order to understand the current status of IT management within credit unions the Central Bank undertook a thematic inspection across 12 credit unions. The IT Thematic inspections took place between June 2017 and October 2017. The sample chosen were selected based on a cross section of the larger IT Suppliers to credit unions, different asset sizes (impact categories of 'Low' or 'Medium Low'), urban and rural credit unions, and aligned with the 2017 calendar of PRISM inspections. The total asset sizes of the sample of credit unions ranged between €13 million and €265 million with membership ranging from just over 4,000 up to almost 73,000. Of the total sample of credit unions, 75% had one or more branches. Significant IT suppliers of the main shares and loans software and the IT support services for hardware, along with one credit union user group, were also engaged with to ensure that a more rounded and comprehensive understanding of IT risks and the controls in the specific areas that are in place.

The inspection work included an assessment of the policies and procedures relating to IT Outsourcing, IT security and Business Continuity Management (BCM), interviews with key credit union personnel, review of a sample of service level agreements (SLAs), and review of risk registers and the BCM testing framework.

The inspection objectives details are contained in Appendix 1.

1.4 Summary of Key Findings

Improvements in credit union IT Governance, IT Security and general IT awareness over the last three years was evidenced during this IT Thematic Review and also acknowledged by the IT Suppliers. Given the pace of change however, these areas require continued focus and ongoing improvement. Areas such as business continuity and

penetration testing are the most notable areas where improvements have occurred. Notwithstanding this, the Inspection Team identified a number of weaknesses across the three categories that were reviewed. As stated previously, the quality of IT governance is not directly related to a credit union's total asset level, membership size or branch structure.

The following is a summary of the findings from the credit union IT thematic inspection.

IT governance and outsourcing

- The majority of credit union managers interviewed demonstrated basic IT knowledge and basic understanding of IT Risk Management. The management of a credit union are responsible for understanding the specific IT risks based on the scale and complexity of the business and to ensure such risks are sufficiently mitigated. This knowledge and understanding must be appropriate to the scale and complexity of the activities undertaken.
- Understanding of IT Governance and its approach is varied and ranges from good knowledge and practice, to being very dependent on external support from IT service suppliers and third party consultants to provide both IT services and assurance.
- Some IT policies were not localised to the individual credit union requirements and therefore were not understood by the credit union's Board and management.
- Exit, termination and transition stages of services from an outsource partner to another third party or back in-house were not included in any outsourcing policies provided.
- Some credit unions viewed IT more as an expense item and did not appear to view IT as a core enabler of their business which requires robust risk management.

Business Continuity Management

- Business continuity for shares and loans systems and penetration testing are the most notable areas of improvement.
- Business Continuity Management ("BCM") policies and the underlying Business Impact Analysis (BIAs) and Business Continuity Plans ("BCP") in place for shares and loans systems were generally comprehensive but when queried as to the concepts and the rationale for the documented controls in place, many credit unions could not articulate them and some did not know what Disaster Recovery ("DR") solutions they had in place.

IT security

- Ongoing and up to date patch management and firewall reviews were not in place in some instances. Some contracts in place between credit unions and their IT service supplier only provide for the restoration of

services or the repair and or replacements of assets. These weaknesses in contracts, coupled with a lack of understanding of the importance of such security incident prevention tools, leaves credit unions vulnerable.

- While there is a heightened level of awareness within credit unions of the vulnerabilities of IT in light of the ongoing publication of reports and media coverage of cyber security incidents, there is a low level of understanding as to how cyber-attacks can occur and moreover what controls are required in order to mitigate cyber risk.
- A small number of credit unions understood the purpose and results of the penetration tests and what the results of these meant and what the true risk was to the credit union.
- In most cases credit unions did not compile and validate an independent inventory of all their IT assets that supports their businesses. Where inventories of assets were provided by credit unions they were, for the most part, compiled by their main IT service provider solely in respect of the assets they supplied (as IT provider) and did not take account of IT assets provided by other providers. There was no process in place to capture hardware provided by other suppliers nor a manual reconciliation between what is actually in place and that provided by all of the IT suppliers.
- Data classification and full awareness as to the storage of credit union-owned data (including jurisdiction where it is stored) and the risks associated with its storage was not demonstrated. There was no evidence of risk assessments being carried out where credit unions engaged cloud storage solutions. This lack of risk assessment leads to poor understanding as to where data is stored. There was lack of clarity as to whether the contract for this service is between the credit union and the cloud provider directly or between their main IT service provider and the cloud provider. While the Inspection Team subsequently noted that in those specific instances, the main IT service providers had carried out due diligence of the cloud service providers data storage solution, it is of concern that credit unions were unaware of this fact.
- The Inspection Team found no evidence of any consideration of the implications of ongoing monitoring or the retrieval of the data stored in the 'cloud' should credit unions wish to terminate the contract.

