International Association of Accountants Innovation & Technology Consultants

ENISA Risk Management
Pilot Study - 2008

Prepared by:
IAAITC
200 Brook Drive
Green Park
Reading RG2 6UB

December 2008

Contents

Executive Summary

Four Member Firms of the IAAITC conducted pilot studies on a number of their clients using the ENISA Risk Management Methodology.

The material used was the ENISA deliverable of 2007 as subsequently amended by the IAAITC to produce a card set colour coded as high /medium / low risk (red / yellow / green).

The same colour coding methodology was used in the preparation of the reports:

Red	=	item was of high importance and required immediate attention
Yellow	=	item was of importance and would require attention
Green	=	complied or was irrelevant

6 businesses (client firms) of differing business types /sizes completed the pilots.

Pilot No	Business Type
1	Accountants
2	Training College (Journalists)
3	Scientific Membership Society
4	Event Management
5	Financial Services
6	Physiotherapy Services

Examination of the Pilot Reports will show that issues were easily and quickly identified:

Pilot No	Risk Profile	No of Red Issues	No of Yellow Issues
1	High	11	7
2	Medium	8	12
3	Medium	6	4
4	Medium	6	6
5	High	4	0
6	High	13	10

Having conducted these pilots we would conclude:

- The ENISA methodology is effective at quickly identifying the relevant issues across businesses from a number of sectors.
- Some familiarisation is required if a consultant is going to use the methodology and material, but this is minimal.
- As the material stands at the moment micro businesses would be unlikely to conduct their own self assessment and are unlikely to be prepared to pay a third party to do it.
- Some customisation / simplification of the material would be of help in rolling it out at the micro and small business level.

1. Introduction

1.1 Background Information

The IAAITC had commenced working with the ENISA deliverable on Risk Management in 2007.

Following the broad concepts as we understood them we developed what is effectively three sets of cards the controls being colour coded red / yellow / green:

- The four step methodology
- Organisational Controls
- Asset Controls

During the later part of 2007 the IAAITC with a number of firms ran some pilot workshops on the topic of Risk Management. These were to general audiences and we found that trying to address businesses of different types and sizes together did not work effectively as it was very difficult to get the level right. Micro businesses did not necessarily accept that they could be HIGH Risk, and larger businesses sometimes felt they should be HIGH when in reality they were not.

During 2008 the IAAITC has run some workshops specifically for Accountants. Using the material as it stands with an audience from one sector is a lot easier. Initially the material was delivered and the delegates were encouraged to reach their own conclusions. More recently we have amended the format so that for example rather than asking them to decide if they are HIGH risk, we tell them that they are and explain why. This approach allows more time to be spent on the controls.

The material could be improved further for this sector which is something we would like to consider with the help of ENISA during 2009.

1.2 Scope and objectives of the pilots

It was agreed with ENISA that a number of IAAITC Member Firms would conduct pilots within their client base. Being Chartered Accountants, with an understanding of audit principles it was felt that accountants would be a possible channel for delivering this material particularly in the micro and small business sectors which tend not to be addressed by the IT industry.

The objective was to conduct 5 Pilots.

The firms selected were from different parts of the country and they were allowed to choose the client(s) they used. They were asked to nominate a number of clients and the final selection was made to ensure that different industry sectors and size of business were involved.

The objectives were as follows:

- How easily could a third party (in this pilot - accountants) grasp the concepts and understand the methodology.
- How effective was the material when used across businesses of different sizes and types.

2. Selection of firms and deployment of pilots

2.1 Selection of firms

A number of Member Firms were given the opportunity to become involved in the exercise. The only criteria being that they had a familiarity with IT, which all members of the IAAITC inevitably have, and a familiarity of audit procedures.

The familiarity with audit had an interesting implication which we failed to consider. Whilst all accountants will be familiar with audit and have done some during their training not all follow this discipline once they qualify.

Where we had a member who was still involved in audit and up to date with current methodology to international accounting standards we encountered some interesting issues. Financial Risk being a topic covered in audit meant that he had slightly different views on how a business should be profiled.

2.2 Approach followed in the deployment

Although five IAAITC Member firms were engaged to conduct pilot studies, in the end only 4 completed the pilots within the required timescales. Only 6 pilots have been done in total.

The material that they were given to use was the material produced by the IAAITC from the ENISA deliverable last year.

The Member Firms were briefed together on the material, although all had already seen it in a workshop environment. The four step process was explained although they were not specifically briefed on a preferred methodology for delivering the material. It was expected that they would in view of their general professional and audit experience all approach the task the same way, which with some minor exceptions proved to be the case.

The Firms, conducting the pilots, all of whom are Chartered Accountants who position themselves as Business Advisors were:

Firm	Location
RMT	Newcastle upon Tyne
WKH	Letchworth
PEM	Cambridge
Morris Owen	Swindon

In selecting the Clients it was agreed that we should endeavour to select businesses that were typical and not geographically specific for this exercise. Our justification for this being if we choose typical businesses then in future there would more possibility in extending the reach for deployment.

So for example there are accountants in every town and city in the UK, similarly there are various types of training /membership establishments / or medical services.

Certain business types are more geographical located. Whilst it would have been interesting to do some work in say the tourist industry we have to accept that in the UK that industry is confined within fairly clear regions.

The business types chosen were therefore thought to be relevant to all parts of the country.

Pilot No	Business Type
1	Accountants
2	Training College (Journalists)
3	Scientific Membership Society
4	Event Management
5	Financial Services
6	Physiotherapy Services

2.3 Validation of the pilots

We have since the beginning of 2008 been working with the School of Computing, Engineering and Information Sciences of Northumbria University. The University was extremely impressed with the ENISA material and the IAAITC treatment of it. They will shortly commence validating the pilot studies as a separate exercise.

3. Comments and issues identified

3.1 Basic Approach

The simplified approach of the 4 step process works extremely well. The concept of the cards is generally good.

From our experience inevitably we feel that there are some areas where more detail is needed and others where less complexity is required. We do however accept that this is a limitation of trying to create generic material.

It is worth noting that one firm although only required to do one pilot, actually did 3 because they **wanted** to and is now waiting to be told what to do next!

3.2 Outsourcing Options

This section could be simplified and there are issues in the questions asked.
If for example we are dealing with micro businesses, asking if they can make available two to five people for the project is probably not an appropriate question. There are also issues over the wording although this is probably a translation issue for example. "Does your business and service offerings include financial transactions?" is basically asking do you sell any goods and services. What we suspect is meant by this is "Does your business and service offering include financial services?" such as those regulated in the UK by the FSA.

We would consider a simpler breakdown – which should be along the lines of:

- Do you have the time available within the organisation to carry out this review?
- Do you have the knowledge available in the organisation to carry out this review?
- Do you want an external assessment of your Risk Management position?

Based on these questions a business should be able to decide whether they wish to carry out the review in-house, outsource all of the review to an external assessment body, or a combination of the two.

Another possible option is to award points to each question and introduce an element of weighting – as in a survey. i.e. On a scale of 1 to 10 – rate your IT knowledge. The decision on whether to outsource can then be based on the overall score.

This would also enable a simple web based survey to be built.

3.3 Risk Profile selection

3.3.1 Legal and Regulatory

The sensitivity of the data held focuses on the data of third parties. Many organisations hold information on their own organisation, products and services which would also represent a major business risk if accessed by unauthorised people. Examples include all forms of Intellectual Property, such as product information for technology companies.

The criteria for this profile could be based on asking the business to identify what they consider the key information held, and then assigning a risk to that data being lost or disclosed to unauthorised people.

3.3.2 Productivity and financial stability

Basing the risk purely on financial turnover or number of employees possibly allows scope for error. The turnover is irrelevant in terms of the level of risk, and risks confusing the issue. The number of employees is useful for giving an idea of the number of contact points, but again this does not take into account the type of business.

A number of the pilot businesses felt that this seemed to bias the survey to small organisations being low risk, whereas in many cases this would not be true.

Also the financial criteria listed have a gap between the medium level (up to £6M) and the High level (over £15M) which needs to be corrected. (This is as a result of us setting the medium level to coincide with the audit threshold. Accountants will view businesses where they are doing a statutory audit slightly differently from businesses where no audit is required.

3.3.3 Reputation and Loss of Customer Confidence

Whilst the idea of this risk area is valid it can be difficult to assess and quantify. We could consider including timescales as well as amount of user access. i.e. would there be a significant impact on the business if an outage lasted one hour, one day or one month? (When we covered this topic at events specifically for accountants the responses varied across departments and the time of year you selected to have a disaster. So for example any form of outage in January which is the peak time in the UK for personal tax returns is unacceptable to the tax department, but the payroll departments could accept outages for quite lengthy periods unless it was the last week of the month when the majority of payrolls are run.)

The other point that needs emphasising is that these are guidelines and not necessary to be taken literally. Any financial criteria need to take into account the business type – a small car dealership may have a very high turnover because it deals in high value goods, but an accountancy firm may have limited turnover because the only sales are service costs. In short – the person carrying out the review should use their discretion to determine the overall risk level of the organisation, using the criteria only as guidelines.

3.4 Asset Selection

This whole section works for larger organisation but at the micro-business level it adds an extra level of complexity.

For Micro-businesses and businesses under 25 employees we would consider a more simplified standard structure. This would still encompass the main typical assets but provide a simpler structure for people to follow.

We would consider basing it on the following six assets:

> Data storage – the machines and locations where you hold your data.
> Archiving and Backup – how you back up and keep protect your information in case of loss.
> Connecting Devices – machines used to access data (PCs, laptops, thin clients, PDAs).
> Staff – your employees and how they access information.
> Infrastructure – access security and resilience.
> Applications – software used to access data.

The current structure of the asset selection can lead to unnecessary duplication. An example of this is where an infrastructure asset is selected; there are numerous questions on data backups. However you also have the ability to select "Archiving and Backup" as an option in its own right. This effectively gives duplicated questions, and also leads us to ask – do you back up your backups?

The whole area of networking assets is possibly only relevant for the larger organisation. There are fewer points of risk associated with these in a small business and arguably are much lower that the other three asset categories. We would therefore suggest making network infrastructure a single asset option in the infrastructure category and reduce the number of categories to three.

One point made by the clients was the lack of focus on soft assets – i.e. the data itself. Perhaps there should be a category or section which focuses on the actual data, procedures for data changing, audit logs of changes, etc.

3.5 Card Selection

The idea of using the risk profile and asset identification to select the appropriate cards is a good one and works fairly straightforwardly. We would certainly recommend that this process is carried on going forward.

As above – for Micro-businesses we would suggest standardising the assets so that the only variant is risk profile, as this would simplify the process for them. For larger organisation the current process is appropriate and relevant.

Alternatively we could consider just apply the simplified asset selection process to organisations with a Low or Medium risk profile, whilst those of a high risk do the full asset selection process.

3.6 Card contents

Generally these are appropriate and produce valid questions for the organisation and assets concerned. The structured layout makes it fairly easy for the assessor to identify the questions to be asked. There is still, however, the need for a degree of discretion on behalf of the assessor to ensure that inappropriate questions are not asked.

There are a number of controls that refer to more technical questions, and therefore it is necessary for the assessor to have a certain level of technical knowledge. We believe that for the assessment to have validity it will be necessary for the assessor to be sufficiently knowledgeable in both IT and business. Few small organisations would have staff of appropriate skills to complete the assessment.

The cards make no allowance for the provision of outsourced services. Many small organisations outsource their IT support and maintenance to third parties, and many of the questions focus on the controls for internal staff. With the expected increase of SaaS, and internet services generally perhaps a separate set of cards could be produced focusing on the provision of outsourced services.

(We have for example come across organisations offering hosted services and whilst the servers may be located in a secure environment (by no means the norm) the associated administration procedures leave much to be desired.)

3.7 Gap analysis

Going through the controls to identify what is currently in place and what gaps exist is fairly straightforward. The general consenus amongst the Member Firms was to use a traffic light system to identify current gaps based on the following:

Red This control is not currently in place in the organisation.
Orange This control is in place, but needs to be reviewed or updated.
Green This control is in place and is up to date.

This then provided a simple checklist from which the client can see the actions they are required to take.

4. General Findings

Our general conclusion is that this methodology works well for companies of a certain size, which would have the resource to do it themselves, but does not scale down sufficiently to provide a suitable framework for micro organisations. These organisations require a simpler framework that can be processed more quickly and with less outside input.

For micro businesses we consider that the Asset Selection could be simplified and probably based on 4 levels of technology assets.

- Stand alone PC
- Multiple stand alone PCs
- Peer to Peer Network
- Single Server Network

We also feel that if variations of the material which were sector specific were developed it would be easier to deploy. The Institute of Chartered Accountants of Scotland (ICAS) has expressed an interest in the possibility of being involved were we to develop material specifically for the accountancy profession.

The likelihood is that other bodies / membership organisations would also be interested if material was available for their specific sector.

1. In general all of the firms are pleased with the deliverable, and would like to see further developments.

2. A general point is the English, whilst we know what you are trying to say, will the small businesses or will other countries where English is not their first language be able to translate into their own native language accurately. We think some work needs to be done on refining the language in some areas.

3. One of the major points to consider is - who is the targeted audience for this material. None of the accountants think that the micro businesses would have the resource or skills to do this themselves, and most would not see a value in paying a third party. There are potentially going to be problems with terminology if we stick to the business sizing according to European guidelines. There are plenty of micro organisations with turnovers of less than 1million, which should be high risk but could classify themselves as low given their size and turnover. Perhaps some of the most obvious examples are small firms of accountants or lawyers.

4. One consideration would be to target the regulated industries with a more specific selection of the material.

5. The review works well for larger organisations where the client is able to devote some time to the project and/or is prepared to pay a fee for an assessor to carry out the review for them. In the case study of a 150 employee firm the project would therefore be seen as a feasible and worthwhile project.

6. For a smaller organisation, such as the case study of 15 employees, the process is too complex and time consuming given the level of value the client would put on the project.

They would not have spent the time using in-house resource to complete the project, and given the time involved the price of this survey from a third party would have been in the region of £500 - £750 for their organisation. Whilst they benefited from the results of the review, in a commercial setting where they were paying for an assessor they would probably have chosen not to go ahead.

7. If the packs had been sent out to the pilot clients, they would possibly have tried doing it themselves as they had already been briefed by the accountant. But if it is generally made available to businesses there needs to be a point of contact for them if they have any questions or require further assistance. Obviously this is a role the IAAITC members could look to cover on a regional basis.

Appendices

Appendices

IAAITC - Risk Management Pilot Studies for ENISA

Key to Pilot Studies

Pilot No	Business Type	Conducted by:
1	Accountants	Peters Elworthy & Moore (PEM)
2	Training College (Journalists)	Peters Elworthy & Moore (PEM)
3	Scientific Membership Society	Peters Elworthy & Moore (PEM)
4	Event Management	Morris Owen
5	Financial Services	WKH
6	Physiotherapy Services	RMT

PEM IT Services

A division of Peters Elworthy & Moore

Salisbury House
Station Road
Cambridge
CB1 2LA

Email: it@pem.co.uk
Tel: 01223 728222
Fax: 01223 461424
www.pemit.co.uk

Risk Management Review

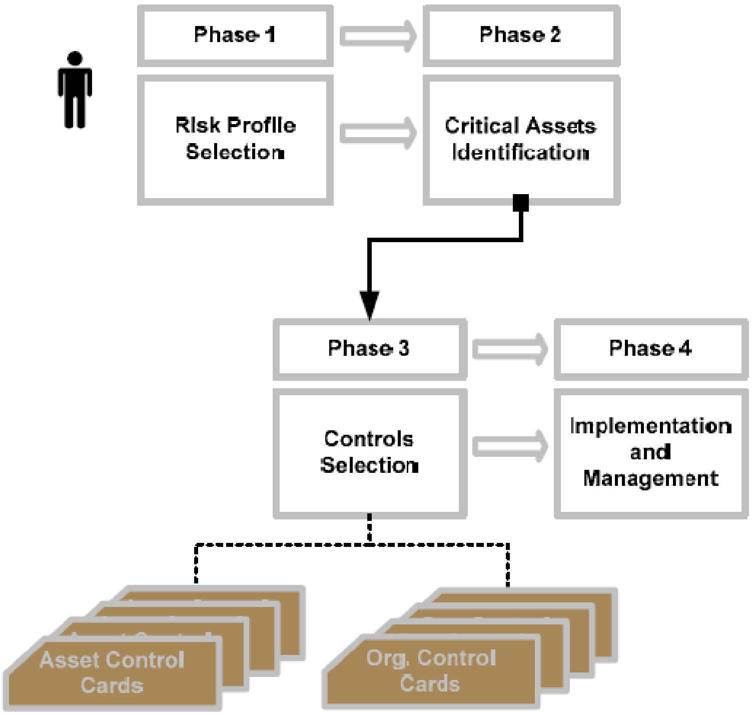
A review
for
Pilot 1

Proposal of IT Services

This document is a review of the Risk Management and IT Security requirements for Pilot 1

Contents

1. Objective of this review



Part of the responsibility of MSB Managers is to provide for the security of their business environment. According to most applicable legal requirements, liability for breaches of security lies with them.

