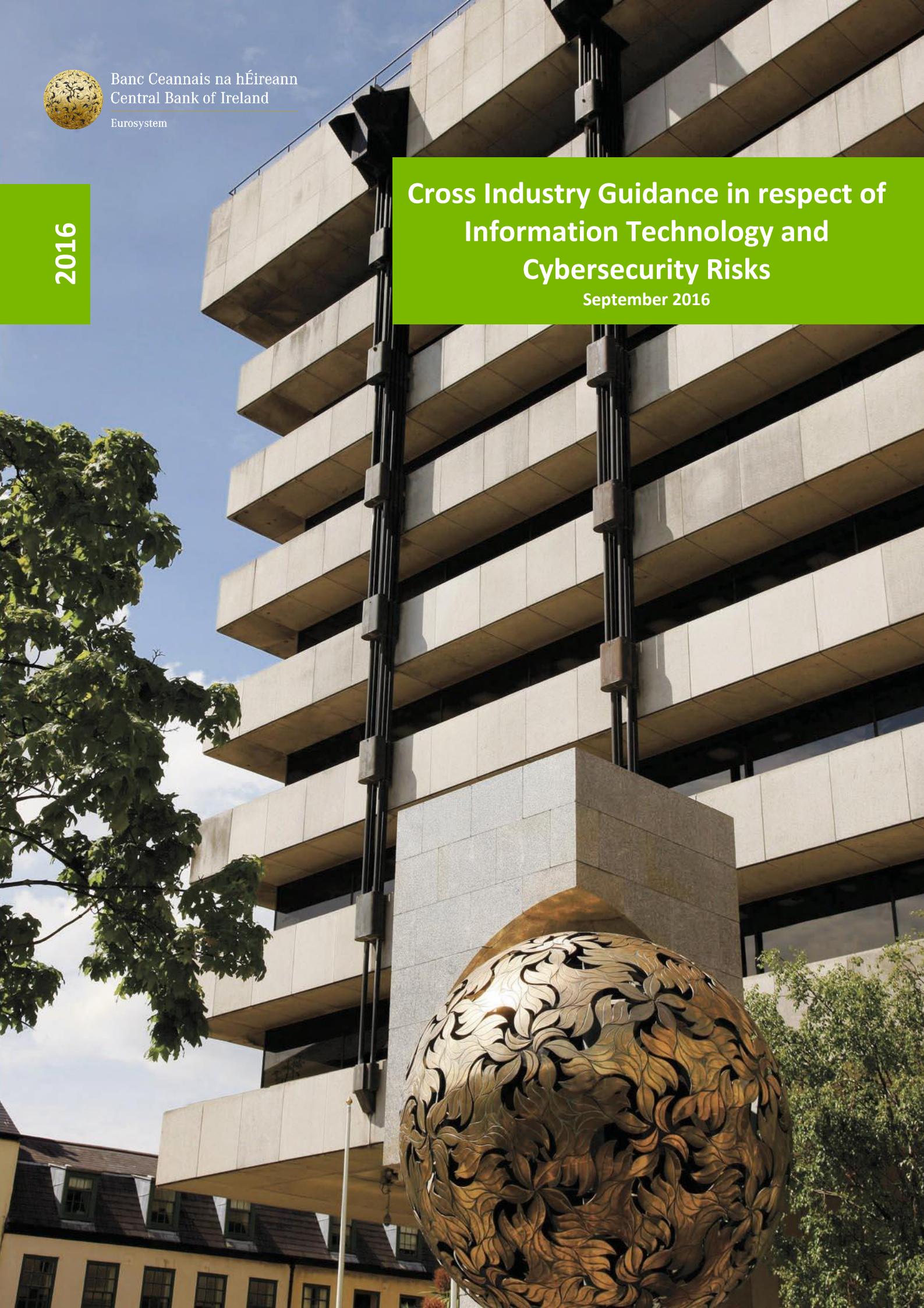

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

2016

Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks

September 2016

CONTENTS

EXECUTIVE SUMMARY

Purpose

This paper sets out the Central Bank of Ireland's ("Central Bank") guidance in relation to information technology ("IT") and cybersecurity governance and risk management by regulated firms in Ireland.

The risks associated with IT and cybersecurity ("IT related risks") are a key concern for the Central Bank given their potential to have serious implications for prudential soundness, consumer protection, financial stability and the reputation of the Irish financial system. Accordingly, the Central Bank expects that the Boards and Senior Management of regulated firms fully recognise their responsibilities in relation to IT and cybersecurity governance and risk management and place these among their top priorities.