These findings are further addressed later in this paper with accompanying examples of good and poor practice observed during the inspections. The Central Bank's expectations in respect of each risk area is also set out in each of the sections.

1.5 Supervisory Expectations

Credit unions should consider the findings and expectations outlined in this report when reviewing their existing IT governance and risk management arrangements and should use this guidance to inform future development of their IT risk management frameworks. Credit unions are required to understand and demonstrate sound IT governance and risk management in accordance with their business model and technological complexity.

Proportionality

Given that the sector includes a range of credit unions of differing size and complexity, the issue of proportionality is pertinent to credit union considerations. There is no one-size fits all solution to IT risks – each credit union must

understand and address the risks that pertain to its business. Accordingly, it is the responsibility of individual credit unions to assess and document the degree to which they meet the expectations within this report and identify necessary actions to satisfy these minimum standards. In seeking to meet the expectations it is recognised that they will have different implications for large more complex credit unions than for smaller credit unions with less complex business models.

The security of credit union data and systems is of primary consideration and steps taken by the credit union must be proportionate to the risks involved. Larger credit unions and those who see themselves on a growth trajectory will be expected to demonstrate strong compliance with all the expectations listed herein as part of an integrated Risk Management Framework.

Assessment of risk should include compliance with the required legislation and regulations (including requirements outside core credit union legislation), best practice and guidance and ensure the credit union is taking appropriate steps to manage and mitigate IT risk. Appropriate consideration and assessment must be given to any proposed changes to ensure any IT exposures are fully understood and are within the credit union's Board-approved risk appetite.

A strong risk management culture should be evidenced through the risk register where all IT risks are captured including appropriate actions to reduce those risks outside the credit union's Board-approved risk appetite to acceptable levels and within reasonable timelines.

The Central Bank's supervisory oversight of IT governance and risk management will continue to intensify in future engagements with credit unions (particularly those undertaking more complex business activities). The degree to which these expectations are met will inform supervisors' views as to the quality of IT governance and risk management in the areas covered by this report.

2. IT Governance

Credit union Boards and management are responsible for setting and overseeing their business strategy and risk appetite and should ensure that IT risk is considered in this context. In addition, management is responsible for the effective implementation of the credit union's business and IT strategies. For the vast majority of credit unions, IT is a core enabler of the business with most, if not all, of the critical business functions supported by IT. As such, it is important that the IT strategy is comprehensive and aligned with the overall business strategy so that it can deliver on objectives to support the current and future strategic direction of the credit union. The IT risk management framework should be comprehensive and is fundamental to facilitating an effective assessment of the IT risks to business operations as well as improved decision-making when dealing with risks that could affect critical business operations. Robust oversight and engagement on IT matters at the Board and management level has a critical role in promoting an IT and security risk conscious culture within the credit union.

The Inspection Team found that the overall understanding of IT governance and approach is varied and ranged from good knowledge and practice, to being very dependent on external support from IT service suppliers and third party consultants to provide both IT services and assurance. As mentioned earlier, this was not proportionate to the size of the credit union's membership size, asset levels or branch network.

Credit unions are required to put in place effective structures to manage IT-related risks that are appropriate for the business model, size and technological complexity of the credit union and the sensitivity and value of information and data assets.

The following table provides instances of good practice and poor practice observed during the course of the on-site inspections in relation to IT Governance:

Observed Examples of Good Practice	Observed Examples of Poor Practice
- Effective business continuity policy in place. - Robust due diligence requirements for the on boarding of an outsourcing partner included in Outsourcing Policy. - IT risk register is comprehensive in terms of IT risks and appropriate mitigants identified. - Credit unions moving to employ IT staff with IT risk knowledge. - IT viewed as a key enabler of business strategy throughout the credit union.	- IT risks on risk register refer to policies as mitigants and not specific monitoring and reporting actions to ensure elements such as anti-virus and patch management take place in a timely manner. - Poor alignment between the IT and business strategies. - The IT strategy is not sufficiently comprehensive or detailed, omitting key elements such as future software and hardware requirements and planning for new functionality requirements. - The use of generic IT policy documents that are insufficiently tailored to the credit union's circumstances. - No evidence of termination and transition phase of outsourcing in outsourcing policies or service level agreements. - There was a lack of knowledge and understanding of the content by management of IT policies when challenged by the Inspection Team. - Data classification frameworks and policies are not established.