Just as they must provide a safe and secure physical environment, they must also make sure that information is protected. Given the fact, however, that computers are not “fix and forget” devices, the protection of information is a permanent concern.

This review provides an overview of the key information security risks for the organisation. It then provides a gap analysis to show the areas which are currently covered by internal procedures and policies, and highlights the areas that still need to be addressed or re-visited.

2. Who should carry out this review?

There are three alternative ways in which this review can be approached:

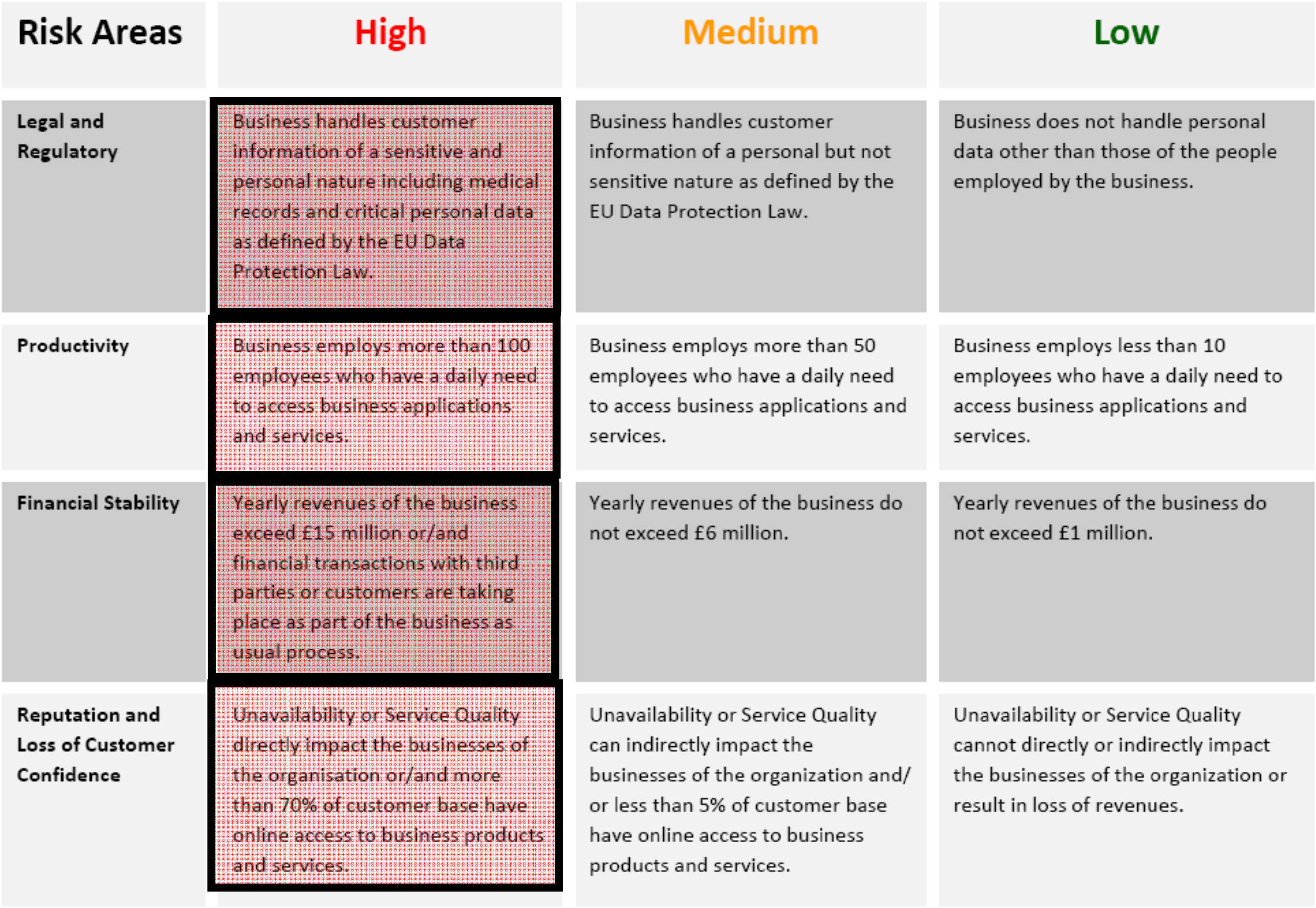
- In-sourcing of risk assessment – all reviews carried out by in-house staff.
- Partial outsourcing of risk assessment –initial review done by external advisor, then ongoing reviews carried out internally.
- Full outsourcing of risk assessment – entire review process is carries out by an external contractor.

Having considered the guidelines from ENISA, Pilot 1 has decided to take the partial outsourcing option. This is based on the following criteria:

- The organisation is over 150 employees, and has a relatively complex IT infrastructure.
- Internal staff have a good internal knowledge of IT Systems and Networks.
- The organisation has two or three employees that they can allocate to this project.
- The organisation operates in a highly regulated business sector that is subject to strict legislation.
- There is a need for staff to focus on their core competencies, so time available for the project is limited.

3. Risk Profile Analysis

The organisation's risk profile has been considered from four separate angles, to identify the level of risk the organisation places on its information security.



Risk Areas	High	Medium	Low
Legal and Regulatory	Business handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	Business handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	Business does not handle personal data other than those of the people employed by the business.
Productivity	Business employs more than 100 employees who have a daily need to access business applications and services.	Business employs more than 50 employees who have a daily need to access business applications and services.	Business employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues of the business exceed £15 million or/and financial transactions with third parties or customers are taking place as part of the business as usual process.	Yearly revenues of the business do not exceed £6 million.	Yearly revenues of the business do not exceed £1 million.
Reputation and Loss of Customer Confidence	Unavailability or Service Quality directly impact the businesses of the organisation or/and more than 70% of customer base have online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/ or less than 5% of customer base have online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

Pilot1 handles very sensitive customer data, including dates of birth, marital status, salary and tax information. Therefore their risk for Legal and Regulatory non-compliance is HIGH.

Pilot 1 employs over 150 people who have a daily need to access business applications and services. Therefore the risk to Productivity is HIGH.

Pilot 1 has an annual turnover under £10 Million, but also has responsibility for client monies, such as the paying of customer staff through it's payroll bureau. Therefore the financial risk is HIGH.

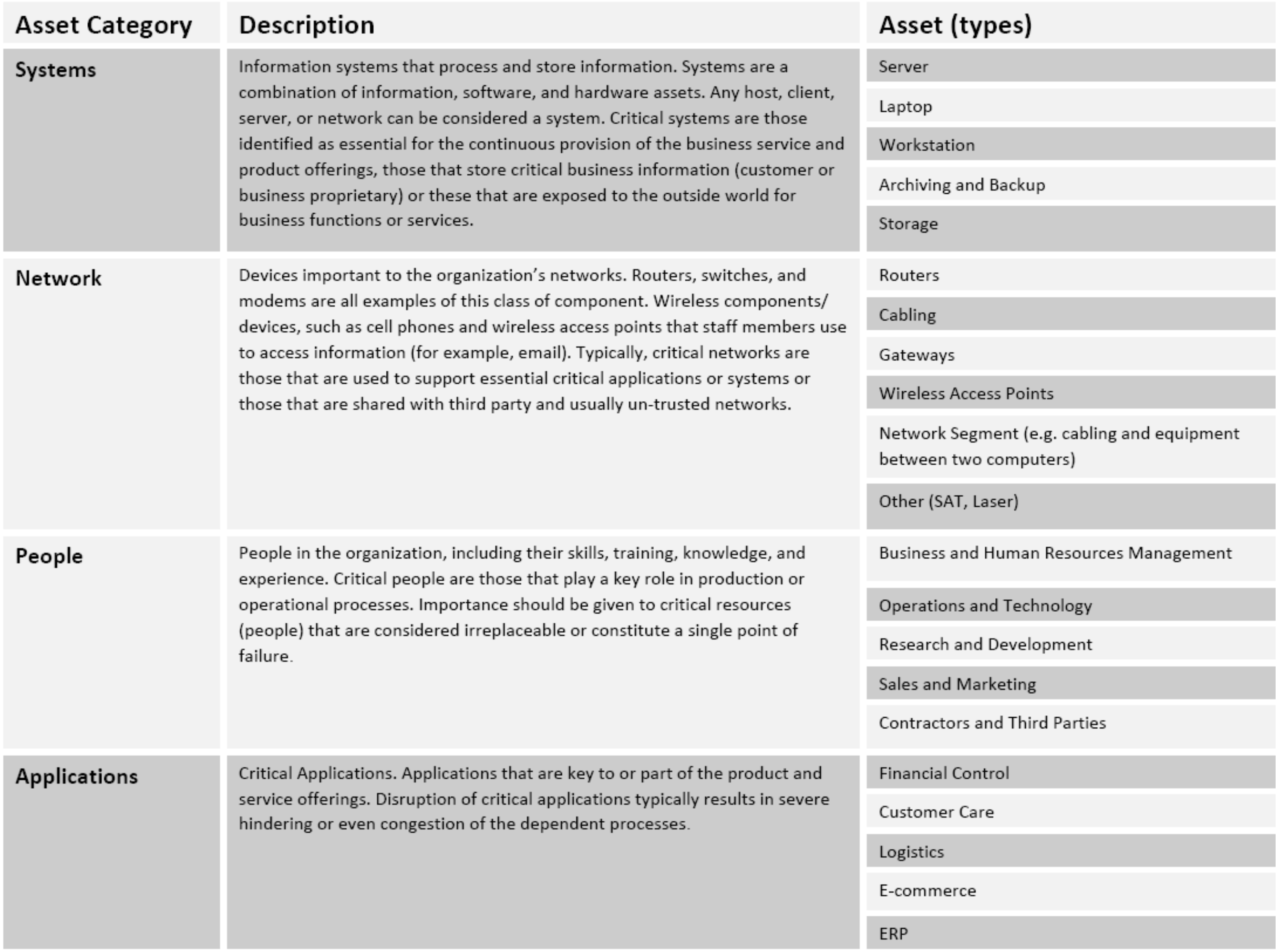
Pilot 1 employees rely on their computer systems for much of their work. The provision of many services are dependant on the IT system, including completing tax returns, providing audit reviews, provision of payroll services, and the provision of bookkeeping services. Furthermore, the organisation is working towards a "Paperless" environment where the data held is only available electronically. This places additional reliance on the IT systems for the provision of their services. Therefore the risk to reputation or loss of customer confidence is HIGH.

It is therefore established that the overall risk level for Pilot 1 is HIGH.

4. Identification of Critical Assets

It is important for the organisation to identify the key assets which the organisation has, from an information security perspective. These need to be identified on the basis of the adverse impact they are likely to have on the organisation in the event of the following:

- Disclosure of information to unauthorised people.
- Modification of information without authorisation.
- Loss or destruction of the asset.
- Interrupted access to the asset or information stored.



Asset Category	Description	Asset (types)
Systems	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information (customer or business proprietary) or these that are exposed to the outside world for business functions or services.	Server Laptop Workstation Archiving and Backup Storage
Network	Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of component. Wireless components/ devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with third party and usually un-trusted networks.	Routers Cabling Gateways Wireless Access Points Network Segment (e.g. cabling and equipment between two computers) Other (SAT, Laser)
People	People in the organization, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes. Importance should be given to critical resources (people) that are considered irreplaceable or constitute a single point of failure.	Business and Human Resources Management Operations and Technology Research and Development Sales and Marketing Contractors and Third Parties
Applications	Critical Applications. Applications that are key to or part of the product and service offerings. Disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.	Financial Control Customer Care Logistics E-commerce ERP

Based on the criteria above, the following assets have been identified as the most critical assets to Pilot1:

1. **Data storage**. Pilot 1 are an information business. The data they hold is critical for the running of the organisation. If that data is lost completely there is a strong likelihood the organisation would not survive. Therefore the servers holding this information are a critical asset.

2. **Archiving and Backup**. Should there be an loss of data from the data storage, it is critical to Pilot 1 that the data can be recovered quickly with minimal loss.

3. **Qualified Staff**. As a knowledge organisation Pilot 1 rely heavily on staff to input, modify and protect client data. To work effectively they have access to large amounts of sensitive information.

4. **IT staff.** To provide support to their staff, Pilot 1's IT staff have high level access to most of the data on the network. They are also responsible for ensuring data is protected and IT policies are properly implemented.

5. **Citrix Servers**. These are used by staff to access the applications that hold the client data. These servers are therefore configured to provide users access to applications they use, and to restrict users from accessing information that they do not need access to.

6. **Laptops**. Whilst the organisation holds most of it's data centrally, staff have the ability to copy data to laptop machines to enable them to work away from the office.

7. **Key Applications**. There are four key applications which manage the majority of information held at Pilot 1.
    a. **MYOB Central** – holds client contact details, along with all the billing and fee information.
    b. **MYOB Pertax** – holds Personal Tax information, including DOB, income and tax details.
    c. **Caseware Audit** – hold all client audit files, including review information for legal compliance.
    d. **Star Payroll Professional** – holds payroll details for all payroll clients and their employees.

The organisation has numerous other assets, which would also potentially provide risks to the data held by Pilot 1. These assets include thin client devices, fibre optic links between the offices, Internet connection, other applications, networking devices and cabling. However the risks associated with these are deemed to be lower than those listed above, and the impact of any disruption caused by failures of these is considered to be lower.

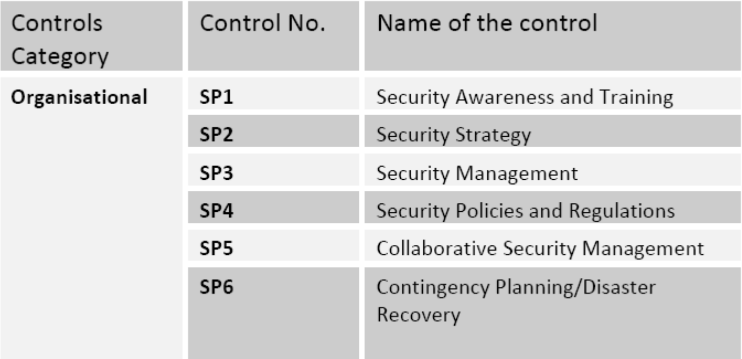
For the organisation to have a comprehensive risk management strategy we would recommend that these assets are reviewed in the future once the high risk assets have been properly examined.

This review will focus solely on the most critical assets identified above.