This paper also sets out observations that incorporate examples from supervisory work carried out by the Central Bank over the course of 2015 and 2016 to assess IT and cybersecurity related operational, governance and strategic risks in regulated firms. The guidance outlined in this paper sets out the Central Bank's current thinking as to good practices that regulated firms should use to inform the development of effective IT and cybersecurity governance and risk management frameworks. This guidance will inform supervisors' views as to the quality of IT related governance and risk management in regulated firms. Failings in respect of this guidance will inform Central Bank supervisory decisions, including those in respect of risk mitigation programmes.

It is important to note that this paper does not address all aspects of the management of IT and cybersecurity risk but rather focuses on those areas that we deem most pertinent at this time based on our supervisory work to date. No guidance from the Central Bank can cover all risks and necessary actions for all regulated firms. It is management's responsibility to understand the specific IT related risks that the firm faces and to ensure that these are sufficiently mitigated in line with the firm's risk appetite. The Central Bank acknowledges that the relevance and importance of the issues raised in the paper will vary

according to the business model, size and technological complexity of the institution and the sensitivity and value of its information and data assets.

This paper is not a replacement for and does not supersede the legislation, regulations, guidelines and standards that firms must comply with as part of their regulatory obligations, particularly in the areas of risk management, internal controls and corporate governance. Firms must at all times refer directly to the relevant legislation, regulations, standards and guidance to ascertain its statutory obligations and to ensure that it is taking appropriate steps to mitigate and manage IT and cybersecurity risk.[1]

Background

The rapid advancement of technology innovations in recent times has fundamentally changed business processes and models in financial firms of all sizes. These advancements have undoubtedly introduced efficiencies and cost savings for firms and their customers. However, these technologies also bring significant risks, as firms become increasingly interconnected and more reliant on complex IT systems and outsourcing service providers to conduct their business and deliver services to customers. In addition, while the adoption of technological innovations has reduced costs and increased efficiencies, it has concurrently provided greater risks for data to be lost, stolen, corrupted or accessed by unauthorised users.

Firms are also increasingly exposed to the risk of cyber-attacks. These have become more sophisticated, more frequent, more targeted and progressively more difficult to detect, with the financial sector one of the most frequently targeted.[2] Cybersecurity has become a risk for all financial firms. The failure of a firm's IT systems can have significant adverse financial, legal, customer and reputational consequences that should not be underestimated. Based on our supervisory experience to date, firms are not implementing sufficiently robust systems and controls and must increase their efforts in developing

[1] Some key international guidance in this regard can be found in the Appendix.

[2] The Gemalto Breach Level Index 2015 report finds that the financial sector suffered 16% of all reported breaches in 2015, second only to the healthcare sector. The IBM 2016 Cyber Security Intelligence Index found that the financial sector was the third most attacked industry sector in 2015.

resilience to IT failures, including cybersecurity incidents, so that they can minimise the potential impact on their business, reputations and the wider financial system.

Firms in particular must take measures to minimise the risk of consumer detriment due to IT and cybersecurity incidents. When the firm becomes aware of an IT incident that could have a material impact on consumers or on the firm's ability to provide services, minimising customer detriment, the resumption of critical business operations and timely customer communications should be key components of any incident management plan.

Firms should assume that they will be subject to a successful cyber-attack or business interruption. For this reason, the incident management approach needs to deal with cybersecurity threats and resilience to reduce both the probability of occurrence and the impact when it does. With that in mind, IT related risk management must be comprehensive and robust, addressing key risk areas such as business strategy alignment, outsourcing, change management, cybersecurity, disaster recovery and business continuity.

Supervisory Issues Identified To Date

In recent periods, the Central Bank has strengthened its supervisory capabilities with regard to IT related risks and sharpened its focus on these risk areas. Sector specific work is underway across the Central Bank's supervisory divisions on different aspects of IT and cybersecurity governance and risk management.

Central Bank IT risk specialist supervisors have carried out a number of inspections. These inspections, along with thematic reviews and our ongoing supervisory engagement, have highlighted a number of areas where IT and cybersecurity governance and risk management has fallen short of the expected standards. While not all of the inadequate practices referred to in this paper arose in any one firm, they are representative of those identified across all firms reviewed. The nature and number of inadequate practices identified indicate a lack of prioritisation, awareness and understanding of IT and cyber

security related risks and that more work is required at Board and Senior Management level to ensure that firms are effectively managing these risks.