	- IT Security policy did not include user access reviews and frequency. - BCP-Policy was more aligned to a Business Continuity Plan than a high level policy. - The outsourcing policy did not consider the exit, termination and transition stages of services from an outsource partner. - The outsourcing policy contained legislative references only and was not tailored to credit union's outsourcing requirements. Similarly, it did not identify who the outsourcing decision makers are. - The outsourcing policy was insufficiently comprehensive. It did not include all outsourcing contracts such as IT communications provider, email provider etc.

IT Governance Expectations

I. Credit unions have a sufficiently robust IT governance structure in place to facilitate effective oversight of the management of IT risks, reflective of the scale and complexity of the business dependency on IT;

II. Documented policies, standards and procedures which address the identification, monitoring, mitigation and reporting of the credit union's IT related risks are in place;

III. IT policies, standards and procedures are regularly reviewed and updated to reflect changes in the internal IT operating environment and the external security environment;

IV. The governance structure provides for independent assurance on the effectiveness of the IT risk management, internal controls and governance processes within the credit union.

V. The inventory of IT assets should include targeted replacement or upgrade schedules which will assist with IT Strategies and forward planning.

3. IT Security

All organisations including credit unions are increasingly exposed to IT security risks such as cyber-attack, malware and computer viruses. IT security risks are ever changing and therefore require proactive updating and monitoring of IT networks and infrastructure including all data storage solutions. The technical complexities of the risks arising from operating in an online channel to customers, or having connectivity to external parties, pose significant challenges as credit unions are required to manage the associated risks and vulnerabilities.

Credit unions are expected to have adequate processes in place to effectively address IT security risk. While it is recognised that there is no 'one size fits all' solution to addressing this risk, all credit unions should understand the implications of IT security risk based on the IT Systems and IT Infrastructure they use. The IT risk management framework, including associated policies and procedures, should be reviewed regularly and updated where appropriate, to ensure they reflect enhanced controls based on IT development changes or the latest safeguards against increasingly sophisticated cyber attacks.

Credit unions should work to reduce the frequency of security incidents by actively maintaining, monitoring and assessing the security of their applications, systems and networks. Adverse impacts arising from security incidents must be mitigated through adequate incident handling capabilities and ensuring that incident recovery plans are in place. Training and continuous reinforcement of users' security responsibilities and the promotion of a strong security culture throughout the credit union is a core mitigant of IT security risks.

The following table provides instances of good practice and poor practice observed during the credit union on-site inspections in relation to IT Security:

Observed Examples of Good Practice	Observed Examples of Poor Practice
- User access reviews occurred at least annually for share and loans system and network access. - Engagement of independent third parties to carry out penetration tests to identify weaknesses. - Demonstrated appropriate understanding of the purpose and results of penetration tests and risks to the credit union. Where issues were identified they were appropriately remedied. - IT security awareness training provided to staff. - IT risks register in place with relevant and appropriate risk mitigants. - Regular vulnerability testing and patch management in place to manage IT security risks for PC and servers.	- No evidence of inventory of IT assets in place. - The inventory of IT assets provided was incomplete. Appropriate understanding as to the purpose of the inventory of IT assets was not demonstrated. - The inventory of IT assets was not risk rated and the criticality of the business processes supported by the assets was not identified. - There was no evidence of user access reviews of either IT network or the share and loan systems. - No evidence of data classification and associated storage of data including assessment of the risks associated with storage solutions based on classification. - No clear action plans to remediate legacy systems in use with known IT security vulnerabilities. - No patch management in place and no contract in place in relation to patch management for PC and servers. - No action plans to remediate identified server patch issues. - Ongoing monitoring and updating of infrastructure and network not in place. - A low level of understanding as to how cyber-attacks can occur and what controls they require in order to mitigate cyber risk.