5. Control Card Selection

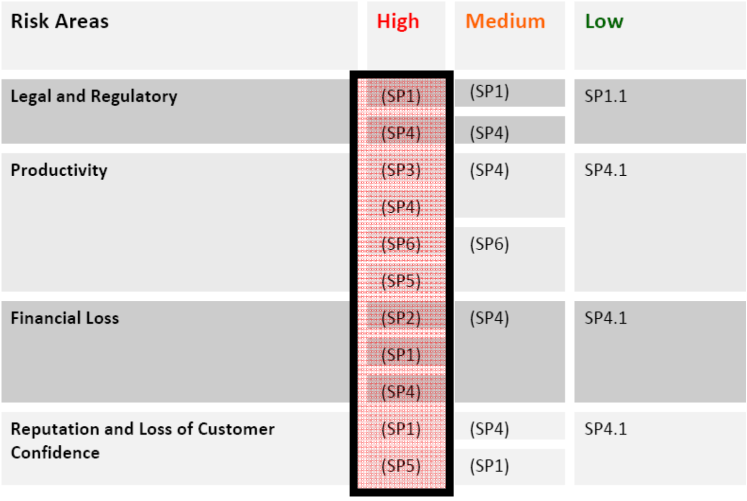
a. Organisational Controls

From the risk profile and asset identification processes above we can now select the appropriate controls that Pilot 1 need to apply in order to mitigate respective risks to their organisation. There are six possible control cards for the organisation as a whole:



Controls Category	Control No.	Name of the control
Organisational	**SP1**	Security Awareness and Training
	SP2	Security Strategy
	SP3	Security Management
	SP4	Security Policies and Regulations
	SP5	Collaborative Security Management
	SP6	Contingency Planning/Disaster Recovery

From the risk profile analysis above, we can see that Pilot 1 are classified as a high risk organisation for all four risk areas. The control cards that need to be applied are therefore as follows:

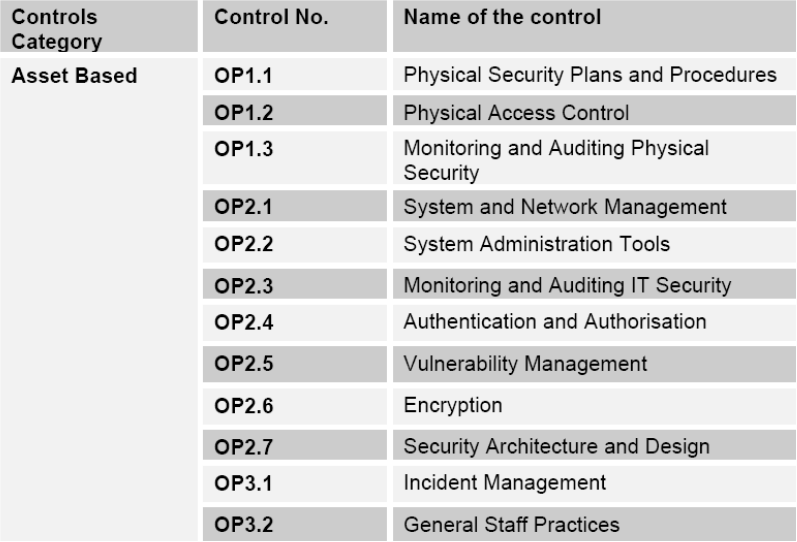


Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Productivity	(SP3) (SP4) (SP6) (SP5)	(SP4) (SP6)	SP4.1
Financial Loss	(SP2) (SP1) (SP4)	(SP4)	SP4.1
Reputation and Loss of Customer Confidence	(SP1) (SP5)	(SP4) (SP1)	SP4.1

This means that SP1, SP2, SP3, SP4, SP5 and SP6 need to be applied to Pilot 1.

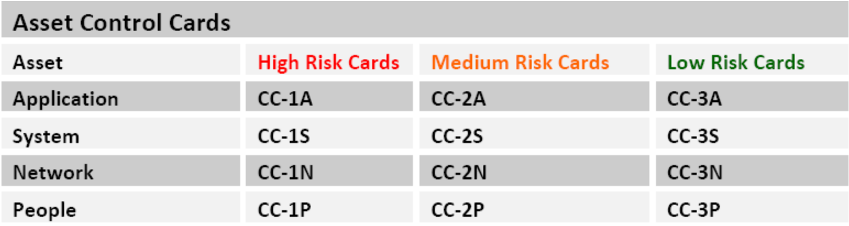
b. Asset Based Controls

There are twelve different asset based controls that can be used.



Controls Category	Control No.	Name of the control
Asset Based	OP1.1	Physical Security Plans and Procedures
	OP1.2	Physical Access Control
	OP1.3	Monitoring and Auditing Physical Security
	OP2.1	System and Network Management
	OP2.2	System Administration Tools
	OP2.3	Monitoring and Auditing IT Security
	OP2.4	Authentication and Authorisation
	OP2.5	Vulnerability Management
	OP2.6	Encryption
	OP2.7	Security Architecture and Design
	OP3.1	Incident Management
	OP3.2	General Staff Practices

The controls for each asset are decided based upon the risk level of the organisation and the type of asset concerned.



Asset Control Cards			
Asset	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

As previously identified – Pilot 1 are a high risk organisation. From our identification of assets and risk levels the following controls need to be applied:

Asset	Asset Category	Control Card Used
Data Storage	System	CC-1S
Archiving and Backup	System	CC-1S
Qualified Staff	People	CC-1P
IT Staff	People	CC-1P
Citrix Servers	System	CC-1S
Laptops	System	CC-1S
Key Applications	Application	CC-1A

6. Risk Management and Implementation

The following pages list the various controls required by Pilot 1.

Each individual control has been reviewed by Pilot 1 to identify whether they believe they are complying with that control.

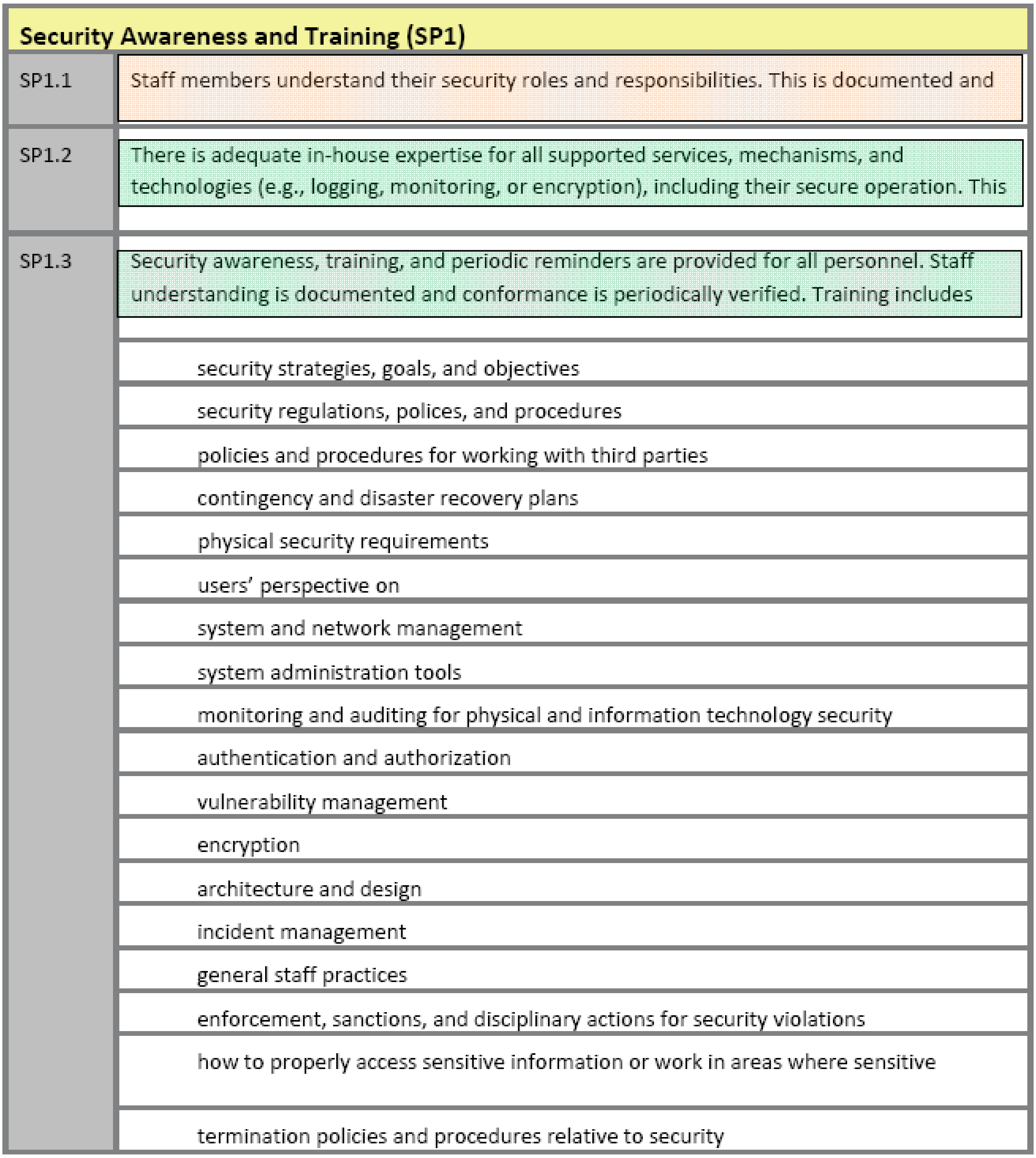
Those highlighted in Green show that they believe they are currently complying.

Those highlighted in Orange show that there is a system in place, but that this needs to be reviewed and possibly updated.

Those highlighted in red show that they currently do not comply.

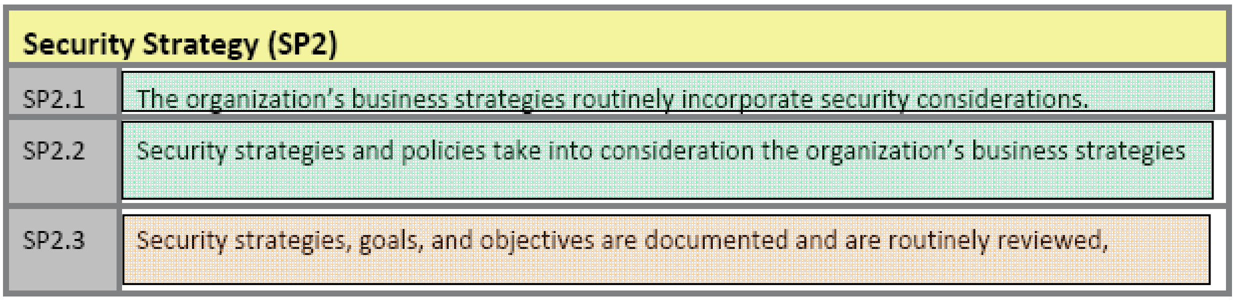
This gap analysis is based entirely on the responses given by Pilot 1. No verification of these responses has been carried out by PEM IT Services. If the client wishes, PEM IT Services can undertake a separate full review of the existing controls and policies. This is outside the scope of this review.

Security Awareness and Training (SP1)



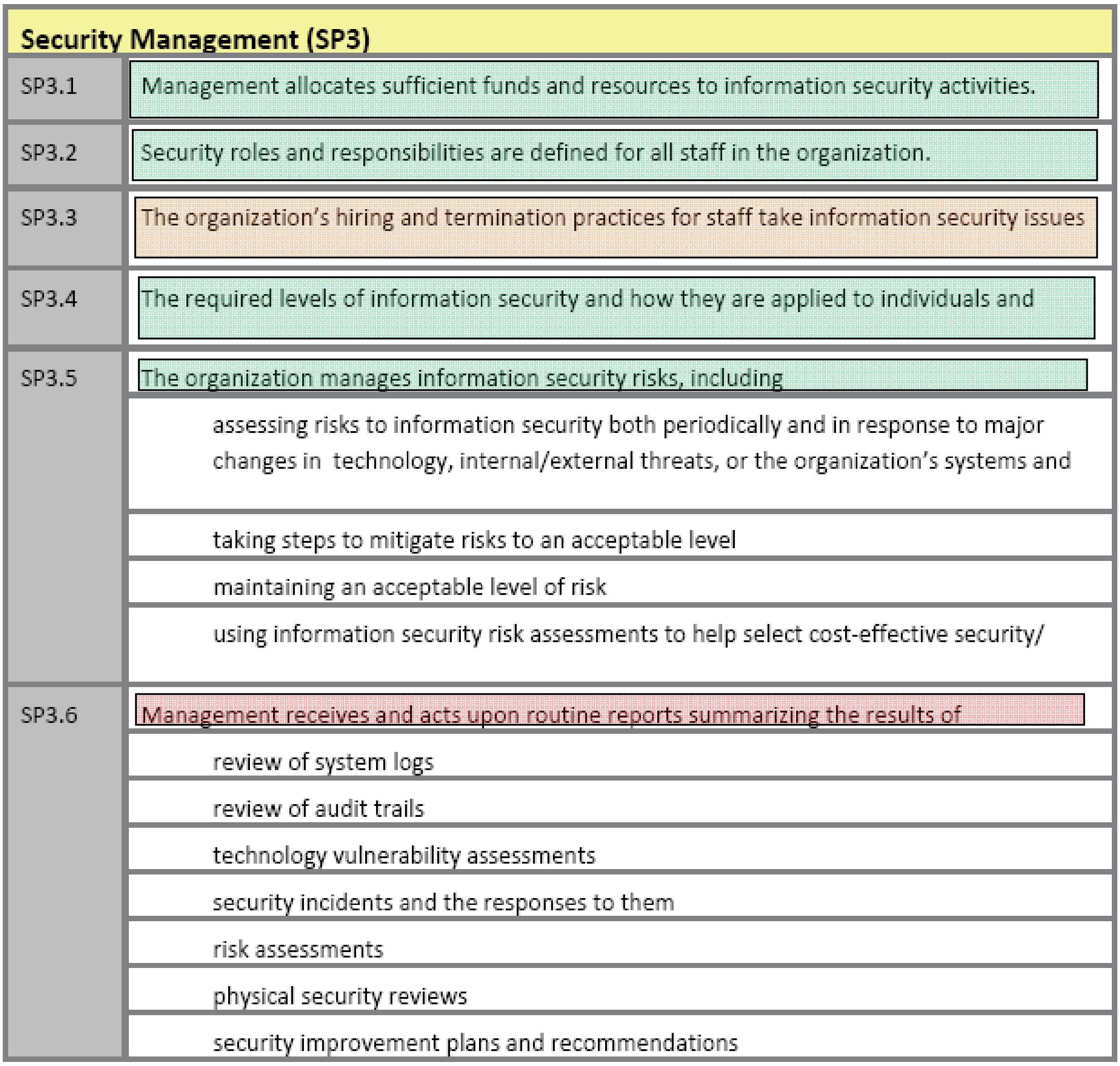
Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and
SP1.2	There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This
SP1.3	Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes
	security strategies, goals, and objectives
	security regulations, polices, and procedures
	policies and procedures for working with third parties
	contingency and disaster recovery plans
	physical security requirements
	users' perspective on
	system and network management
	system administration tools
	monitoring and auditing for physical and information technology security
	authentication and authorization
	vulnerability management
	encryption
	architecture and design
	incident management
	general staff practices
	enforcement, sanctions, and disciplinary actions for security violations
	how to properly access sensitive information or work in areas where sensitive
	termination policies and procedures relative to security

Security Strategy (SP2)