The following is a summary of these findings, which are set out in more detail later in the paper:

- Alignment between firms' IT strategy and the overall business strategy is weak. IT capabilities are not matched to the business ambitions.
- Firms are not taking a holistic view of IT risks across the business, which results in poor identification, monitoring and mitigation of IT risks.
- Shortcomings in IT risk assessment and identification with many firms not maintaining comprehensive IT risk registers and risk identification being backward rather than forward looking.
- Older technology supporting key business operations and requiring significant resources and/or investment to manage associated risks.
- Non-existent or inadequate data classification frameworks and policies.
- Staff not sufficiently trained on cybersecurity risks.
- Ineffective firewall management/inadequate intrusion detection processes with weak IT security monitoring.
- Deficiencies in governance of IT related outsourcing including a lack of thorough due diligence on prospective service providers, poorly documented/constructed outsourcing agreements and inadequate monitoring of service delivery.
- Inadequate and untested disaster recovery and business continuity plans.

Next Steps

The Central Bank's supervisory oversight of IT and cybersecurity related risks will continue to intensify in future engagements with firms. This supervisory engagement will be

informed by the issues raised and guidance outlined in this paper and supervisors will discuss with firms their progress in understanding and addressing these issues. Firms should consider the issues outlined in this paper when reviewing their existing IT related governance and risk management arrangements and use this guidance to inform future development of their IT risk management frameworks.

This paper sets out the Central Bank's current thinking and guidance in relation to IT and cybersecurity governance and risk management. Our thinking will continue to evolve as our knowledge of these areas deepens through supervisory engagement and policy formulation. The Central Bank will continue to engage in open dialogue with firms and industry stakeholders in order to inform future policy development in this area.

1. GOVERNANCE

1.1 Board of Directors and Senior Management Oversight of IT and Cybersecurity Risks

The Board of Directors (the "Board") and Senior Management are responsible for setting and overseeing the firm's business strategy and risk appetite and should ensure that IT risk[3] is considered in this context. In addition, Senior Management is responsible for the effective implementation of the firm's business and IT strategies. For the vast majority of financial firms, 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 firm. The firm's 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 Senior Management level has a leading role in promoting an IT and security risk conscious culture within the firm. Setting the right 'tone from the top' is a crucial element in fostering a robust IT risk management culture.

In assessing the quality of Board and Senior Management oversight of IT risks, the Central Bank has identified a number of inadequate practices, including:

- Insufficient alignment between the IT and business strategies. In some cases, this resulted in inadequate capabilities of the IT infrastructure to support the strategic business objectives of the firm.
- 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.

[3] For the remaining sections of this paper, the term "IT risk" will refer to IT risks including cybersecurity risks, unless expressly noted otherwise.

- The quality and/or frequency of IT related reporting to the Board is highly variable and in many cases, deficient. In general, the Board and Senior Management are not being sufficiently informed about the operational risk profile of the firm, including IT and cybersecurity risks.

With regard to the quality of Board and Senior Management oversight of IT risks, the Central Bank expects that:

1. Firms develop and document a Board approved comprehensive IT strategy that is aligned with the overall business strategy. IT strategy objectives should include maintaining the capacity to effectively anticipate, detect and recover from cybersecurity attacks on the firm so as to ensure overall IT resilience.

2. Sufficient resources are allocated to execute the business-aligned IT strategy, including an adequate IT budget, staff levels and relevant expertise. There is a plan in place to identify and address any resourcing and capability gaps that would obstruct the achievement of the wider strategic objectives, including those relating to the execution of change management on a present and forward-looking basis.

3. Firms have in place a well-defined, comprehensive and functioning IT risk management framework that enhances the level of oversight and also provides clarity and gives assurance to the Board regarding the management of IT risk within the firm.

4. The Board receives updates on key IT issues including major IT projects, IT priorities and significant IT incidents as well as regular reports on key IT risks. Where these reports deal with IT risks which fall outside the firm's risk appetite, they should include plans to mitigate those risks.

5. The Board as a whole and Senior Management possess sufficient knowledge and understanding of the IT related risks facing the firm and take steps to ensure that these risks are well understood and properly managed throughout the firm and can demonstrate this to supervisors.

1.2 IT Specific Governance

Firms 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 firm and the sensitivity and value of its information and data assets.

In assessing the IT governance structures in place, the Central Bank has identified a number of inadequate practices, including:

- Failure to perform reviews and updates to IT related policies on a sufficiently regular basis.
- Failure to perform a substantive review of the IT policies, with the approach, in some instances, being akin to a 'tick-box' exercise.
- The use of generic IT policy documents that are insufficiently tailored to the firm's circumstances.
- The role of the Operational Risk function as the second line of defence is not clearly defined.
- Older systems supporting key business applications in some firms make the production of key management information used by decision makers more time consuming and potentially subject to error. Many of these older systems require significant maintenance, while the skills needed to maintain them are becoming increasingly scarce.