IT Security Expectations

I. A thorough inventory of IT assets, including all physical components of the IT network, both hardware and software should be maintained and classified by business criticality. For example, communications hardware which are not owned by a credit union but are critical to supporting connectivity to branches should be included.

II. There should be a manual reconciliation of the physical IT Assets held by the credit union against the documented inventory of IT assets.

III. An up-to-date list of identified IT risks (often referred to as the "IT risk register") is developed and maintained, wherein the risks are prioritised and described in sufficient detail so as to be clearly understood by the credit union enabling their proactive management.

IV. Credit unions must implement strong controls over access to IT systems, whether from inside or outside the credit union, by their own staff or their third party suppliers and outsourcing service providers ("OSPs"). Users should only be granted the level of access required to perform their responsibilities ("Principle of Least Privilege") and only persons with proper authorisation are permitted to access sensitive or critical data and systems. User access to systems and their access rights should be reviewed and documented on an annual basis.

V. Staff with privileged access rights, in particular, should be aware of good IT security behaviour and all staff should have an appreciation of the importance of security to critical business activities and objectives.

VI. Credit unions should develop and implement security awareness training programmes to provide information on good IT security practices, common threat types and aligned with the credit union's policies and procedures regarding the appropriate use of applications, systems and networks.

VII. Processes are developed, implemented and maintained to ensure that data is appropriately classified and that critical or sensitive data is correctly identified and adequately safeguarded. This classification should directly link to the classification of the criticality of the IT asset that it is stored or transmitted across.

VIII. The effectiveness of IT controls are subject to periodic independent review and, where warranted, penetration testing. Such reviews are conducted by individuals with appropriate IT audit expertise and details of the key findings and associated implications are provided to the Board. Weaknesses identified in the control environment should be remediated in a timely manner.

IX. Where legacy systems support critical business operations, credit unions should have a strategy in place to evolve the legacy systems and transition to next generation capabilities over time. Solutions to legacy systems should provide for adequate investment to be made to implement the solution.

X. Adequate processes are in place to monitor information systems and assets and to detect security events and incidents in a timely manner, preferably using predictive indicators. The effectiveness of detection processes and procedures are tested periodically. This can be achieved by conducting penetration testing exercises.

XI. The prevention and detection of security events and incidents is contingent upon clarity of responsibilities between the credit union and the IT Supplier on key areas such as patch management, penetration testing and proactive monitoring. The contracts and/or SLAs with IT Suppliers should specify the degree to which such services are provided.

4. Business Continuity Management

The high reliance on IT for critical business operations and services exposes credit unions to the risk of severe business interruption should a technology disruptive event or emergency occur. A severe business interruption has the potential to damage the credit union's reputation and cause it to incur financial loss as well as adversely affecting members. Credit unions' disaster recovery and business continuity planning should encompass the recovery, resumption and maintenance of all aspects of the business. Periodic and comprehensive testing of these plans is essential to build preparedness in effectively handling a disruptive event.

The Inspection Team noted that credit unions inspected are more aware and engaged with regard to business continuity management and planning than any of the other areas reviewed during the inspection. All of the credit unions inspected have policies in place and have at a minimum a disaster recovery solution for their share and loan system. They also have local daily backups occurring of their share and loan systems at a minimum with many having their core data backed up off site to another branch, or data centre managed by their IT service provider. The focus for most credit unions inspected is on business continuity and DR for the share and loan systems. However, many credit unions could not confirm if their backup solutions covered all of the remaining critical systems and data and accordingly were unable to confirm if the backup solutions were appropriate for their business continuity requirements. While IT providers were in a position to confirm the scope of the backups in place, it is the responsibility of the Board and management to understand their full business continuity requirements and ensure that it is in place. Credit unions should have a documented backup strategy for critical data in place and conduct regular backup restore tests to verify the restore capabilities for critical systems.