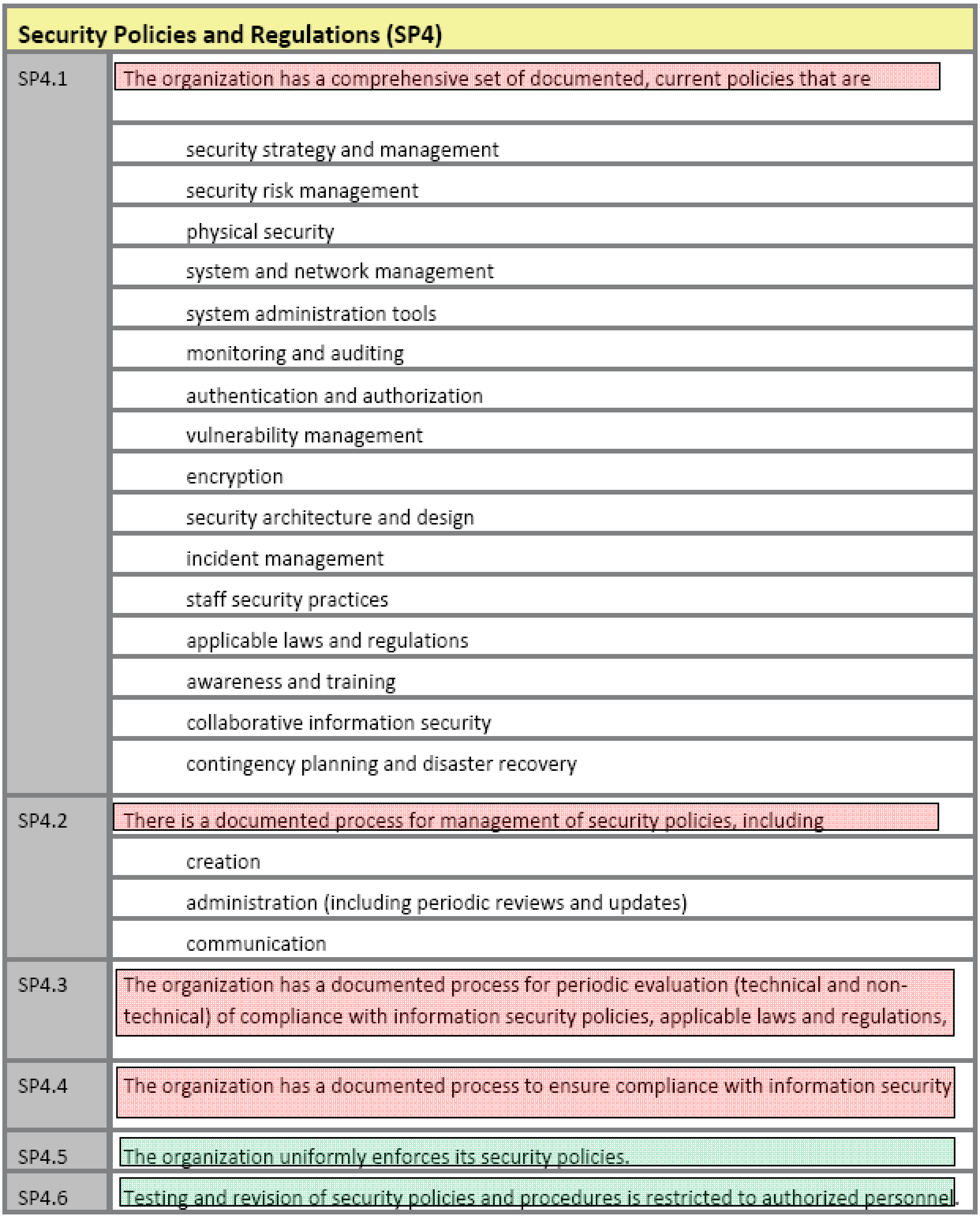
Security Strategy (SP2)	
SP2.1	The organization's business strategies routinely incorporate security considerations.
SP2.2	Security strategies and policies take into consideration the organization's business strategies
SP2.3	Security strategies, goals, and objectives are documented and are routinely reviewed,

Security Management (SP3)



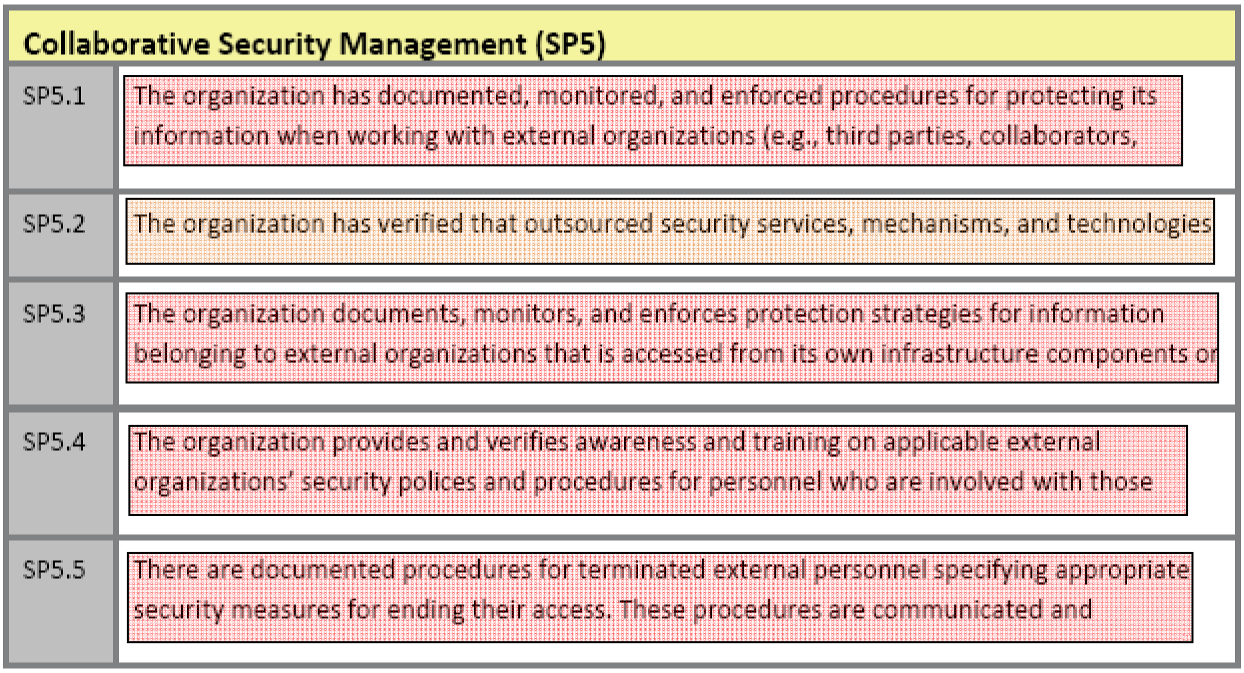
Security Management (SP3)	
SP3.1	Management allocates sufficient funds and resources to information security activities.
SP3.2	Security roles and responsibilities are defined for all staff in the organization.
SP3.3	The organization's hiring and termination practices for staff take information security issues
SP3.4	The required levels of information security and how they are applied to individuals and
SP3.5	The organization manages information security risks, including
	assessing risks to information security both periodically and in response to major changes in technology, internal/external threats, or the organization's systems and
	taking steps to mitigate risks to an acceptable level
	maintaining an acceptable level of risk
	using information security risk assessments to help select cost-effective security/
SP3.6	Management receives and acts upon routine reports summarizing the results of
	review of system logs
	review of audit trails
	technology vulnerability assessments
	security incidents and the responses to them
	risk assessments
	physical security reviews
	security improvement plans and recommendations

Security Policies and Regulations (SP4)



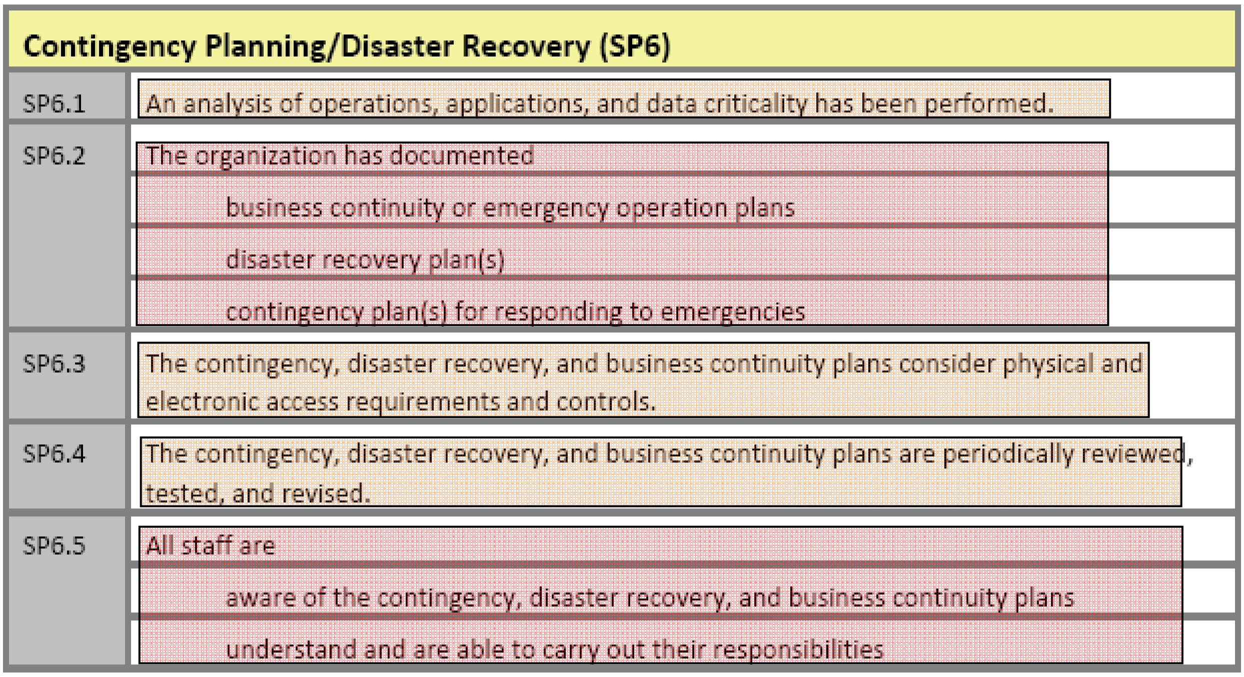
Security Policies and Regulations (SP4)	
SP4.1	The organization has a comprehensive set of documented, current policies that are
	security strategy and management
	security risk management
	physical security
	system and network management
	system administration tools
	monitoring and auditing
	authentication and authorization
	vulnerability management
	encryption
	security architecture and design
	incident management
	staff security practices
	applicable laws and regulations
	awareness and training
	collaborative information security
	contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including
	creation
	administration (including periodic reviews and updates)
	communication
SP4.3	The organization has a documented process for periodic evaluation (technical and non-technical) of compliance with information security policies, applicable laws and regulations,
SP4.4	The organization has a documented process to ensure compliance with information security
SP4.5	The organization uniformly enforces its security policies.
SP4.6	Testing and revision of security policies and procedures is restricted to authorized personnel.

Collaborative Security Management (SP5)



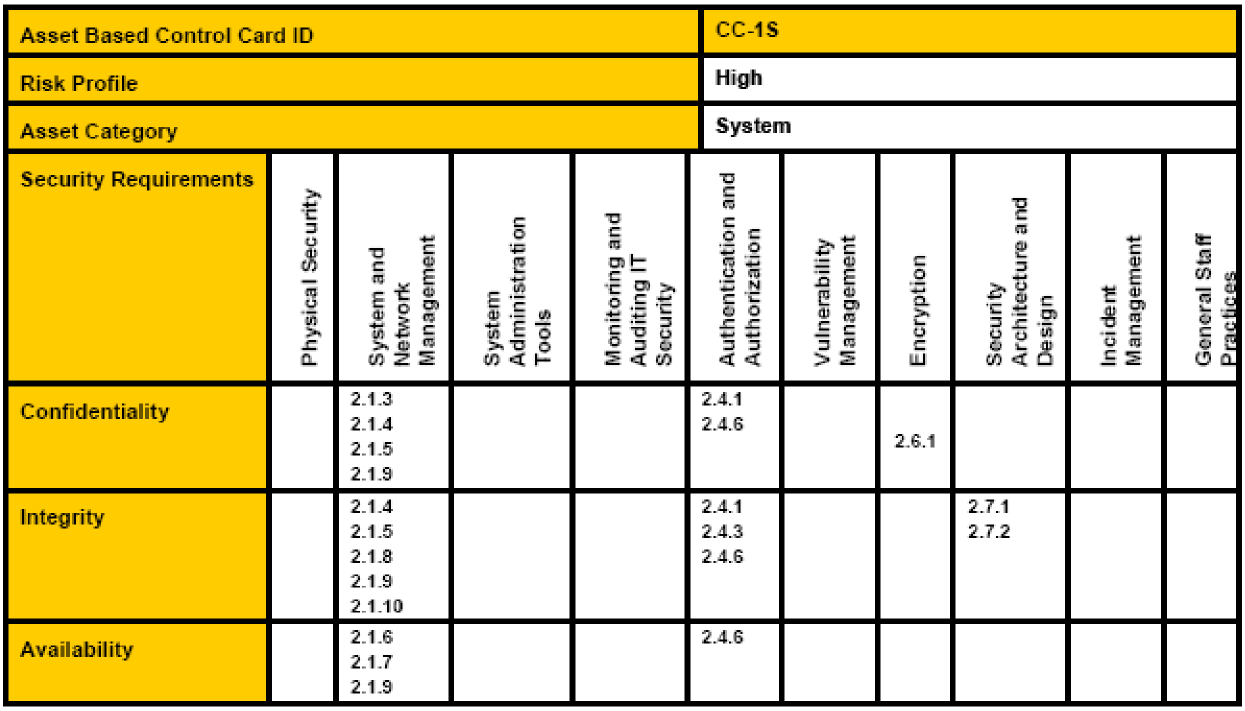
Collaborative Security Management (SP5)	
SP5.1	The organization has documented, monitored, and enforced procedures for protecting its information when working with external organizations (e.g., third parties, collaborators,
SP5.2	The organization has verified that outsourced security services, mechanisms, and technologies
SP5.3	The organization documents, monitors, and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or
SP5.4	The organization provides and verifies awareness and training on applicable external organizations' security polices and procedures for personnel who are involved with those
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access. These procedures are communicated and

Contingency Planning/Disaster Recovery (SF



Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented
	business continuity or emergency operation plans
	disaster recovery plan(s)
	contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are
	aware of the contingency, disaster recovery, and business continuity plans
	understand and are able to carry out their responsibilities

System Asset – Data storage



Asset Based Control Card ID	CC-1S
Risk Profile	High
Asset Category	System

Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

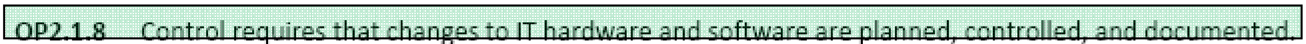
OP2.1.4 Control requires that the integrity of installed software is regularly verified.

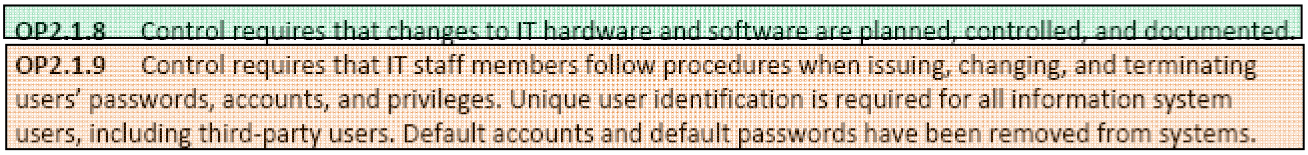
OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

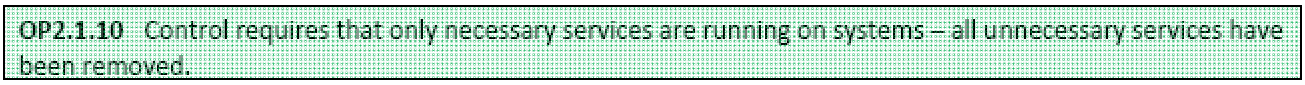
OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

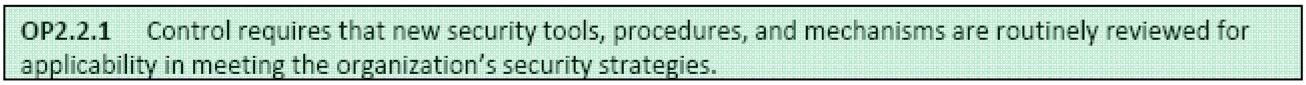
OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

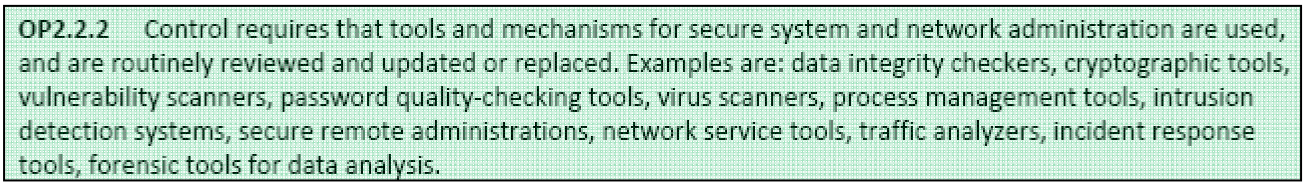
System Asset – Data storage (continued)

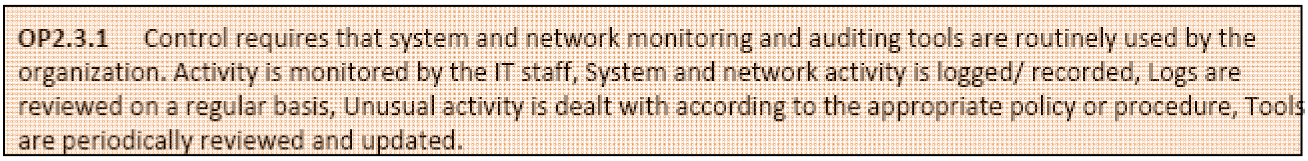

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented.