With regard to the IT governance arrangements in place, the Central Bank expects that:

1. Firms have a sufficiently robust IT governance structure in place to facilitate effective oversight of the management of IT risks, taking into consideration the nature, scale and complexity of the business operations of the firm.

2. Documented policies, standards and procedures which address the identification, monitoring, mitigation and reporting of the firm's IT related risks are in place. These should be regularly reviewed and updated to reflect changes in the internal IT operating environment and the external security environment.

3. The roles and responsibilities in managing IT risks, including in emergency or crisis decision-making, are clearly defined, documented and communicated to relevant staff. A clearly defined role(s) is established, at a sufficiently senior position within the firm, which is responsible for IT and cybersecurity matters.

4. Firms which are part of a larger multinational group ensure that group driven IT strategies and governance documents are appropriately tailored from a regulatory and operational perspective for the Irish firm.

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

2. RISK MANAGEMENT

2.1 IT Risk Management Framework

The IT risk management framework should be an integral component of the overall operational risk management framework, which in turn forms part of the enterprise wide framework. The framework should be comprehensive and facilitate effective assessment of the IT related risks specific to the firm. IT risk management should be continuous and proactive, requiring oversight, not only of the technology, but also of the people and the processes that use and support the technology. Firms can mitigate the impact of IT incidents by having well developed and tested incident handling plans and processes in place.

The Central Bank has identified a number of inadequate practices in place around the management of IT related risk, including:

- The IT risk assessment and risk identification process is insufficiently robust. It is often event or incident driven and lacks forward-looking assessments of new or emerging risks.
- IT risk registers are not established, or where they do exist, they are not sufficiently comprehensive and are not current.
- Inadequate monitoring of IT risk registers (where these are in place) with risk mitigation frequently slow or non-existent due to resource or funding constraints.
- In larger groups where multiple risk assessment tools are used, they are frequently not aligned. This impedes the firm from having a holistic view over IT risks across the firm.
- Weak IT asset management processes and poor quality, or non-existent, inventory of IT assets in operation. As a result, firms are not fully aware of all the hardware, software and data assets on their networks and, as such, cannot assess the associated risks in a holistic manner.
- Data classification frameworks and policies are not established or, where they do exist, are not adequately designed or implemented. The data dictionaries that did exist often

focussed only on a particular application with no holistic view of all systems or even of all key systems.

- The maturity of IT incident management differs greatly between firms. Even those with good incident management processes are more reactive than proactive in their management of the risks.

With regard to IT risk management, the Central Bank expects that:

1. Firms develop, implement, maintain and communicate an appropriate IT Risk Management ("ITRM") framework. The ITRM framework should:
   - facilitate a comprehensive view of the IT risks including a clear line of sight of the links and dependencies between people, business processes and the IT systems and assets that support those people and processes;
   - encompass risk identification, assessment and monitoring, the design and implementation of risk mitigation and recovery strategies and the testing of their effectiveness; and
   - set out staff and senior management responsibilities and accountabilities.

2. Relevant best practices and internationally adopted frameworks for IT risk management are considered, and incorporated as appropriate, in the development of the ITRM framework.[4]

3. IT risk assessments are conducted at regular intervals. Assessments are comprehensive, consider internal and external sources of risk, and have appropriate parameters for evaluating and prioritising risk such as risk likelihood and potential impact on the business operations of the firm.

[4] There are many such standards in use but some of the more widely adopted standards for overall IT governance include the IT Infrastructure Library (ITIL) and Control Objectives for IT (CoBIT). The ISO/IEC27001 and ISO/IEC27002 and the National Institute of Standards and Technology (NIST) 800 series focus specifically on information security. These are the industry standards, inter-alia, that will inform and shape the Central Bank's supervisory and inspections approach to IT and IT Risk (Information Security/Cybersecurity) management.

4. The firm can demonstrate that it has assessed the risks associated with the continued maintenance of older ("legacy") systems and that appropriate controls are implemented to effectively manage the risks associated with older IT infrastructure. Where legacy systems support critical business operations, firms have a strategy in place to deal with ageing infrastructure including assessing where additional investment is required or whether to transition to next generation capabilities over time.

5. A thorough inventory of IT assets, classified by business criticality, is established and maintained. A process (Business Impact Analysis) is in place to regularly assess the business criticality of IT assets, even in cases where it may transpire that there are no IT business critical assets.

6. 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 firm, enabling their proactive management.

7. Adequate management processes and plans for IT incident detection, notification and escalation are developed by firms. Appropriate recovery and resumption objectives are developed to prepare for when incidents occur and reducing impact when they do, with prioritisation given to the recovery and resumption of critical functions.