The following tables provides instances of good practice and poor practice observed during the credit union on-site inspections in relation to Business Continuity Management:

Observed Examples of Good Practice	Observed Examples of Poor Practice
- Disaster recovery solution in place for shares and loans system. - SLA contracts with IT suppliers support DR plans. - Local daily backups and regular off-site data backup (to another branch or data centre managed by their IT service provider). - Demonstrated good understanding of what is required in a BIA and a BCP. - Evidenced BCP tests in the last 12 months including follow up lessons learned with action plans to remediate any issues noted. - Call trees and registers of staff members contact details were maintained. - Evidenced contingency plans containing for instance the availability of alternative locations (such as a branch office) or in the case of credit unions with no branches, that they have agreements in place with other financial	- Credit unions could not confirm if their backup solutions covered all of their critical systems, including data, and whether they were appropriate for their business continuity requirements. - BCP plans had not considered the impact of the loss of a service provider for an IT critical service. - Credit union management were unable to articulate their DR and backup solution or demonstrate a reasonable understanding of the content of the BCM policy, or how the plan would be operationalised or tested. - BCP plan did not address email data backup.

institutions to allow them to work from their business premises.	

Business Continuity Management Expectations

I. Credit unions should have sufficient resources to support effective DR and BC planning, testing and execution, and credit union management should fully understand their DR plans.

II. Documented BIA with complete end-to-end reviews of business critical processes showing the impacted resources, business processes and their interdependencies are in place.

III. Credit unions should consider a range of plausible events and disaster scenarios, these should cover the loss of people, place of work, Outsource Service Providers and IT systems events in their DR and BC planning.

IV. A documented DR plan is in place that enables the credit union to recover and resume services in the event of a disaster or emergency situation. The plan includes details of recovery time objectives and recovery point objectives for all IT assets based on business criticality.

V. Credit unions should have a documented backup strategy for critical data in place and conduct regular backup restore tests to verify the restore capabilities for critical systems.

VI. Credit unions should ensure DR and BC plans are tested annually.

VII. DR and BC plans are regularly reviewed (at least annually) and updated to reflect changes in the credit union's operating environment and to incorporate lessons learned from testing.

VIII. The Board receives updates on the scenarios considered and the development and testing of DR and BC plans and understand what the objectives of these are, in terms of maintaining availability of critical IT systems and business operations.

5. IT Outsourcing

Credit unions are reliant on OSPs for a range of IT services including back-office functions, cloud services, system development and maintenance, infrastructure, website hosting, security and disaster recovery. Credit unions are reminded that responsibility for the effective management of those risks rests with credit union Boards. Outsourcing in the area of IT can expose credit unions to additional and/or increased levels of risk relating to security, operational performance and business continuity, if not properly managed. Credit unions are required to have adequate governance and risk management processes in place to effectively address the risks associated with outsourcing of IT services, including cloud services.

The following tables provides instances of good practice and poor practice observed during the credit union on-site inspections in relation to IT Outsourcing:

Observed Examples of Good Practice	Observed Examples of Non-Compliance / Poor Practice

- Robust due diligence and risk assessments were carried out on new IT Suppliers of shares and loans system.
- Ongoing and proactive monitoring and updating of infrastructure and network in place (e.g. IT Managed Services).
- Evidence of annual independent financial assessment of outsourced provider.
- SLA contracts contained Key Performance Metrics.
	- No evidence of formal reviews of IT provider performance.
	- SLA not signed by credit union.
	- SLA did not have a complete list of services and applications including the criticality of each application.
	- No evidence of independent IT reviews carried out by third parties or qualified internal resources to verify appropriateness of IT solutions.
	- Contracting data storage to the cloud without due diligence or knowledge as to who the contracted parties are and how the contract can be terminated to ensure data retrieval is appropriate. In addition, the location of the data stored (in terms of jurisdiction) was not in evidence.
	- Lack of understanding by credit union management in relation to:
	  - Contractual obligations with IT suppliers.
	  - Location of cloud data.
	  - Exit arrangements and data implications.

Outsourcing Expectations

I. Thorough due diligence is conducted on prospective IT Service Providers. Due diligence includes consideration of, inter-alia, the IT Service Providers' technical capabilities, performance track record and financial strength and viability. The due diligence also considers whether the IT Service Provider can meet its requirements in relation to service quality and reliability, security and business continuity in normal and stressed circumstances.

II. The signed contract between the credit union and its selected IT Service Provider includes a documented SLA or equivalent. The SLA clearly sets out the nature, quality and scope of the service to be delivered as well as the roles and responsibilities of the contracting parties.