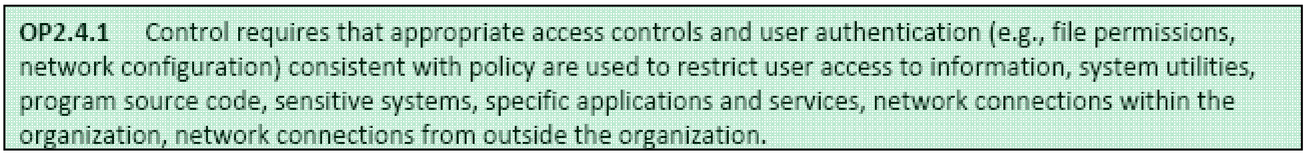

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

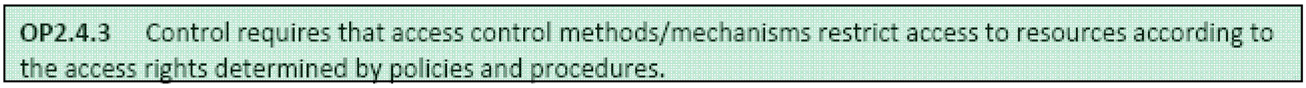

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

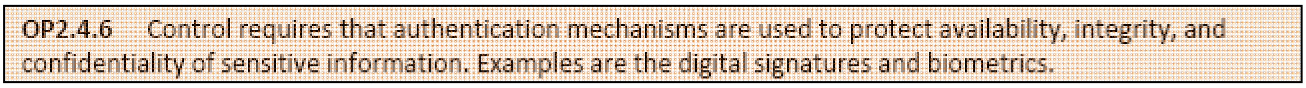

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

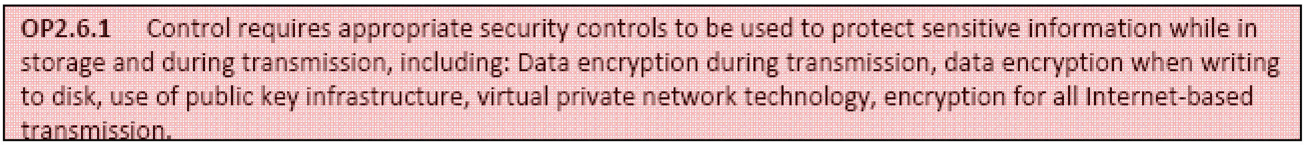

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

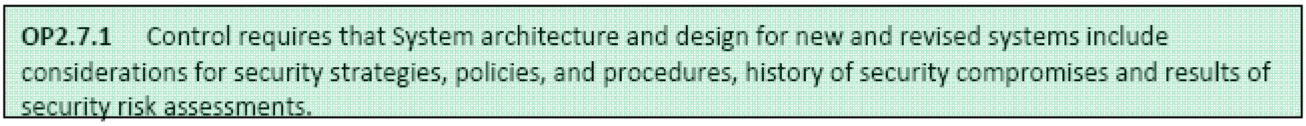

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

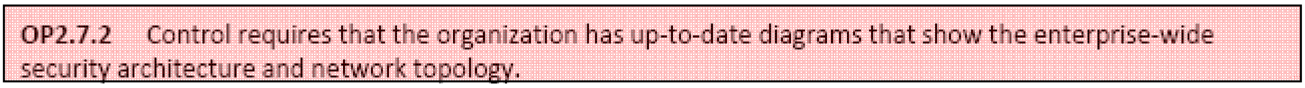

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.


OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

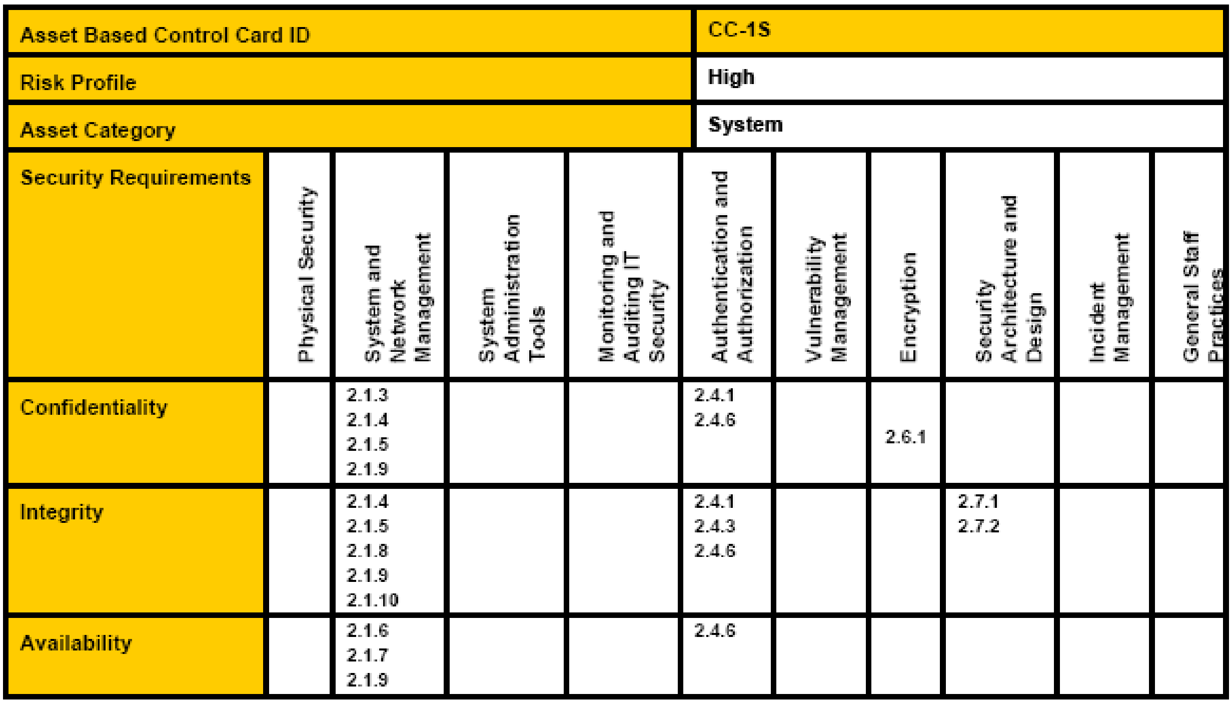

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.


OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.


OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.


OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

System Asset – Archiving and Backup



Asset Based Control Card ID	CC-1S									
Risk Profile	High									
Asset Category	System									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

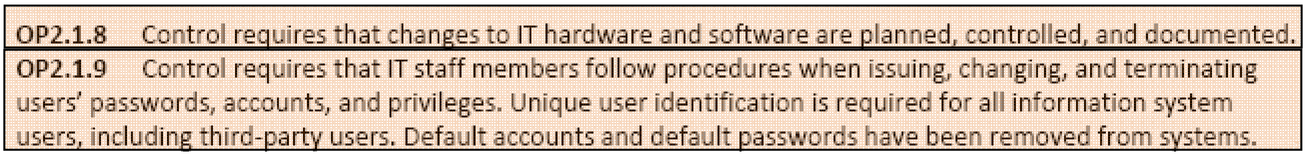
OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

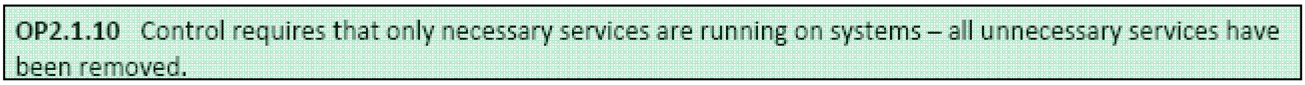
OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

System Asset – Archiving and Backup (continued)

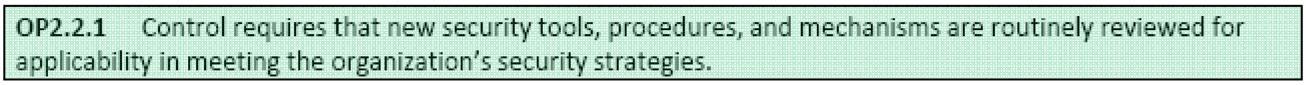


OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented.

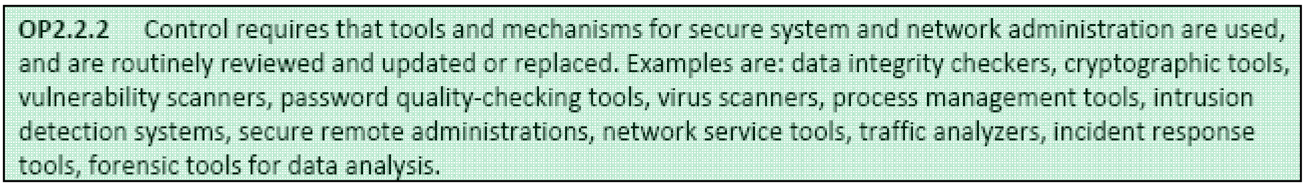
OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.



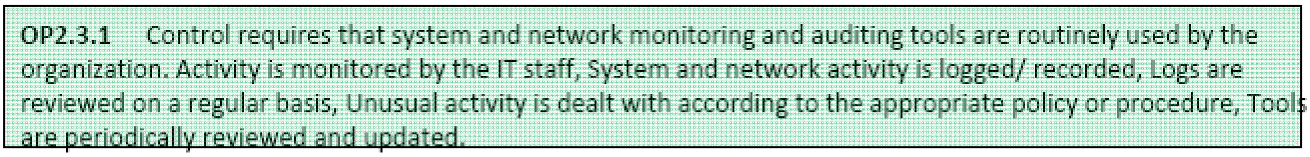
OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.



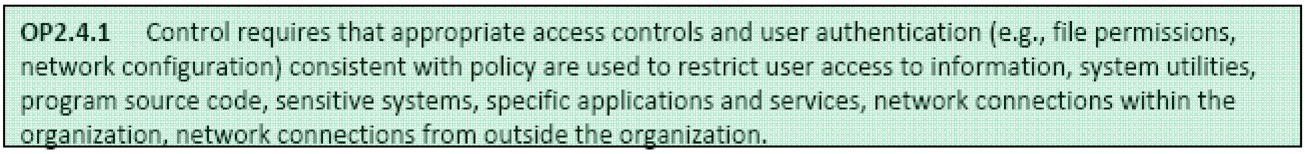
OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.



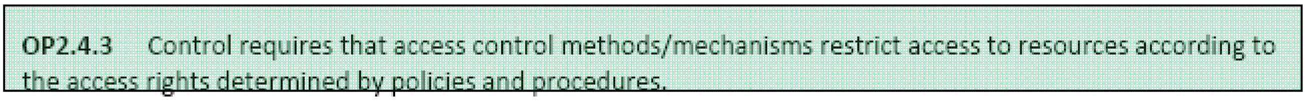
OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.



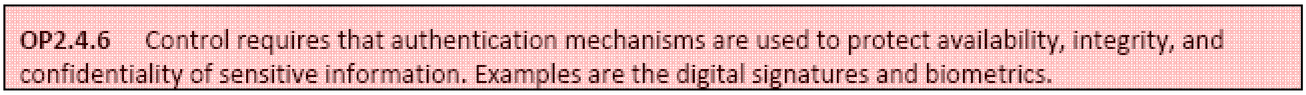
OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.



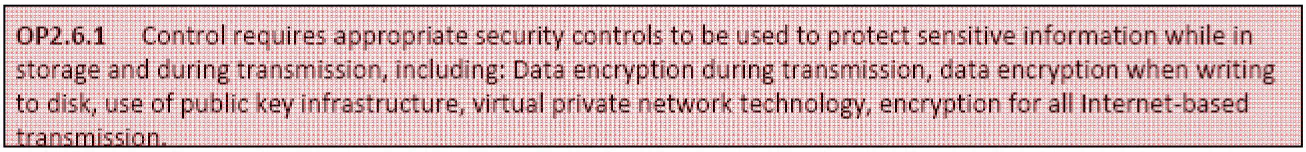
OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.



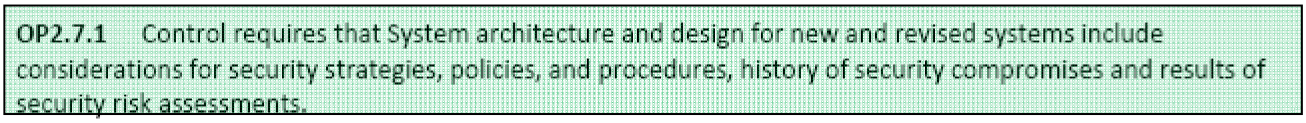
OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.



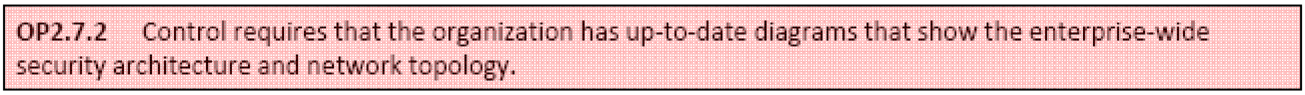
OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.



OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.



OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.



OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

People Asset – Qualified Staff

Asset Based Control Card ID	CC-1P									
Risk Profile	High									
Asset Category	People									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										3.2.1 3.2.2 3.2.3
Integrity	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Availability										

A high risk profile implies threats that occur in management of people and in human resources in general. The level of staff commitment on using the appropriate security controls on network resources determines level of protection that can be achieved.

The manipulation of information and the reuse of older records with high value for the organization is a critical aspect. Internal or confidential information from staff should be treated respectfully. Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP3.2.3 Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

OP1.3.2 Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for.

People Asset – IT Staff

Asset Based Control Card ID	CC-1P									
Risk Profile	High									
Asset Category	People									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										3.2.1 3.2.2 3.2.3
Integrity	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Availability										

A high risk profile implies threats that occur in management of people and in human resources in general. The level of staff commitment on using the appropriate security controls on network resources determines level of protection that can be achieved.

The manipulation of information and the reuse of older records with high value for the organization is a critical aspect. Internal or confidential information from staff should be treated respectfully. Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

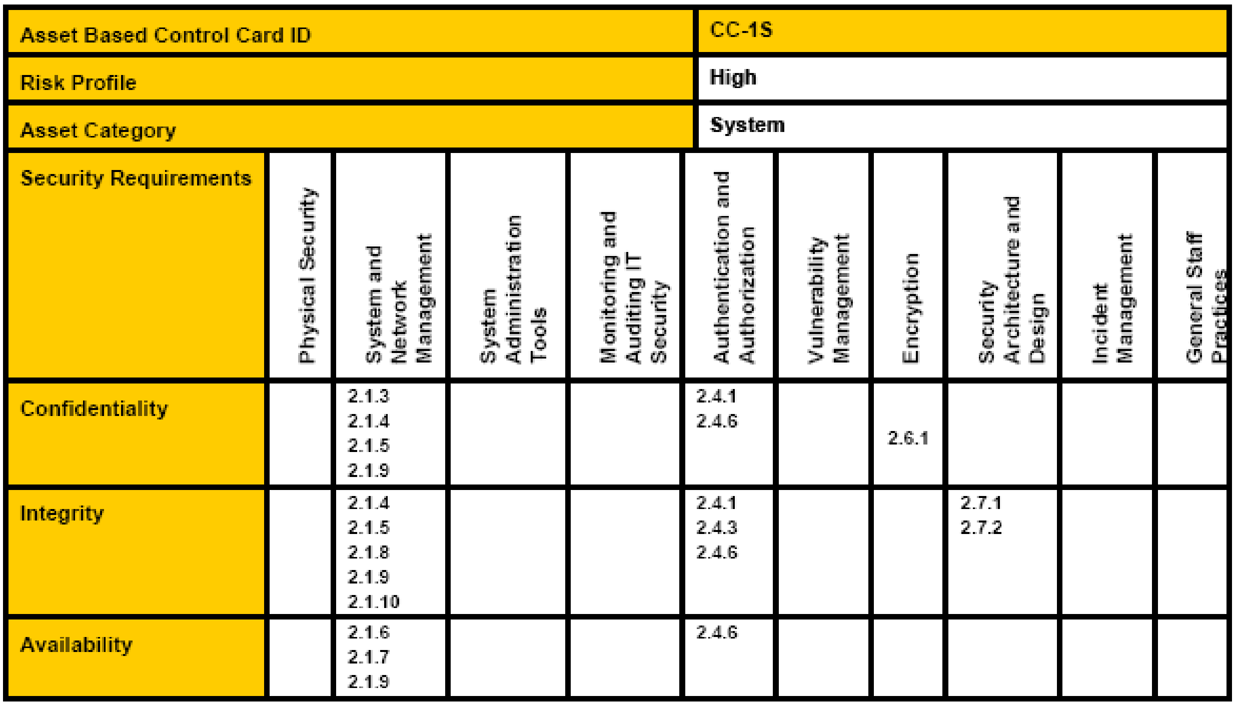
OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP3.2.3 Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

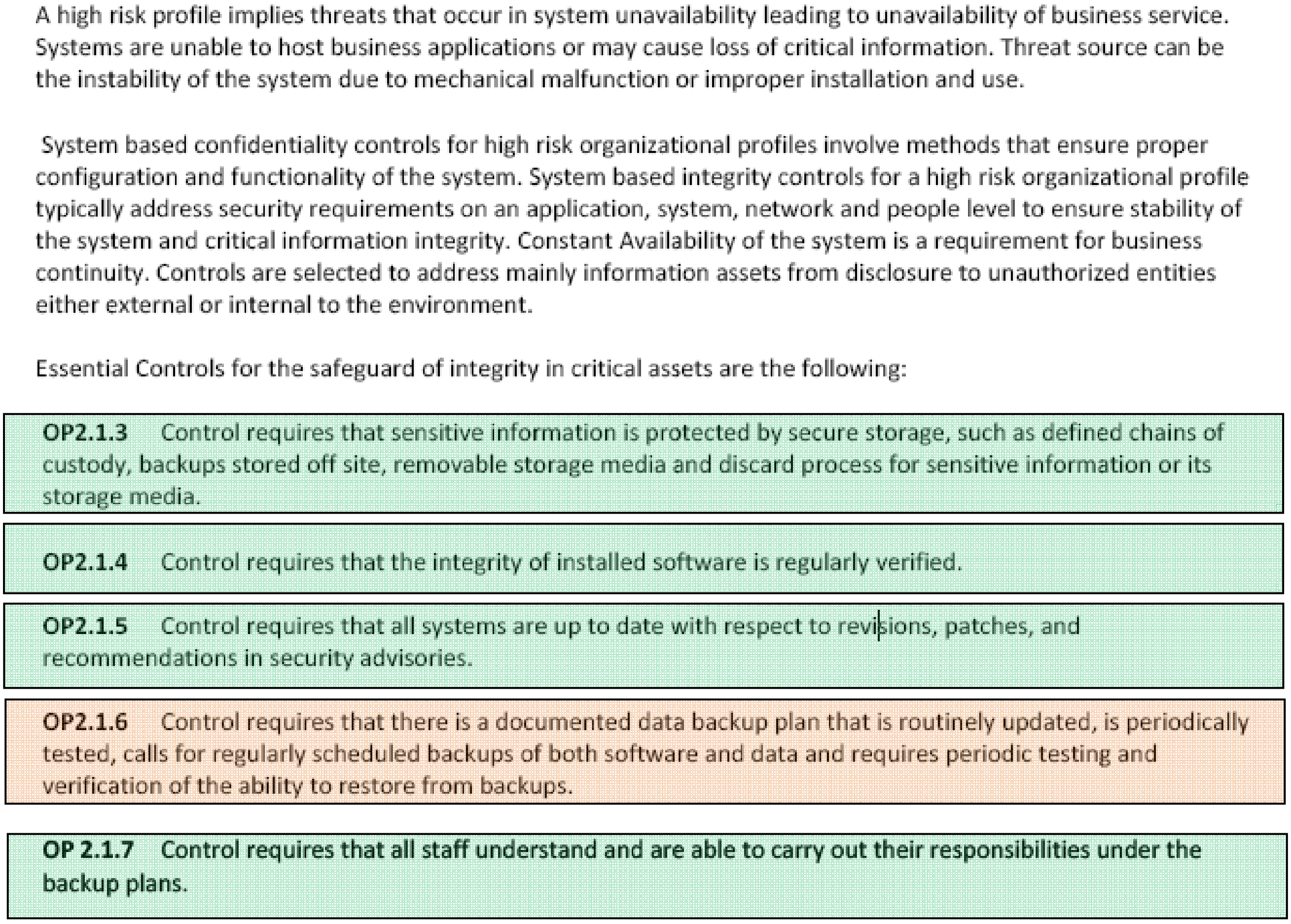
OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

OP1.3.2 Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for.

System Asset – Citrix Servers



Asset Based Control Card ID	CC-1S									
Risk Profile	High									
Asset Category	System									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					



A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

System Asset – Citrix Servers (continued)

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

System Asset – Laptops

Asset Based Control Card ID	CC-1S									
Risk Profile	High									
Asset Category	System									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

System Asset – Laptops (continued)

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

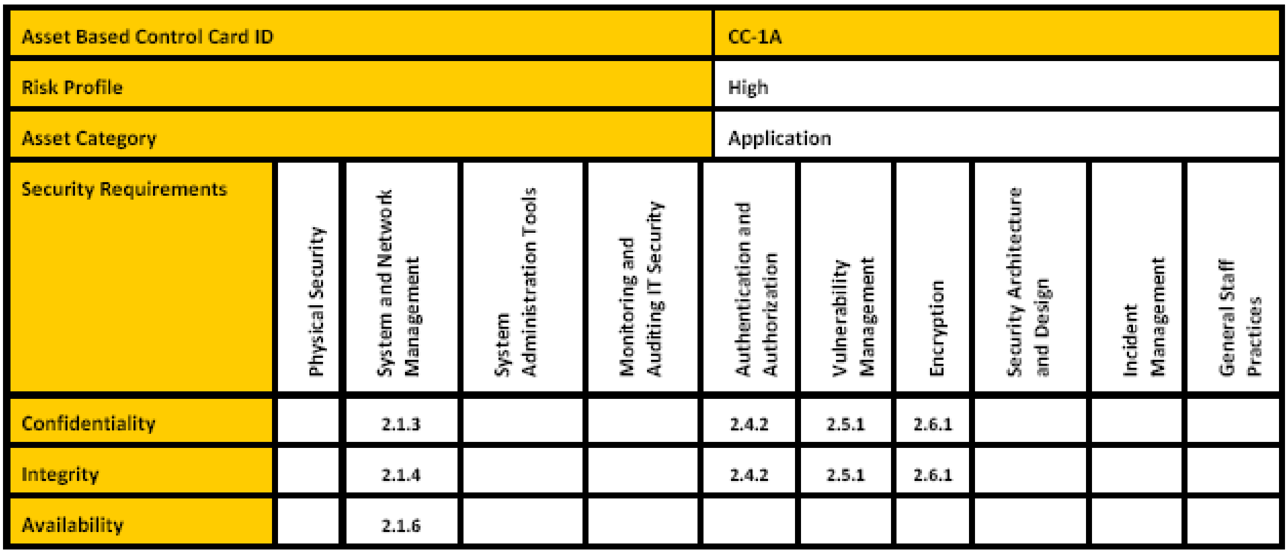
OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

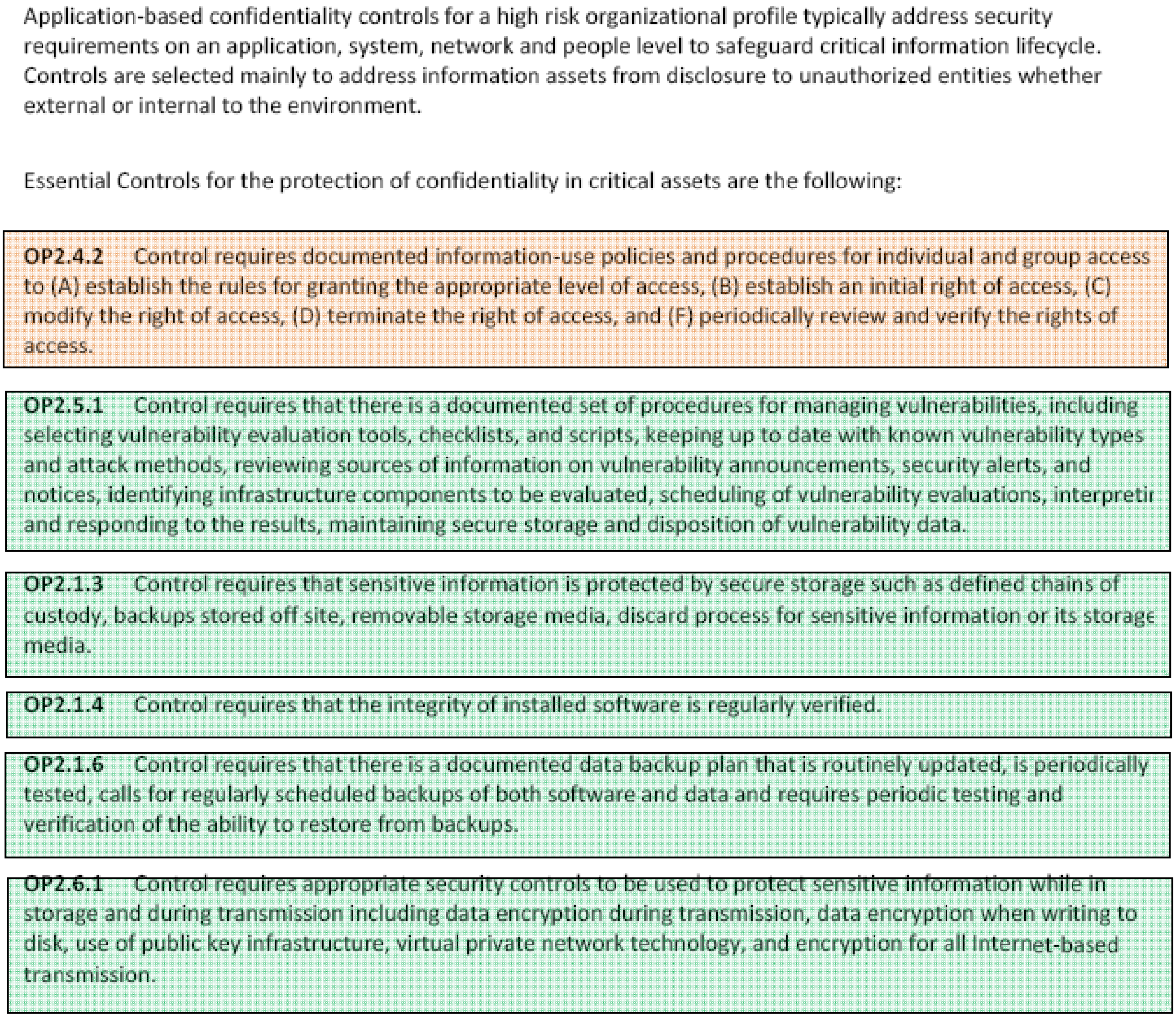
OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Application Asset – MYOB Central



Asset Based Control Card ID					CC-1A					
Risk Profile					High					
Asset Category					Application					
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								



Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpretir and responding to the results, maintaining secure storage and disposition of vulnerability data.

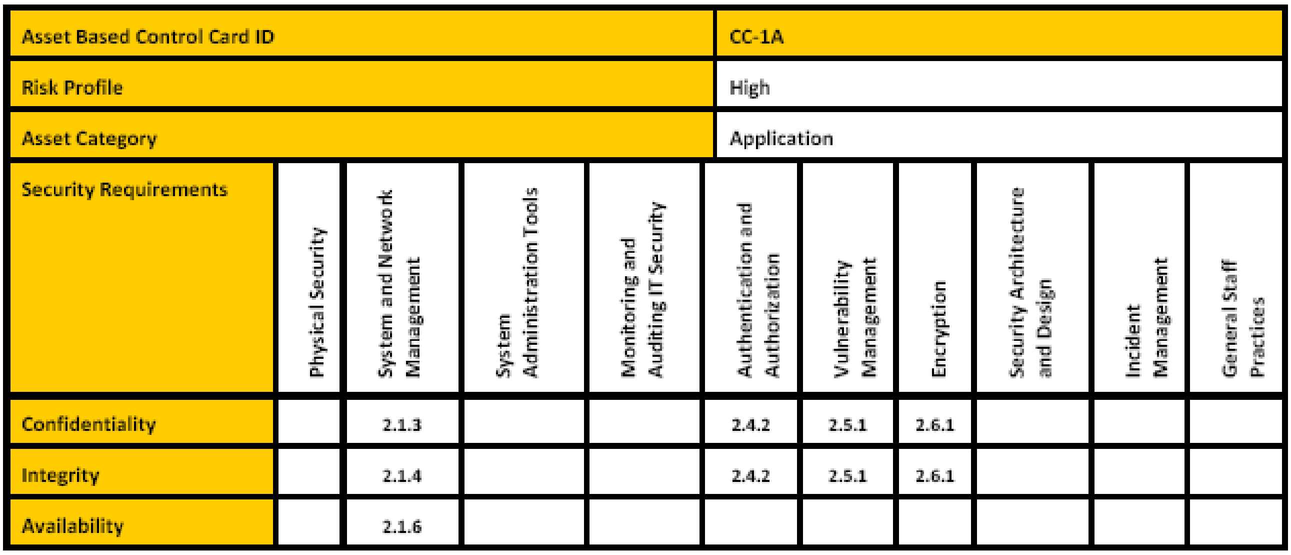
OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

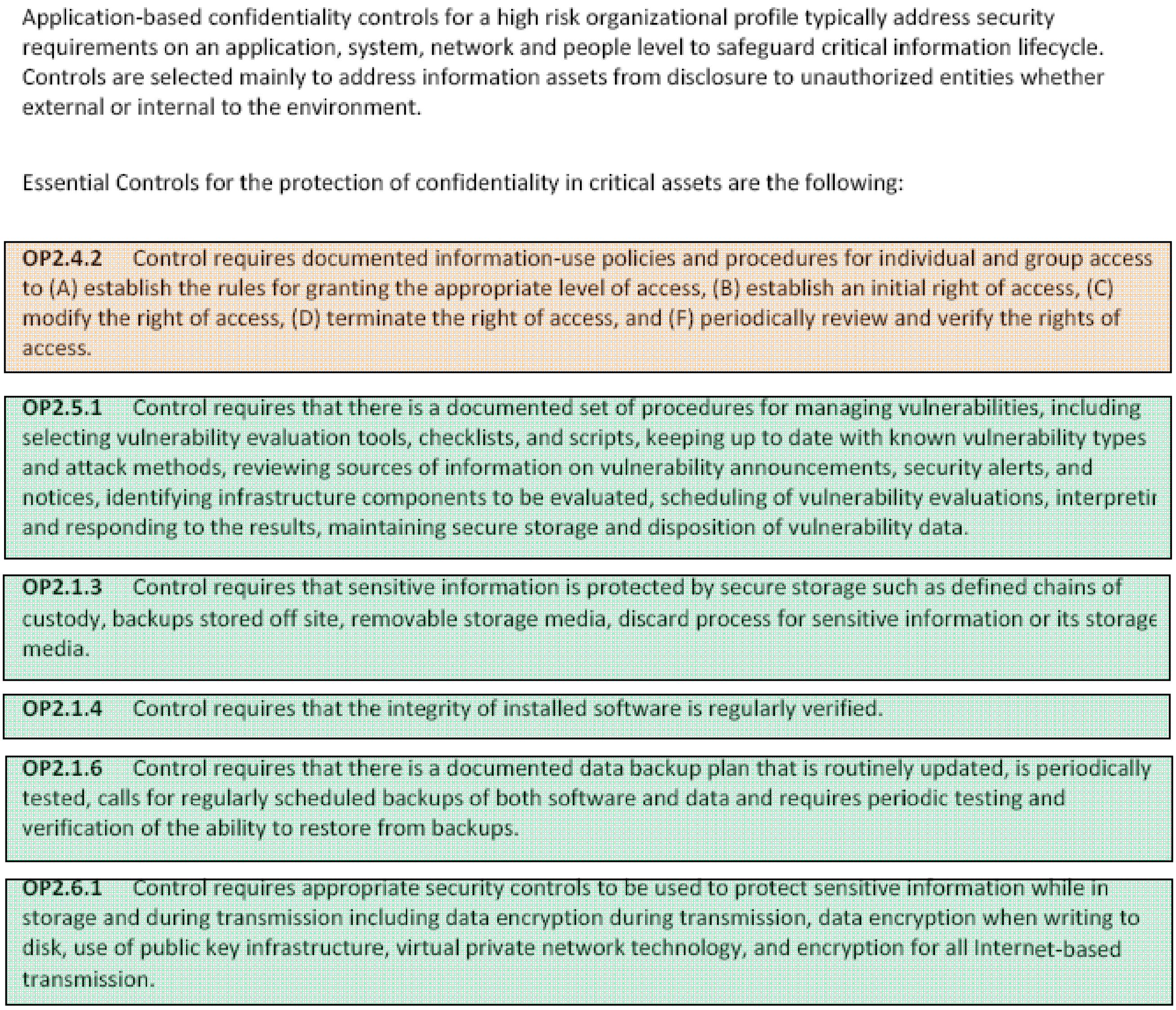
OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

Application Asset – MYOB Pertax



Asset Based Control Card ID	CC-1A
Risk Profile	High
Asset Category	Application

Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								



Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpretir and responding to the results, maintaining secure storage and disposition of vulnerability data.

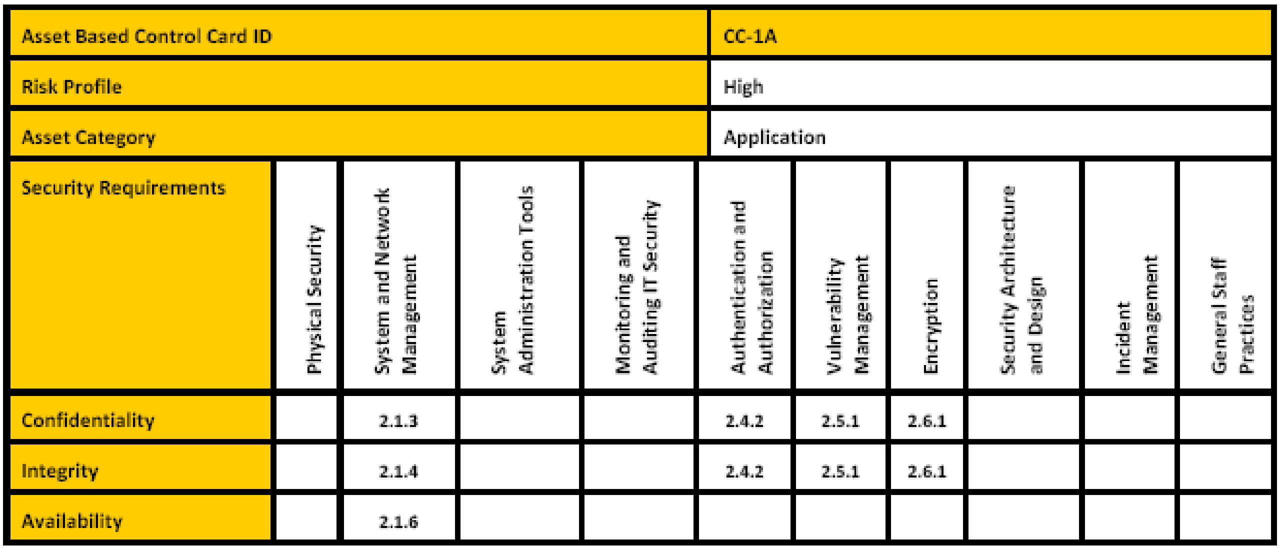
OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

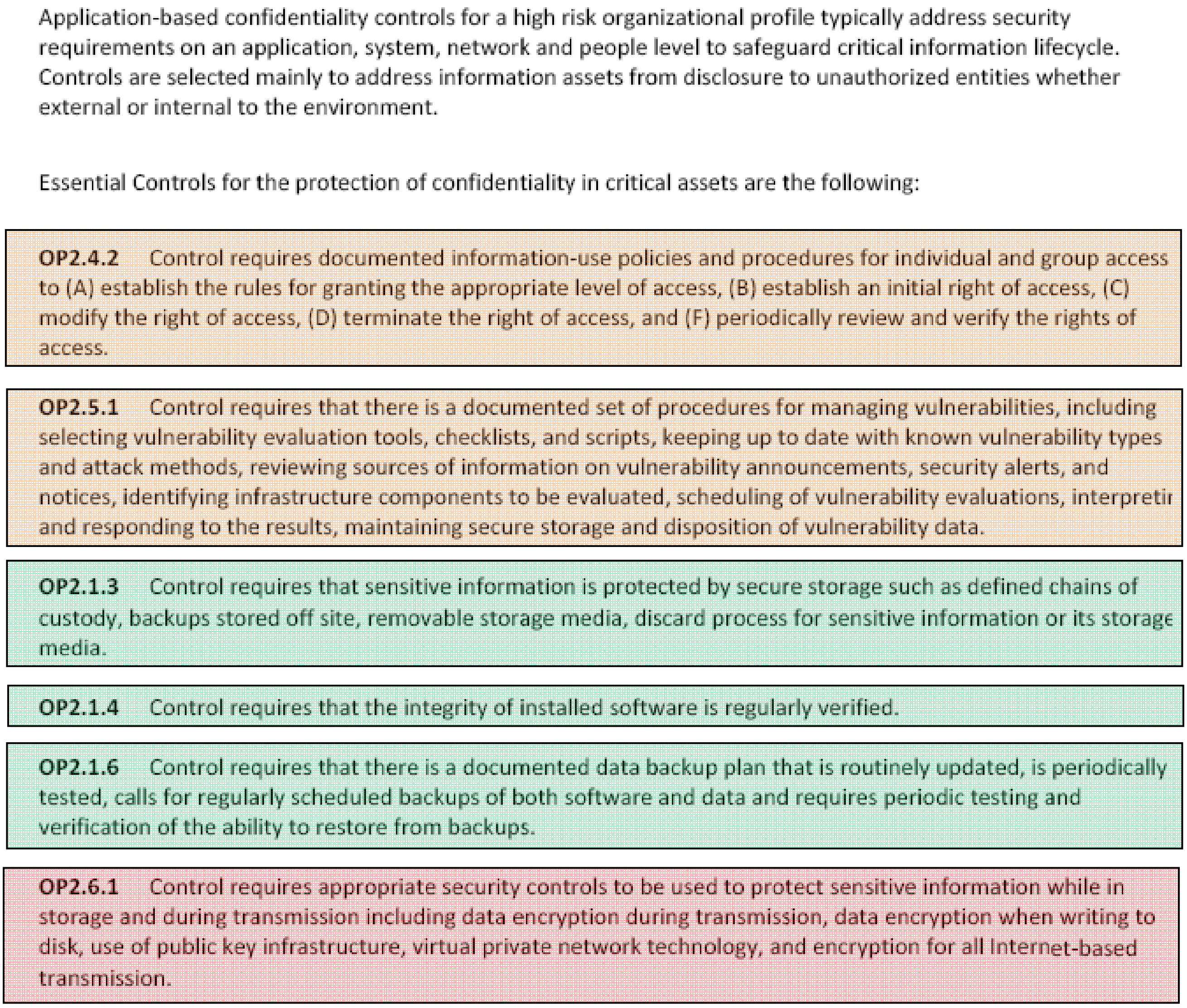
OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

Application Asset – Caseware Audit



Asset Based Control Card ID	CC-1A										
Risk Profile	High										
Asset Category	Application										
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								



Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpretir and responding to the results, maintaining secure storage and disposition of vulnerability data.

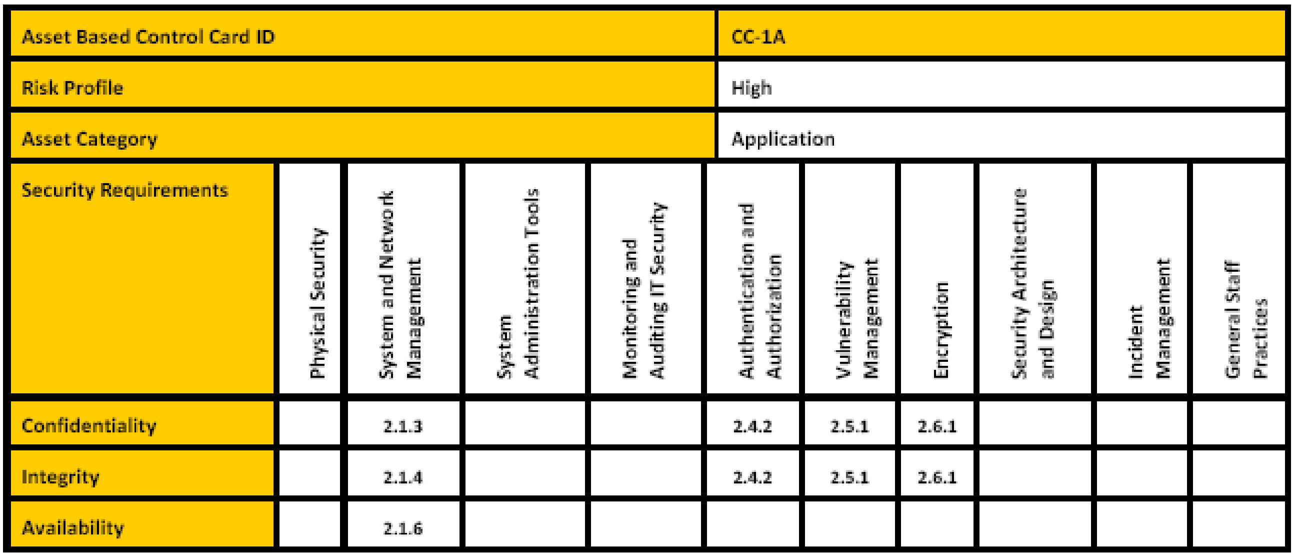
OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

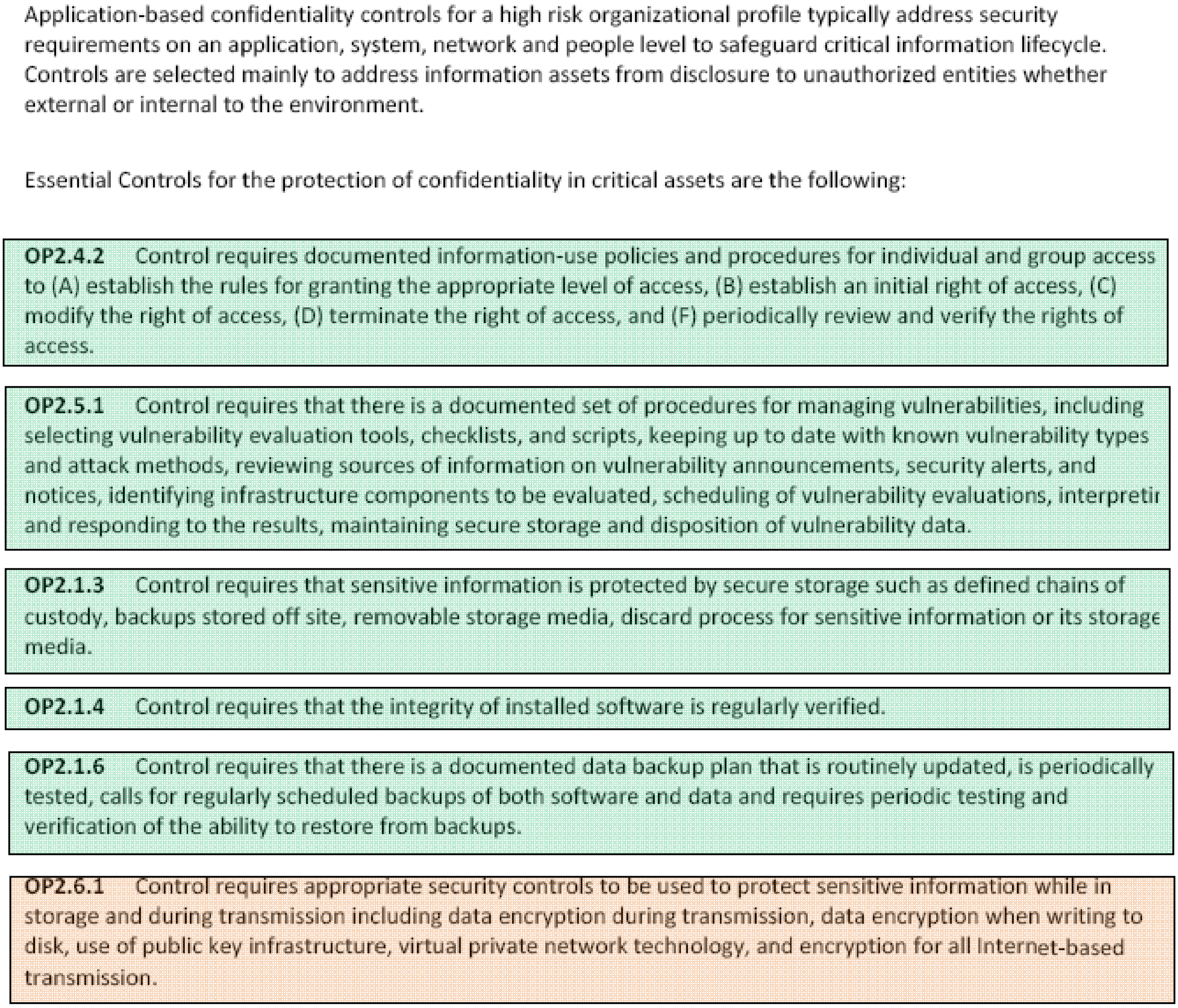
OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

Application Asset – Star Payroll Professional



Asset Based Control Card ID	CC-1A									
Risk Profile	High									
Asset Category	Application									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								



Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpretir and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

7. Summary of findings

Peters Elworthy and Moore are a high risk organisation with regard to information security, because of type of information they hold and the businesses high reliance on the availability and accuracy of this data.