8. The firm notifies the Central Bank when it becomes aware of an IT incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

9. 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.

10. The effectiveness of IT controls is subject to periodic independent review and, where warranted given the nature and scale of the firm, penetration testing is carried out. 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 must be remediated in a timely manner.

2.2 IT Disaster Recovery and Business Continuity Planning

The high reliance on IT for critical business operations and services exposes firms to the risk of severe business interruption should a disruptive event or emergency occur. A severe business interruption has the potential to damage the firm's reputation and cause it to incur financial loss as well as adversely affecting its counterparties and customers. Firms' 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.

In reviewing IT disaster recovery and business continuity planning arrangements, the Central Bank found a number of inadequate practices in place, such as:

- Failure to conduct or regularly refresh the Business Impact Analysis.
- Inadequate and/or infrequent testing of disaster recovery ("DR") and business continuity ("BC") plans and failure to inform the Board of the outcomes of this testing.
- Inadequate prioritisation of critical business operations in BC plans. Some plans were overly focussed on recovering the full IT system with little or no prioritisation of critical business operations.
- Failure to perform regular backup and restore tests to verify the restore capabilities for critical systems.

With regard to IT disaster recovery and business continuity planning, the Central Bank expects that:

1. Sufficient resources are provided to support effective DR and BC planning, testing and execution.

2. Documented Business Impact Analysis with complete end-to-end reviews of business critical processes showing the impacted resources, business processes and their interdependencies is conducted.

3. Firms consider a range of plausible event and disaster scenarios, including cybersecurity events in DR and BC planning.

4. A documented DR plan is in place that enables the firm to recover from and resume services in the event of a disaster or emergency situation. The plan includes details of targeted recovery timeframes.

5. A documented BC plan is in place that enables the firm to maintain IT and business operations and services in the event of a disruption. For critical systems and dependent services, firms should have a level of availability commensurate with the criticality of these services and ensure that 24/7 support capabilities are in place.

6. Firms have a documented back-up strategy for critical data and conduct regular back-up and restore tests to verify the restore capabilities for critical systems.

7. DR and BC plans are tested periodically, as appropriate for the firm. The level of testing, ranging from walkthrough to 24/7 operations, is commensurate with the firm's dependency on IT or other critical infrastructure. Plans are also regularly reviewed (at least annually) and updated to reflect changes in the firm's operating environment and to incorporate lessons learned from testing.

8. The Board receives updates on the scenarios considered and the development and

testing of DR and BC plans and understands what the objectives of these are in terms of maintaining availability of critical IT systems and business operations.

2.3 IT Change Management

Firms should have adequate processes in place to manage change involving hardware, communications equipment and software, system software and all documentation and procedures associated with the development, running, support and maintenance of live systems. Deficiencies in or lack of formal change management processes can lead to poor decisions being made to approve or deny proposed changes with impacts to business areas not being adequately considered. Depending on the nature of the change, this can potentially lead to disruptions to business operations and/or customer services.

When reviewing the approach taken by firms in relation to managing the risks associated with IT change, the Central Bank identified a number of inadequate practices, such as:

- Lack of formal change management processes and procedures.
- Failure to perform risk and impact assessments of proposed changes.
- Insufficient testing of new technologies, systems and products prior to deployment.
- Inadequate planning for and insufficient testing of upgrades and patches to existing systems prior to deployment.

With regard to IT change management undertaken by firms, the Central Bank expects that:

1. Firms have formal IT change management processes, including approval requirements, in place.

2. Adequate processes are in place to effectively address operational risks associated with the upgrade or the development/acquisition and implementation of new systems and software. These processes should include sufficient testing and consideration of security requirements in all stages of system or product design, development and testing.

3. IT project plans are documented. For major proposed changes to the IT infrastructure, a thorough prior risk and impact analysis is performed and documented and establishes whether it is within the firm's risk appetite. The Board receives periodic updates on the progress including the risk status of major IT projects.

3. CYBERSECURITY

Organisations are increasingly exposed to the risk of a cyber-attack due to the growing frequency and targeting of attacks, which are simultaneously becoming more sophisticated and difficult to detect. In addition, current and long-term technological trends (such as cloud computing, 'big data', mobile devices, financial technology and 'the internet of things') will further increase exposure to cyber risk. The technical complexities of the risks arising from operating in the digital society, with organisations required to manage a multiplicity of interrelated risks and vulnerabilities, pose significant challenges.

Firms are expected to have adequate processes in place to effectively address cyber risk. While it is recognised that there is no 'one size fits all' solution to addressing this risk, all firms should understand the strategic implications of cyber risk. The cyber risk management elements of the IT risk management framework, including associated policies and procedures, should not be viewed as static. Firms should review and update the framework regularly to reflect threat intelligence and changes in the internal and external operational environment.