III. The SLA includes requirements for service levels, availability and reliability, including measurable performance metrics and remedies for performance shortfalls. Using the key provisions of the SLA, credit unions should regularly monitor the service delivery performance to determine if the IT Service Provider is delivering to the required standards. Where performance shortfalls are identified, these are addressed with the IT Service Provider in a timely manner. Credit unions should implement a formal process to review the performance of suppliers of key services on a regular basis to ensure that services are performed as stipulated in contracts and SLAs and meet the needs of the credit union.

IV. The SLA includes provisions relating to system and information/data security, business continuity and disaster recovery, service scalability, assurance and service termination based on the criticality of the service provided. In particular, where new storage services are utilised, such as cloud, contracts with cloud providers specify the location(s) where the institution's data is stored, processed and managed (including the jurisdiction), and the security measures required when transmitting and storing data.

V. Credit unions should satisfy themselves that the selected IT Service Provider has sufficient and robust controls in place in relation to its cybersecurity.

VI. Credit unions should develop and maintain an exit management strategy to reduce the risks of business disruption should key IT outsourced services be unexpectedly withdrawn by the IT Service Provider, or voluntarily terminated by the credit union. Viable options for resuming the impacted service(s) should be identified which are proportionate to the scale and complexity of the credit union's activities for example, in the case of smaller credit unions where transaction volumes are modest, a plan to revert to manual systems (with appropriate controls implemented) for a short period may be appropriate, depending on the circumstances. In particular, where new storage services are utilised, such as cloud, contingency plans are in place that allow for the cloud service to be transitioned to a backup facility, an alternative service provider or managed within the institution itself if necessary.

VII. The outsourcing policy includes a provision that any outsourcing arrangements entered into by the credit union should not impede effective on-site or off-site supervision of the credit union by the Central Bank. This should also be reflected in any specific contracts entered into by the credit union.

6. Conclusion

Improvements in IT Governance, IT Security and General IT awareness over the last three years were evidenced during this IT Thematic Review and also acknowledged by the IT Suppliers. Given the pace of change however, these areas require continued focus and ongoing improvement. Areas such as business continuity and penetration testing are the most notable areas of improvement. While acknowledging these improvements, nonetheless, greater engagement by credit unions in managing their IT risks and integrating IT risk management into their overall risk management frameworks is required. Credit unions must understand and appreciate the importance of the data that they process and store and from this assess their IT assets with regard to risk and business criticality. Such an approach should be clearly aligned to their overall risk governance structures and assist in the identification of a comprehensive IT strategy which is aligned with the overall business strategy. Credit unions can use the sound principles of effective IT asset management to build out the risk controls of these assets and the future cost thereby assisting in their IT strategy and assisting in aligning it to their business strategy. Credit unions should work either individually or collectively to ensure they understand the scale and scope of IT services they are receiving and assess the true cost of the uplift required in their IT governance as they increase their IT risks through diversity into digital customer channels. The mind set of IT being viewed as a cost is outdated and the recognition that IT is the repository and carrier of their critical assets, data, and the enabler of business growth must be accepted by Boards and management and embraced with appropriate risk management frameworks.

Appendix 1: Inspection objectives details

IT Security: to obtain reasonable assurance that IT Security in the credit unions follows a defined and approved policy. Areas of review included assessing whether:

- The policy is appropriate and fit for purpose;
- Perimeter security is in place, e.g., fire-walls, DMZ, web application firewalls, IDS/IPS, logging and monitoring;
- Regular penetration testing is taking place, e.g. by independent competent specialist;
- All employees, including IT staff, receive IT security awareness training; and
- Vulnerabilities are identified, analysed, classified and patched accordingly and within an acceptable timeframe.

Outsourcing: to obtain reasonable assurance that the outsourcing agreement covers at a minimum:

- The nature and scope of the business activity that is to be outsourced;
- Clearly defined roles and responsibilities for the credit union and the service provider;
- Service level and performance requirements are documented; and
- Reporting and monitoring arrangements are in place to enable the credit union to effectively monitor the performance of the service provider.

Business Continuity Management: should include the business continuity arrangements in relation to outsourced activities where a defect or failure in its performance would materially impair:

- The continuing compliance with the conditions and obligations of the credit union's registration or its other obligations under the financial services legislation;
- The credit union's financial performance;
- The soundness or continuity of the credit union's financial performance;
- The soundness or continuity of the credit union's business; and
- Business continuity procedures in place in the event that changes to information systems cause interruption to the business of the credit union, including roll-back plans, where appropriate.

Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem