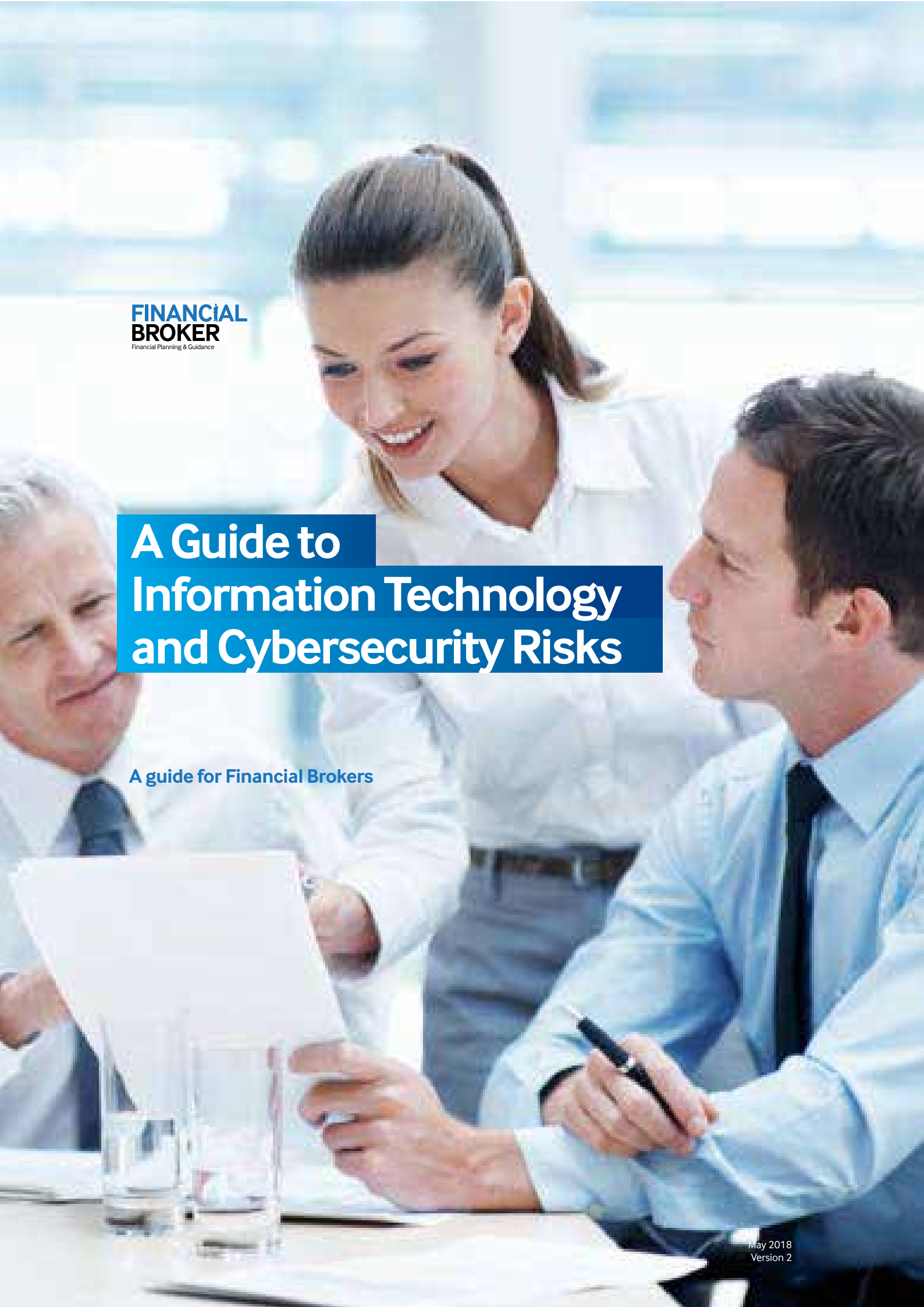
FINANCIAL BROKER
Financial Planning & Guidance

One – Unified Voice

A Guide to Information Technology and Cybersecurity Risks

A Guide for Financial Brokers

Creating your success through
Financial Planning



FINANCIAL BROKER
Financial Planning & Guidance

A Guide to Information Technology and Cybersecurity Risks

A guide for Financial Brokers

May 2018
Version 2

Contents

Version 1 published in 2017 authors Ray Armstrong and Jeffrey Hughes

Introduction

The purpose of these guidelines is to provide definition where required and advise members on the appropriate steps to be taken. Brokers Ireland recognises that the issues raised and requirements on members vary in accordance with the business model, size, and technological complexity of each member firm, and the sensitivity of its information and data. Consequently, for smaller firms, i.e. sole traders and onetwo person firms, some of the more specific aspects of the following sections may not be directly applicable.

The Central Bank's paper represents current thinking and is a reference point for regulated firms in relation to the expectations around information technology (IT) and cybersecurity governance and risk management. The paper doesn't represent all aspects of IT and cybersecurity, but rather those areas deemed most pertinent at the time of its publication. The Central Bank's guidance aims to minimise the risk of consumer detriment through effective mitigation strategies.

Brokers Ireland's guidelines are focused on the four core areas of Governance, Risk Management, Cybersecurity and the Outsourcing of IT systems and services. It is important to note that any IT touch points within a member firm fall under IT governance. This includes IT infrastructure, mobile devices, hardware, software, file storage and any other IT systems used within the firm.

Similar to the Central Bank's approach, this paper doesn't represent all facets of IT and cybersecurity, but rather those viewed as being most important for Brokers Ireland's members. The guidelines contained herein should not replace or supersede the legislation, regulations, guidelines, or standards that form part of a firm's regulatory obligations. No guidance from Brokers Ireland can cover all IT risks and necessary requirements.

About Saros Consulting

Saros Consulting, established in 2012, is headquartered in Dublin city centre. We provide independent, impartial expertise in:

- Consultancy and Advice
- IT Strategies
- IT Architecture and Design
- Project Management Services
- Vendor Selection and Management
- Reviews, Assessments and Audits
- Compliance

We work with clients in all sectors of national and international business. Our service enables you to meet your business objectives by having a solid, robust and scalable IT strategy. A Saros strategy will align your IT investments with your business goals.

IT is a vital component of modern business, be it big or small, but all too often the proposed solutions create more problems than they resolve; they add expense where they should create value.

Our vision is simple: we believe that great IT is transformational, driving business development and connecting people to their goals. Our approach is equally simple: we put our expertise to work in your best interests; we are part of your team, on your side always. We will examine, explore and evaluate, we will do so without fear or favour, in a manner that is clear and actionable. We provide the advice that empowers positive change.

We transform IT from a mandatory business component into a vital engine powering simplicity and security, connectivity and control all unified by our in-depth understanding. This is not about technology: this is about creating the springboard that drives business where it needs to go next.

About the Authors

Ray Armstrong

Ray is currently MD of Saros. Ray has over 15 years' international IT experience in varying industries including pharma, medical device, manufacturing, and professional services. He is an innovative, adaptable international IT executive with a highly effective mix of IT and business skills. His expertise is in IT strategy and programme management. Ray has gained considerable experience in the development, deployment and management of mission critical international IT environments.

Jeffrey Hughes

Jeffrey is an IT Strategy Consultant at Saros. He holds a Ph.D. in Strategy and IT from Trinity College Dublin. At Saros, Jeffrey's expertise resides in advisory and compliance services pertaining to IT strategy, in addition to being a certified PRINCE2 Practitioner in project management. The EU's upcoming General Data Protection Regulation (GDPR) and the Central Bank's IT and cybersecurity guidelines represent particular areas of focus.

Section 1 - How to approach IT Compliance

Firstly, the firm needs to identify and appoint a person within the firm who is responsible for IT. This person should be sufficiently senior and report to the Board. Subsequently, the pertinent stages in any IT compliance project are Assessment of the current position, Gap Analysis, i.e. identifying what shortfalls exist, and Remediation, i.e. action to be undertaken and new systems/measures to be put in place. Upon remediation, it is incumbent on the firm to continually monitor, audit and follow process (See Figure 1 for an overview of the key stages involved).

An initial understanding of the firm's IT environment is of paramount importance. Therefore, the project will generally begin with an assessment phase, with all areas of the IT environment in scope. For smaller firms or where it is felt that there is nobody within the firm with the required expertise to undertake these exercises, it would be recommended to enlist the services of a third-party provider. It is important that the firm should undertake due diligence when selecting a third-party provider, i.e. assess a range of suitable vendors, compare pricing, establish what service level agreements (SLAs) are available, and seek references from similar firms who have worked with the vendor.

In the context of the Central Bank's guidelines, there are four key categories with associated requirements. These categories and associated requirements should be at the forefront of the firm's approach.

With the above in mind, the following sections detail a pragmatic approach to achieving compliance.

Figure 1. Key Stages in Reaching Compliance and Remaining Compliant

2.1 Assessment

(Some aspects of assessment may not be applicable to smaller firms, e.g. the IT infrastructure of a sole trader may not have dedicated on-site servers or additional hardware more commonly found in larger firms.)

The assessment phase requires a thorough understanding and evaluation of all aspects of the firm's existing IT environment.

The assessment (either carried out by the sole trader/appointed individual within the firm for IT or third-party service provider) covers areas such as

- Infrastructure: a health check to ascertain the current state of all physical hardware, machines, office equipment, networks (how you connect to the outside world or other offices), models/versions, renewal dates, security (anti-virus), firewalls, disaster recovery, and business contingencies, e.g. if there is a fire and your server is destroyed, you need a system for getting the firm back up and running.

- IT systems and business applications: establish whether current systems are supported; their warranties, licences, and systems security; where they are stored and if they are backed up to an alternative environment; the firm's email provider, e.g. Hotmail, Gmail, Office365, and the associated security provided, i.e. email providers have differing degrees of security attached; the firm's domain name and domain name provider (if your firm does not have a domain name you should register one).

- Data security analysis: ascertain if client data is archived or backed up internally or to an external device, when backups are carried out and how frequently (see included Back up and Restore Business Continuity Standard Operating Procedure (SOP)). Conduct a walk-through of the incident response procedure should a data breach occur, e.g. if your email account is hacked or a laptop is stolen (see included Incident Management SOP).

- Governance: Does a governance framework exist? Are there SOPs governing IT? Example: if a member of staff takes home a laptop that has client information stored on it, are there safety procedures in place to protect the client's data?

- Strategy: does the firm have a written IT strategy or action plan in place? (See Appendix VIII for an IT strategy template.)

An inventory is usually conducted on all business applications and business process flows, including software and internal/external data. The assessment phase also reviews 'IT Housekeeping' type practices within a firm, including any current standard due diligence exercises regularly conducted that protect IT health and that are performed during the normal running of the business, e.g. ensuring that your anti-virus software is up to date.

Upon completion of the assessment phase all findings should be documented.

2.2 Gap Analysis

The gap analysis follows the assessment phase and is a comparative study between a firm's current IT environment versus the future compliant IT environment, effectively revealing the distance between the two. The gap analysis establishes whether the firm is compliant and acts as an enabler for future remediation activities. In the current context, a member firm's IT environment, i.e. the results of the assessment phase, are to be compared to the recommendations as found in the included IT Requirements Matrix (Appendix I).

A three-step process may be employed when conducting a gap analysis:

1. Analyse the firm's current situation
2. Identify the desired future state the firm wishes to reach (see included IT Requirements Matrix – Appendix I)
3. Define the distance between the two situations.

Upon completion of the above steps, it can be determined whether or not the requirements are being met. The Central Bank has specified key areas and has recommended that these areas of IT require focus. Prior to completing a Gap analysis, it is important that a firm has a solid understanding of these topics. The following

2.2.1 IT Strategy

(Some aspects of IT strategy may not be applicable to smaller firms.)

An IT strategy can be viewed as a firm's action plan. It is important that IT has its own plan that complements and supports the firm's business strategy.

In its simplest form, an IT strategy encapsulates strategic business and IT initiatives. Following strategic IT planning, the IT initiatives can be distilled into projects that support the firm in achieving its strategic business objectives. The purpose of the IT strategy is to ensure control around IT and to provide IT value-add services and projects.

A more detailed IT strategy can be viewed as a blueprint of a medium or long-term IT vision. It may remain relatively static over the duration of its tenure, or develop as a more fluid plan in response to the market and technology needs of a firm. See Appendix VIII for an IT strategy template.

2.2.2 IT Governance

At its core, IT governance is a framework that oversees effective and efficient use of IT throughout a firm. IT governance supports stated business goals. IT governance can be viewed as the structures around which firms align IT strategy with business strategy. It also aims to ensure that firms stay on track to achieve their strategies and goals. An IT governance framework should show how IT is functioning, including the key metrics management requires.

2.2.3 Risk Management

IT Risk Management (ITRM) can be defined as identifying, assessing, mitigating and managing risks within an IT environment. It can be viewed as the application of principles that manage IT risks within the firm. ITRM provides a process for managing risks associated with business operations. Its implementation does not ensure instant protection from risks. Moreover, a commitment is required to its active implementation on an ongoing basis. Ultimately, its function is to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions.

It's imperative for firms to continuously monitor risks within its business environment (see included Risk Register, Risk Management, and Risk Assessment SOPs), and subsequently instill an appropriate array of protection mechanisms. The included Risk Register provides a rating scale of 1-5 (with 1 = very low risk and 5 = very high risk, e.g. cyber-attack = 5) to document the likelihood of risks occurring, their potential impact upon the business, and an overall risk rating.

2.2.4 IT Disaster Recovery - Business Continuity Planning

A disaster recovery plan enables a firm to plan and recover from an unforeseen event and resume normal operations. Business continuity planning describes the processes needed to ensure that essential functions can continue during and after a disaster. These practices prepare a firm for unexpected events that could negatively impact business operations. This may include restoring data from backups or provisioning a second Internet connection in the event of the primary connection failing (see included Backup and Restore Business Continuity SOP).

2.2.5 IT Change Management

IT change management is the process, tools, and techniques used to manage the IT side of change so that the desired firm outcome is effectively and efficiently achieved. Change management is composed of at least three different components: adapting to change, controlling change, and effecting change. A change management policy details the process that governs IT changes within a firm. From an internal audit perspective, the policy tracks the scope, authorisation of the change, and roll-back plans. Examples of IT projects that may require change management include the implementation of a new customer relationship management (CRM) platform or moving to a new email service provider.

2.2.6 Cybersecurity

Cybersecurity can be defined as the protection of the firm's systems, networks and data. It protects against increasing incidents of IT attacks (see included Incident Management SOP). Such threats or attacks are becoming ever more prevalent, sophisticated and complex. Cybersecurity is increasingly important as firms continue to connect to the Internet in new ways.

A firm's cybersecurity policy should be proportionate to the risks faced by each individual firm, the basis of which should be a risk assessment.

Cyber-attacks may come in two forms:

- Firms may be subject to a deliberate attack should they be viewed as having valuable data
- The attack may be opportunistic in nature, brought about due to the discovery of a weakness in a firm's structure.

Data, intellectual property, and a company's reputation are becoming progressively important. Retaining control of these key assets is a challenge because of the aforementioned sophistication and regularity of cyber-attacks. Therefore, it is essential that each firm establishes an effective cybersecurity process (see Appendix V for Incident Management SOP) that is commensurate to its size, the nature of the business, and data requirements. This should include adequate staff training and on-going communication with staff regarding potential risks (see line 15 in the included IT Requirements Matrix – Appendix I). Cyber risk management should be aligned within the parameters of the overall IT risk management framework. A cyber security risk assessment is necessary to identify the gaps in your firm's critical risk areas and to determine actions to close those gaps. It should be assessed regularly.

2.2.7 IT Outsourcing

(Some aspects of IT outsourcing may not be applicable to smaller firms.)

IT outsourcing may be defined as the use of external service providers to effectively deliver IT-enabled business processes, applications, services and infrastructure solutions.

IT outsourcing management should provide a process to help select the right IT service providers, structure the best possible contracts, and govern deals for sustainable win-win relationships with external vendors. Key points to be considered when outsourcing:

- The establishment of clearly defined service level agreements (SLAs) with outsourcing providers that detail, but are not confined to, the nature, scope and quality of the service being offered by the outsourcing provider.
- The exit strategy should an outsourced service be voluntarily discontinued or withdrawn by the outsourcing provider. This may include an assessment of the viable options available for returning to business as usual, thus reducing the risk of business disruption.
- An assessment of the dependency on outsourcing service providers to ascertain whether there is an over-reliance on a small number of outsourcers and the establishment of remediation activities to address such a risk if present (may not be applicable to smaller firms that don't have the requirement for a large number of outsourcing service providers).
- Clarity that outsourcing arrangements in no way impede the Central Bank's ability to supervise the firm either on or off-site.

2.2.8 Standard Operating Procedures (SOPs)

SOPs are a set of instructions amalgamated by a firm to facilitate personnel in carrying out routine business operations in a uniform fashion. They help maintain ongoing compliance and reduce miscommunication. SOPs pertaining to risk management (Appendix II), risk register (Appendix III), risk assessment (Appendix IV), incident

management (Appendix V), backing up and restoring business continuity (Appendix VI), and a control matrix (Appendix VII) are included with this guideline.

2.3 Remediation

With a thorough understanding of the key topics above and having completed an assessment and a gap analysis, the remediation phase can begin.

The remediation phase aims to rectify any issue noted in the gap analysis phase. This phase also includes the writing of documents including SOPs and a control matrix (see included SOPs).

Remediation involves the creation of an action plan that will bridge the documented gaps. This plan facilitates moving from a state of non-conformity, i.e. if a non-secure environment exists, to a secure environment. Remediation plans generally impact:

- IT infrastructure, i.e. all physical hardware, machines, office equipment, models/versions, renewal dates, security (anti-virus), firewalls, disaster recovery, and business contingencies
- Applications that reside on internal or external IT infrastructure
- Governance, e.g. the SOPs within the firm that govern IT
- IT strategy: if there is an established strategy or action plan in place.

Remediation plans can include:

- IT projects such as infrastructure upgrades
- The writing of SOPs
- The implementation of controls
- The implementation of business systems
- The writing of a control matrix.

A control matrix (see included Control Matrix SOP) is an important element of the project and should be detailed during the remediation phase. Each SOP will have a series of controls. The controls require testing on a defined, regular basis. The controls are stored in the control matrix, along with the testing frequency and the evidence required to pass the test. The control matrix should be completed during the remediation phase and it is the guiding document during the adherence phase.

2.4 Adherence

Once the remediation activities have been completed, the firm can progress to business as usual, which incorporates embedded IT processes.

When a status of compliance has been achieved, it is incumbent upon an organisation to maintain that status. This covers the monitoring and auditing of the IT environment. Examples of adherence activities include, but are not limited to, audits, change management surveys, and reviews of standards and policies. Such activities enable the firm to remain secure and compliant on a continuing basis. The frequency of adherence activities is dependent upon the business model, size, and technological complexity of the member firm and the sensitivity of its information and data, but examples may include on a quarterly or bi-annual basis.

Any new business initiatives that have an impact on the IT environment should be reviewed and their impact assessed. All frequencies and review cycles are captured in the control matrix, which highlights the key controls. Audits are the key tool for continued compliance. A comprehensive review of a firm's adherence to regulatory guidelines is usually conducted by independent auditors. For example, they may review the firm's controls, security policies and risk management procedures. They evaluate the quality and completeness of preparations.

Section 2 - Summary

This document and its associated SOPs provide Brokers Ireland's members with a set of guidelines to assist in safeguarding against IT and cybersecurity risks. In summary, the outlined stages are:

- The firm needs to identify and appoint a person within the firm who is responsible for IT. This person should be sufficiently senior and report to the Board.
- Assessment: of the firm's IT environment, i.e. what systems and procedures are currently in place? The assessment stage may be carried out by a third party.
- Gap Analysis: compares the firm's current IT environment with the desired IT environment.
- Remediation: rectifies any issues noted in the gap analysis phase.
- Adherence: retains an ongoing status of compliance (aided by the use of the included SOPs and a commitment to continuous staff training around IT and cybersecurity risks).

APPENDIX I

IT Requirements Matrix v2.0

Central Bank IT Expectations	Reference Section in Central Bank paper	Current Status	Difference between Column A and Column C	Remediation required Y/N	Actions Required (Remediation)	Comments
Firms develop an IT strategy that is aligned and proportionate with the business strategy of the firm	Governance					
Firms have in place a comprehensive and functioning IT risk management framework (ITRM)	Governance					
Firms have a sufficiently robust IT governance structure in place - this will depend on the number of individuals within the firm	Governance					
Firms develop, implement, maintain and communicate an ITRM framework	Risk Management					
An IT risk register is developed and maintained	Risk Management					
Processes for IT incident detection, notification and escalation are developed by firms and all staff receive training on same	Risk Management					
The firm notifies the Central Bank when it becomes aware of an IT incident	Risk Management					
Firms have formal IT change management processes in place	Risk Management					
Resources are provided to support effective Disaster Recovery (DR) and Business Continuity (BC) planning, testing and execution	IT Disaster Recovery and Business Continuity Planning					
A documented DR plan is in place	IT Disaster Recovery and Business Continuity Planning					

APPENDIX I CONTINUED

IT Requirements Matrix v2.0

Central Bank IT Expectations	Reference Section in Central Bank paper	Current Status	Difference between Column A and Column C	Remediation required Y/N	Actions Required (Remediation)	Comments
A documented BC plan is in place	IT Disaster Recovery and Business Continuity Planning					
Firms have a documented back-up strategy for critical data	IT Disaster Recovery and Business Continuity Planning					
Firms have a well-considered and documented strategy in place to address cyber risk	Cybersecurity					
Security awareness staff training programmes are in place (N/A for sole traders)	Cybersecurity					
Robust safeguards are in place to protect against cybersecurity events and incidents	Cybersecurity					
Firms implement strong controls over access to their IT system	Cybersecurity					
The firm notifies the Central Bank when it becomes aware of a cybersecurity incident	Cybersecurity					
Thorough due diligence is conducted on prospective Outsourcing of IT Systems and Services Providers (OSPs)	Cybersecurity					
The contract between the firm and its selected OSP includes a documented SLA	Outsourcing of IT Systems and Services					
Central Bank supervision of the firm is not impeded by outsourcing agreements	Outsourcing of IT Systems and Services					

APPENDIX II
IT Requirements Matrix v2.0

[Insert Company Name] Standard Operating Procedure

Title: Change and Risk Management

Author	Company Name	Initiation Date	20th January, 2017
Document Number	SOP1008	Revision Number	1

Definitions/Abbreviations
SOP: Standard Operating Procedure
IT: Information Technology

Purpose
The purpose of this SOP is to assess the impact and risks of IT changes within [insert Company Name]. The change and risk management procedure applies to all computer systems in scope and ensures changes are evaluated, controlled and implemented correctly.

Scope
This procedure is applicable to all IT infrastructure systems including servers, switches, networking hardware, laptops, mobile devices and Microsoft Office applications. This procedure also applies to [insert Company Name] business applications.

Out of scope
IT systems outside the remit of [insert Company Name].

Responsibilities
Staff are responsible for reporting and informing of any risks and requesting changes where applicable.

Management are responsible for reviewing and approving changes.

The person responsible for IT strategy [insert Name] is responsible for reviewing risks and managing/applying changes.

IT vendors are responsible for applying changes where applicable.

Procedure
(Insert your own requirements here):

- A change request is received by the person responsible for IT [insert Name].
- The person responsible for IT [insert Name] reviews the change request.
- The person responsible for IT [insert Name] ascertains if budget monies are required.
- If applicable, the person responsible for IT [insert Name] requests management approval.
- The person responsible for IT strategy [insert Name] reviews change and assesses impact and risks.
- Risk assessment is conducted.
- Request is logged with support company.

- Support ticket is issued.

- Change is approved and implemented.

- Emergency changes: An emergency change is implemented to prevent continued business downtime or disruption If insufficient time is available, the person responsible for IT strategy, [insert Name], may secure change approval from the management team verbally. Post emergency change all details of the change and the approver must be documented.

Contact

The person responsible for IT strategy [insert Name]
[Insert Company Name] management team.

APPENDIX III
Example SOP Risk Register

Risk Register – [insert Company Name]
(Range of 1-5 for (P) and (I), with 1 = very low and 5 = very high)
Probability (P): likelihood of risk occurring / Impact (I): effect on firm should risk occur

Threat	Probability (P)	Impact (I)	Risk = P + I ÷ 2
Flooding			
Fire			
Severe Storms			
Wind Storm			
Snow Storm			
Explosion			
Gas Leak			
Structural Failure, e.g. Office Collapse			
IT – System Software			
IT – Applications			
IT – Hardware			
IT – Viruses			
IT – Hacking, Unauthorised Intrusions			
IT – Communications, Connectivity			
IT – Vendor Failure			
IT – Operational (Human) Error			
Utilities – Water			
Utilities – Electricity			
Utilities – Gas			
Utilities – Communications			
Criminal – Theft			
Criminal – Break-ins			
Criminal – Vandalism			
Criminal – Bribery			
Strike			
Human Error			
Other			

APPENDIX IV

Risk Assessment Template

- Used to assess an identified risk
- Probability scale of 1-5 (with 1 = very low and 5 = very high)

Risk	Probability	What needs to be done

APPENDIX V
Incident Management

[Insert Company Name] Standard Operating Procedure

Title: Incident Management

Author	Company Name	Initiation Date	20th January, 2017
Document Number	SOP1004	Revision Number	1

Definitions/Abbreviations
SOP: Standard Operating Procedure
IT: Information Technology

Purpose
The purpose of this procedure is to define the process that [Company Name] use to report, escalate, resolve, and communicate IT problems and issues.

Scope
The scope of this SOP covers the process [Company Name] follow when requesting technical support.

In scope
- Hardware
- Software

Out of scope
N/A

Responsibilities
[Company Name] employees are responsible for informing the person responsible for IT [insert Name] of any IT problems or issues. If the person responsible for IT [insert Name] is unable to resolve the issue, they should then contact the helpdesk of their service provider where applicable.

[Insert Service Provider company name] are responsible for providing IT support via their helpdesk to all [Company Name] employees.

Business application vendors are responsible for providing IT support relating to their applications.

Incident Prioritisation
When dealing with a third-party provider, ensure that you have a suitable coding process. Please refer to the below example.

Priority coding system			Urgency		
			High	Urgency	Low
			• The complete service cannot be used • Risk of high financial impact • Risk of legal violations • Obvious security Company Name??? What does this mean? • No workaround or other temporary solution is available to enable continuation of work	• Limited usage of service • Work can be postponed using a workaround • Security at risk	• Limited usage of the service, only a few parts or modules cannot be used • A workaround, other temporary solution is available to enable continuation of work
Impact	High	•All users are affected or •An entire site or individual production is affected or	1	2	3
	Medium	•All users are affected or •Complete department affected	2	3	4
	Low	•1-5 users are affected	3	4	4

Procedure

- [Company Name] users contact help desk via email [insert email] or phone [insert phone number].
- Support company receives issue and log ticket.
- [Company Name] receives a ticket number via email.
- Support company assesses issue and resolves.
- If issue cannot be resolved by help desk, issue is escalated to next level of your support.
- Troubleshooting complete, issue resolved.
- (Depending on the severity of the incident, e.g. if clients' data has been compromised, a communication strategy and/or disaster recovery and business continuity plan may need to be devised.)
- User notified and ticket closed.
- Emergency out of hours issues are escalated to [name of Service Provider].

Contacts

[Name of Service Provider]
Phone number: [insert phone number], Email: [insert email address]

Emergency contact numbers

Contact name, e.g. Helpdesk Manager (number as listed for Service Provider office).

APPENDIX VI

Back up and Restore Business Continuity

[Insert Company Name] Standard Operating Procedure

Author	Company Name	Initiation Date	20th January, 2017
Document Number	SOP1003	Revision Number	1

Definitions/Abbreviations

NAS: Network Area Storage
SOP: Standard Operating Procedure
IT: Information Technology

Purpose

The purpose of this SOP is to detail the process within [insert Company Name] to back up and restore data and information. The [insert Company Name] network holds information and data that requires restore in the event of loss or a serious systems disaster scenario.

Scope

This SOP describes the back-up and restore procedure that is used for all network data.

Out of Scope

Information stored on third-party vendor servers, e.g. Office 365.

Responsibilities

- The person responsible for IT strategy is responsible for ensuring that correct data is backed up.
- [Insert Company Name] management are responsible for ensuring backup governance.
- How long data is required (Should it say who is responsible for deciding this? Either way it's not a complete sentence so it jars with the rest.)
- [Insert Service Provider name] are responsible for maintaining all backups.
- [Insert Service Provider name] are responsible for executing restores.
- [Insert Service Provider name] are responsible for test restores.
- The person responsible for IT strategy is responsible for approving restores.

Procedure

(Insert your own requirements here.)

Example:

File and data backups should be completed using off-site (cloud) type solutions or historically tape-based back-up solutions.

Example 1: Cloud backup

- An appropriate provider should be selected (see Outsourcing section).
- The back-up routine should be agreed.
- Recommended: weekly, monthly, and yearly full backups and daily incremental backups.
- Upon completion of any backup, the firm should receive an email notification report.
- If the backup has been successful, no intervention is required. If the backup has failed, intervention is required from the service provider.
- A test restore from the backup should occur frequently.

Example 2: Tape backup

If you are currently using a tape backup, we recommend migration to a cloud solution as noted in Example 1.

- An appropriate provider should be selected (see Outsourcing section).
- The back-up routine should be agreed.
- A tape drive should be connected to a server.
- 20 tapes should be procured
  - 4 daily tapes
  - 4 weekly tapes
  - 12 monthly tapes.
- The rotation process
  - 4 times per week a daily tape is used for a backup
  - Once per week a weekly tape is used for a backup
  - Once per month a monthly tape is used for a backup.
- Upon completion of any backup, the firm should receive an email notification report.
- If the backup has been successful, no intervention is required. If the backup has failed, intervention is required from the service provider.
- A test restore from the backup should occur frequently.

Contact

[Name of Service Provider]
Phone number: [insert phone number], Email: [insert email address]

APPENDIX VII
Control Matrix

Please find below a list of the key attributes of an IT strategy:

Time Frame
An IT strategy usually covers three to five years; however, it can be tailored to suit shorter time frames if necessary.

Document Length
This is dependent upon the size and scope of the organisation, i.e. it may be a one-page document or it can be 12-15 pages in length in a complex IT environment.

Executive Summary
The plan should begin with a summary targeted for the business audience, i.e. relating the IT plan to the business objectives.

Scope
Provides an overview of the IT strategy and the associated goals and plans. It may take the form of a roadmap for IT.

Business Context
This is an important aspect in ensuring alignment of the IT strategy with the business strategy. This section effectively lays out how the requirements of the business acted as a driver to shape the IT strategy, e.g. the firm is pushing to reduce costs, and a range of IT hardware and software has been identified to assist in achieving this requirement.

IT Objectives
Sets out the objectives from an IT perspective that the firm wishes to achieve.

IT Principles
The tenets that influence all aspects of IT decision making within the firm, e.g. a cost-conscious approach will see the firm look to procure low cost IT hardware and software. IT principles normally take the form of short statements.

Metrics
Essentially a range of tools that enable the firm to assess the progress of the IT strategy without the need to wait for a formal review, e.g. all laptops to be upgraded by a certain date.

Review
A formal review should take place at pre-defined time frames, e.g. bi-annually, to assess in detail the progress of the IT strategy.

FINANCIAL BROKER
Financial Planning & Guidance

Financial Broker *a Brokers Ireland initiative* for all Financial Brokers

87 Merrion Square, Dublin 2
T: +353 (0)1 492 2202 **F:** +353 (0)1 499 1569

www.financialbroker.ie

Creating your success through Financial Planning