Firms can reduce the frequency of security incidents by actively maintaining the security of data, applications, systems and networks. Adverse impacts arising from security incidents can be lessened by maintaining adequate incident handling capabilities and ensuring that incident recovery plans are in place. Further, poor security awareness in a firm is a significant contributor to increased cyber risk. Awareness can be increased through training and continuous reinforcement of users' security responsibilities and by the promotion of a strong security culture throughout the firm.

In assessing firms' cybersecurity arrangements, the Central Bank identified a number of inadequate practices, such as:

- Inadequate IT security awareness training of staff.
- Failure to develop a formal plan to address the specifics of cyber risk.
- Cyber risk assessments not being performed on a sufficiently regular basis.

- Ineffective firewall management/inadequate intrusion detection processes and weak security monitoring.
- Customer data not encrypted at rest or in transit.
- Insecure protocols used for data transmission.
- Older systems, with known IT security vulnerabilities supporting key business applications in some firms.

With regard to cybersecurity, the Central Bank expects that:

1. Cyber risk is managed within the context of overall IT risk management.

2. Firms have a well-considered and documented strategy, reviewed and approved by the Board, in place to address cyber risk. Documented cybersecurity policies and procedures are maintained, monitored and enforced which support effective implementation of the security risk management strategy. Cybersecurity roles and responsibilities are clearly defined, documented and communicated to relevant staff.

3. Firms develop and implement security awareness training programmes to provide information on good IT security practices, common threat types and the firm's policies and procedures regarding the appropriate use of applications, systems and networks. 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.

4. At a minimum, cyber risk management addresses:
    - the identification of threats, vulnerabilities and risks and quantification of exposure specific to the firm;
    - the prevention and detection of security events and incidents, including reducing likelihood of occurrence and potential impact when it does;
    - security incident handling; and
    - recovery planning for stabilisation and continuity of operations in the immediate aftermath of a security incident.

5. Cyber risk assessments are performed on a regular basis and include identification of external and internal threats. To support intelligence gathering on current and emerging threats and vulnerabilities, firms should consider participating in security information sharing forums.[5]

6. Robust safeguards are in place to protect against cybersecurity events and incidents. Techniques and technologies that firms may consider include, but are not limited to, strong authentication, encryption, intrusion prevention and detection, advanced malware protection, strong access controls (including physical controls) and network segmentation providing isolation and defence in depth when required.

7. There are processes in place to classify data enabling the firm to identify sensitive, valuable and critical data that the firm stores, processes or transmits. Appropriate safeguards (commensurate with the value or importance of the data) are implemented to ensure that it remains secure, complete, accurate and readily available to authorised users who need it. The processes should provide for the secure logging of all data access.

8. Firms implement strong controls over access to their IT systems, whether from inside or outside the firm. Users are granted only the level of access required to perform their responsibilities ("Principle of Least Privilege") and only staff with proper authorisation are permitted to access sensitive or critical data and systems.

9. 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

[5] Cybersecurity information sharing networks, whether formal or informal, can provide valuable intelligence on threats, attacks and vulnerabilities and allow participants to benefit from the collective experiences, knowledge and analytical capabilities of the group.

undertaken by either the firm's staff or trusted third parties.

10. Firms have a documented cybersecurity incident response plan in place that provides a roadmap for the actions the firm will take during and after a security incident.[6] Incident response plans address, inter-alia, the roles and responsibilities of staff, incident detection and assessment, reporting and escalation as well as response strategies to be deployed. A plan for communications with relevant external stakeholders, including customers, also forms a part of the response plan.

11. The firm notifies the Central Bank when it becomes aware of a cybersecurity incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

12. A documented recovery plan is in place to resume critical operations rapidly following a cybersecurity incident. Key findings from the lessons learned from cybersecurity incidents are incorporated into the refinement and update of control structures and the incident response and recovery plans.

13. Firms consider relevant good practices and internationally adopted frameworks for IT security risk management as may be appropriate for their firm.[7]

[6] There are many publicly available cybersecurity specific incident response guides that firms may find useful in this regard. These include but are not limited to: the Good Practice Guide for Incident Management from the European Network and Information Security Agency (ENISA), NIST Computer Security Handling Guide (Special Publication 800-61) and ISO/IEC 27002 (section 16) Information Security (Security Techniques) Code of Practice for information security controls.

[7] There are many frameworks and standards available including, for example, the ISO/IEC27001 and ISO/IEC27002, the National Institute of Standards and Technology ("NIST") Special Publication 800 series, and the NIST Framework for Improving Critical Infrastructure. The Payment Card Industry Security Council Standards, while mandatory for merchants accepting credit card payments, may also be a useful resource.

4. OUTSOURCING OF IT SYSTEMS AND SERVICES

Regulated firms increasingly rely on outsourcing service providers ("OSPs") of IT services, in many cases outsourcing all or part(s) of the IT function. A wide array of IT outsourcing services are available including those related to back-office functions, cloud services, system development and maintenance, website hosting, security and disaster recovery. Outsourcing does not reduce the inherent risks associated with IT or the business lines that are using it and firms are reminded that responsibility for the effective management of those risks remain with the regulated firm. Outsourcing can expose firms to additional and/or increased levels of risk relating to security, operational performance and business continuity, if not properly managed. Firms 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.[8]

In assessing the governance and risk management structures in place around outsourcing of IT systems and services, the Central Bank identified a number of inadequate practices, such as:

- Failure to carry out thorough due diligence on prospective IT OSPs.
- Service Level Agreements ("SLAs") lacking sufficiently robust provisions in relation to security, service availability, performance metrics or penalties.
- Failure to ensure that the outsourcing agreement provides for appropriate levels of support to be available for critical IT services.
- Inadequate monitoring of OSP service performance. This has resulted in, for example, shortfalls in service delivery going undetected by the firm for an extended period.
- Insufficient development of OSP exit management strategies and contingency plans.
- In respect of intra-group IT outsourcing and where the parent or group entity provides the IT service to the Irish firm, the Central Bank has frequently observed that SLAs were either not formally agreed or that only limited or umbrella SLAs existed. Where SLAs did

[8] Cloud services is an emerging area which the Central Bank and other supervisory authorities are giving ongoing consideration to. The Central Bank will be cognisant of future international regulatory guidance on this topic. Firms must fully understand the risks associated with utilising cloud services.

exist and key performance indicators ("KPIs") had been agreed, they were often not sufficiently monitored or reported on.

With regard to the governance and risk management structures in place around outsourcing of IT systems and services, the Central Bank expects that:

1. A framework is in place with clear lines of responsibility for ongoing management, operational oversight, risk management and regular review of the firm's OSPs.

2. Thorough due diligence is conducted on prospective OSPs. Due diligence includes consideration of, inter-alia, the OSP's technical capabilities, performance track record and financial strength and viability. The due diligence also considers whether the OSP can meet its requirements in relation to service quality and reliability, security and business continuity in both normal and stressed circumstances. Firms satisfy themselves that the selected OSP has sufficient and robust controls in place in relation to its cybersecurity. These controls should be at least as strong as the controls utilised by the firm itself.

3. The contract between the firm and its selected OSP 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;
   - includes requirements for service levels, availability, and reliability, including measurable performance metrics and remedies for performance shortfalls. Using the key provisions of the SLA, firms regularly monitor the service delivery performance to determine if the OSP is delivering to the required standards. Where performance shortfalls are identified, these are addressed with the OSP in a timely manner; and
   - includes provisions relating to system and information/data security, business continuity and disaster recovery, service scalability, assurance and service termination, where appropriate. In particular, where new storage services are utilised, such as cloud, contracts with cloud providers specify the location(s) where

the firm's data is stored, processed and managed, and the security measures required when transmitting and storing data.

4. Firms develop and maintain an exit management strategy to reduce the risks of business disruption should key IT outsourced services be unexpectedly withdrawn by the OSP, or voluntarily terminated by the firm. Viable options for resuming the impacted service(s) should be identified which are proportionate to the nature, scale and complexity of the firm; for example, in the case of smaller firms where transaction volumes are modest, a plan to revert to manual systems (with appropriate controls implemented) for a short period may be appropriate. 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.

5. Firms apply the same level of controls and oversight to intra-group IT outsourcing arrangements as to arrangements with external OSPs.

6. Firms monitor for the development of potential concentration risks and take appropriate action if they are, or are likely to become, reliant on a small number of OSPs to provide critical IT services. A high reliance on a single, or small number of providers, exposes the firm to a greater scale of potential business disruption risk.

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

Appendix 1: Glossary

In this paper, the following definitions are used:[9]

Business continuity: The capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.[10]

Cyber-attack: The use of an exploit by an adversary to take advantage of a weakness(es) with the intent of achieving an adverse effect on the IT environment.[11]

Cyber risk: The combination of the probability of an event occurring within the realm of a firm's or person's information assets, computer and communication resources and the consequences of that event for a firm or person.[12]

Cybersecurity: Refers to the set of controls and organisational measures and means (human, technical, etc.) used to protect information system assets and communication networks against all non-physical attacks, irrespective of the attack being initiated through a physical or logical security breach. Controls and measures include preventing, detecting and responding to all malicious IT activities perpetrated to information system assets, potentially affecting systems or data confidentiality, integrity or availability, as well as the traceability of operations executed on these information systems and networks.

Cybersecurity risk management: The process used by a firm to establish an enterprise-wide framework to manage the likelihood of a cyber-attack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyber-attack. The management of a firm's cyber-risk should support the business processes and be integrated into the firm's overall risk management framework.[13]

---

[9] In providing these definitions, it is recognised that there is limited standardisation and hence alternative definitions for some terms can be found in other sources.

[10] ISO 22301:2012, Societal security - Business continuity management systems - Requirements.

[11] Committee of Payments and Market Infrastructures & Board of the International Organization of Securities Commissions ("CPMI-IOSCO"), 'Guidance on Cyber Resilience for Financial Market Infrastructures', June 2016.

[12] *Ibid.*

[13] Committee of Payments and Market Infrastructures & Board of the International Organization of Securities Commissions ("CPMI-IOSCO"), 'Guidance on Cyber Resilience for Financial Market Infrastructures', June 2016.

Cloud services: Services utilising the storing, processing and usage of data on remotely-located computers, accessed via the internet.[14]

Disaster recovery: The process of rebuilding business operations or infrastructure after the disaster has passed.[15]

Information Technology ("IT"): Services, interconnected systems or hardware that make up the firm's IT infrastructure. This includes but is not limited to computers, their peripherals, storage devices, software, services (including cloud services and professional services that support the IT infrastructure) and related resources.[16]

IT inventory of assets: A comprehensive, regularly updated record of IT assets (including hardware, software, databases, connectivity arrangements and external services) employed by the Financial Firm and the policies for their operation, maintenance, upgrade and monitoring.[17]

IT risk register: A regularly updated listing of the attributes of known and potential IT risks that could affect the firm. At a minimum, the register should detail the likelihood and potential business impact of each risk materialising, and the owner of each IT risk type within the firm.[18]

Information assets: refer to data, hardware, software, networks or other elements of a firm's IT landscape that support information-related activities.

Regulated Firms (or Firms): Refers to entities regulated by the Central Bank of Ireland.

Operational risk: Operational risk is the possibility of negative financial, business and/or reputational impact resulting from inadequate or failed internal governance and business processes, people, systems, or from external events.

---

[14] European Commission - 'Unleashing the Potential of Cloud Computing in Europe', 2012
[15] SANS Institute White Paper 'Introduction to Business Continuity Planning'
[16] FFIEC - Information Technology Examination Handbook, 2015.
[17] ISO - Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2014.
[18] ISACA - Risk IT Framework, 2009.

Outsourcing: an authorised entity's use of a third party (the "outsourcing service provider") to perform activities that would normally be undertaken by the authorised entity, now or in the future. The supplier may itself be an authorised or unauthorised entity.[19]

Outsourcing service provider: the supplier of goods, services or facilities, which may or may not be an authorised entity, and which may be an affiliated entity within a corporate group or an entity that is external to the group.[20]

Risk appetite: The aggregate level and types of risk an organisation is willing to assume within its risk capacity to achieve its strategic objectives and business plan.[21]

Security event: Any observable occurrence in a system and/or network. Events sometimes provide an indication that an incident is occurring.[22]

Security incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[23]

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.[24]

[19] EBA - Guidelines on outsourcing, 2006.
[20] *Ibid.*
[21] FSB - Principles for an Effective Risk Management Framework, 2013.
[22] NIST Glossary of Key Information Security Terms.
[23] NIST Glossary of Key Information Security Terms.
[24] NIST Computer Security Handling Guide (Special Publication 800-61).

Appendix 2: Key International Guidance for Firms

Organisation	Guidelines	Issue date
Basel Committee on Banking Supervision	Principles for the sound management of operational risk	June 2011
Committee on Payments and Market Infrastructures & International Organization of Securities Commissions	Guidance on Cyber Resilience for Financial Market Infrastructures	June 2016
European Banking Authority	Guidelines on Internal Governance	September 2011
European Banking Authority	Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)	December 2014
European Banking Authority	Guidelines on the security of internet payments	December 2014
European Banking Authority	Guidelines on outsourcing	December 2006
European Insurance and Occupational Pensions Authority	Guidelines on system of governance	September 2015

September 2016

T **+353 1 224 4000**

www.centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Bosca PO 559, Sráid an Dáma, Baile Átha Cliath 2, Éire
PO. Box No 559, Dame Street, Dublin 2, Ireland