This review has highlighted a number of areas for action by Peters Elworthy and Moore to minimise the risks associated with Information Security in their organisation. Whilst they have already put in place a number of steps to mitigate the risks there remain several areas that should be addressed, including:

- Documenting the current security procedures and policies, and making these available to all staff.
- Documenting the procedures and policies relating to access by third parties.
- Documenting the process for review of compliance with security policies.
- Implementing and documenting a full Disaster Recovery plan, and making this information available to all staff.
- Set up the protection of data when transmitted off-site, including when used on laptops and other portable devices.
- Set up appropriate protection of backup devices to avoid unauthorised access.
- Document the current security topology, and implement appropriate change procedures.

In order to reduce the business risks from information security it is recommended that Pilot 1 look to address these gaps as a matter of urgency. Furthermore, once these have been addressed it is recommended that the system is reviewed at regular intervals in the future to ensure that the risks continue to be minimised.

As identified at the start of this review, Pilot 1 intend to carry out the future reviews in-house using their own staff. It is recommended that such checks are carried out by those who do not have a direct responsibility for establishing and maintaining the policies. This will ensure that any checks are objective.

PEM IT Services

A division of Peters Elworthy & Moore

Salisbury House
Station Road
Cambridge
CB1 2LA

Email: it@pem.co.uk
Tel: 01223 728222
Fax: 01223 461424
www.pemit.co.uk

Risk Management Review

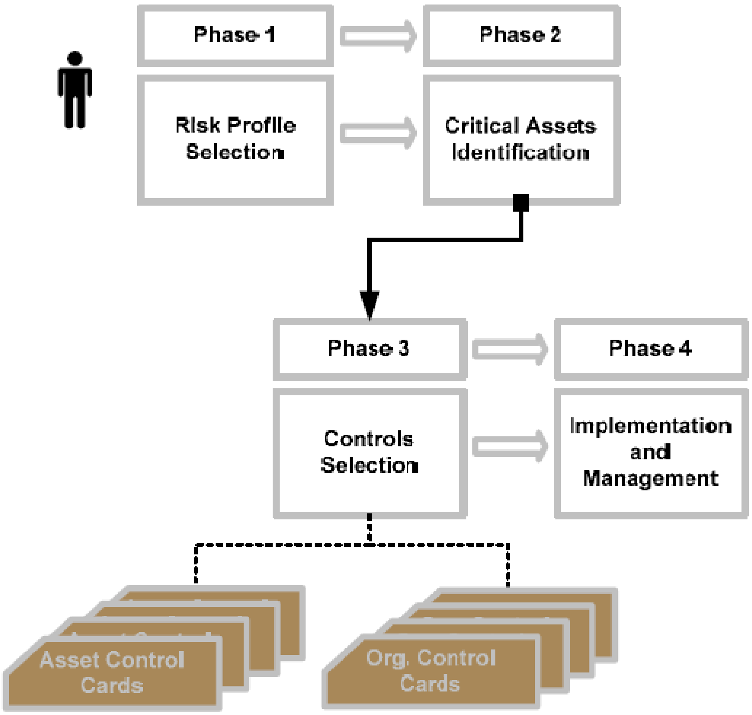
A review
for the
Pilot 2

Proposal of IT Services

This document is a review of the Risk Management and IT Security requirements for Pilot 2.

Contents

1. Objective of this review



Part of the responsibility of MSB Managers is to provide for the security of their business environment. According to most applicable legal requirements, liability for breaches of security lies with them.

Just as they must provide a safe and secure physical environment, they must also make sure that information is protected. Given the fact, however, that computers are not “fix and forget” devices, the protection of information is a permanent concern.

This review provides an overview of the key information security risks for the organisation. It then provides a gap analysis to show the areas which are currently covered by internal procedures and policies, and highlights the areas that still need to be addressed or re-visited.

2. Who should carry out this review?

There are three alternative ways in which this review can be approached:

- In-sourcing of risk assessment – all reviews carried out by in-house staff.
- Partial outsourcing of risk assessment –initial review done by external advisor, then ongoing reviews carried out internally.
- Full outsourcing of risk assessment – entire review process is carries out by an external contractor.

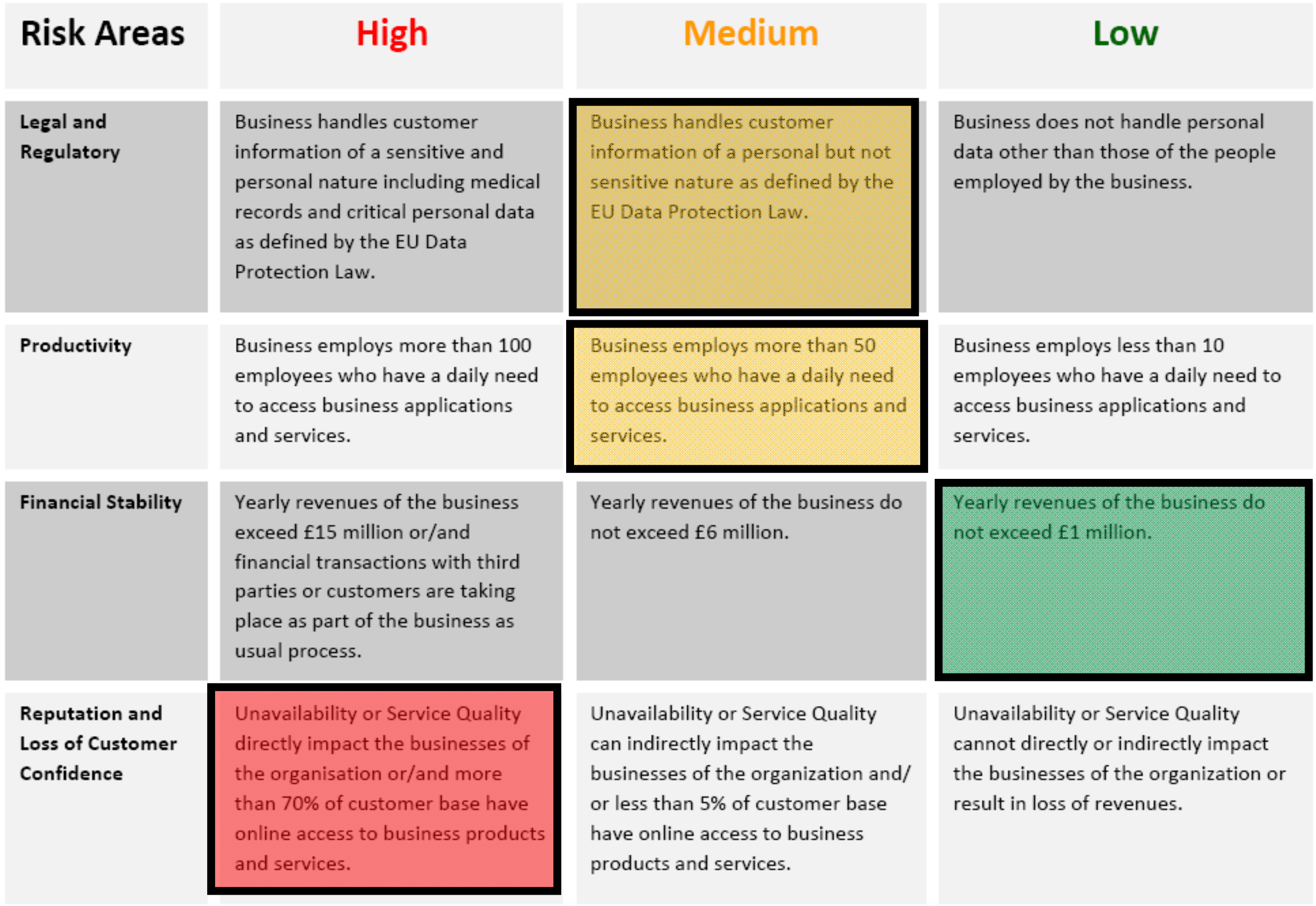
Having considered the guidelines from ENISA, PILOT 2 would probably have decided to try to carry out the review in-house. This is based on the following criteria:

- The organisation is under 15 employees, and has a relatively simple IT infrastructure.
- The organisation has some time and resources to allocate to the project, although not the three to five people suggested in the guidance.
- PILOT 2 are not sure if they have the correct skills to complete the review in-house, but would call on external assistance as and when required.

For the purposes of this trial, PILOT 2 agreed for PEM IT Services to carry out the review on their behalf.

3. Risk Profile Analysis

The organisation's risk profile has been considered from four separate angles, to identify the level of risk the organisation places on its information security.



Risk Areas	High	Medium	Low
Legal and Regulatory	Business handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	Business handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	Business does not handle personal data other than those of the people employed by the business.
Productivity	Business employs more than 100 employees who have a daily need to access business applications and services.	Business employs more than 50 employees who have a daily need to access business applications and services.	Business employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues of the business exceed £15 million or/and financial transactions with third parties or customers are taking place as part of the business as usual process.	Yearly revenues of the business do not exceed £6 million.	Yearly revenues of the business do not exceed £1 million.
Reputation and Loss of Customer Confidence	Unavailability or Service Quality directly impact the businesses of the organisation or/and more than 70% of customer base have online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/ or less than 5% of customer base have online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

PILOT 2 handle a large amount of personal information, including membership details and exam results. However, none of this is of a highly sensitive nature, therefore the Legal and Regulatory risk is MEDIUM.

PILOT 2 have a heavy reliance on access to their information to perform their daily work. This includes access to the membership database to process information and to allow members to make purchases. PILOT 2 have limited paper records, so much of the data is only held in electronic format. Therefore the risk to Productivity is MEDIUM.

PILOT 2 has an annual turnover under £1 Million. Financially any issues are likely to be an inconvenience rather than a major financial loss. Therefore the financial risk is LOW.

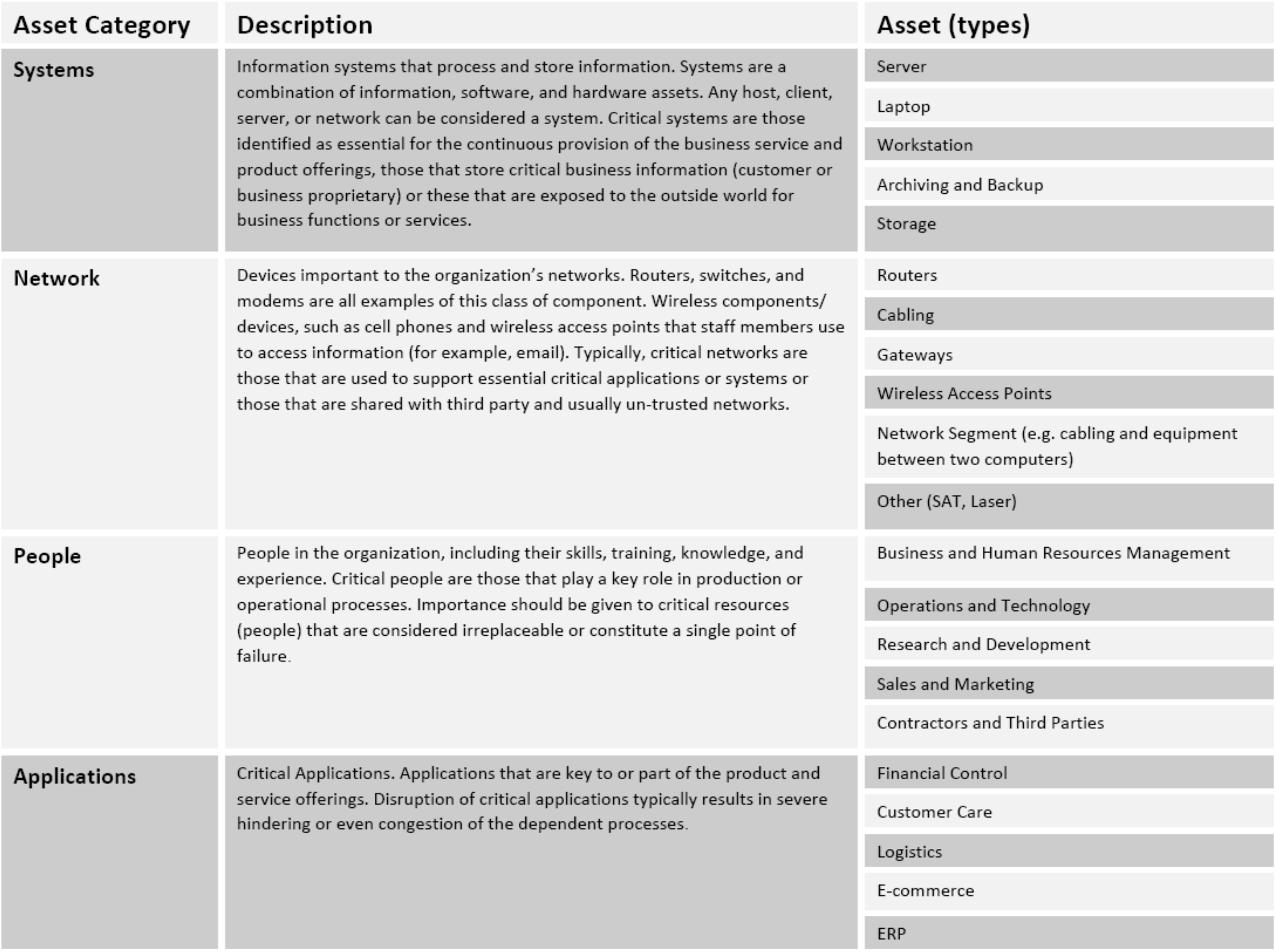
PILOT 2 are an information based organisation, and public perception is a key factor in the organisations success. This needs to be protected. PILOT 2 hold qualifications information for members, and access to this information is critical. It is also important that this information is accurate and reliable. Therefore the risk to reputation or loss of customer confidence is HIGH.

It is therefore established that the overall risk level for PILOT 2 is HIGH.

4. Identification of Critical Assets

It is important for the organisation to identify the key assets which the organisation has, from an information security perspective. These need to be identified on the basis of the adverse impact they are likely to have on the organisation in the event of the following:

- Disclosure of information to unauthorised people.
- Modification of information without authorisation.
- Loss or destruction of the asset.
- Interrupted access to the asset or information stored.



Asset Category	Description	Asset (types)
Systems	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information (customer or business proprietary) or these that are exposed to the outside world for business functions or services.	Server Laptop Workstation Archiving and Backup Storage
Network	Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of component. Wireless components/ devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with third party and usually un-trusted networks.	Routers Cabling Gateways Wireless Access Points Network Segment (e.g. cabling and equipment between two computers) Other (SAT, Laser)
People	People in the organization, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes. Importance should be given to critical resources (people) that are considered irreplaceable or constitute a single point of failure.	Business and Human Resources Management Operations and Technology Research and Development Sales and Marketing Contractors and Third Parties
Applications	Critical Applications. Applications that are key to or part of the product and service offerings. Disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.	Financial Control Customer Care Logistics E-commerce ERP

Based on the criteria above, the following assets have been identified as the most critical assets to NCTJ:

1. **Data server and storage**. PILOT 2 are an information business. The information they hold is important for the running of the organisation. If that data is lost completely there would be a major impact on the organisation. Therefore the servers holding this information are a critical asset.

2. **Archiving and Backup**. Should there be any loss of data from the server, it is critical to PILOT 2that the data can be recovered quickly with minimal loss.

3. **Workstations**. Staff at PILOT 2 use their workstations to access data on the network, and therefore management of these is important to the organisation

4. **Wireless Access Points.** These allow wireless enabled devices to access the PILOT 2office network.

5. **Third Party contractors**. PILOT 2 outsource their IT support to a third party. They also outsource the development of their membership database and the management of their web site. This means that PILOT 2is heavily reliant on these third parties for the control and management of their information.

6. **Key Applications**. There are three key applications which are crucial to the running of PILOT 2:
    a. **Database** – custom build for PILOT 2 and used to manage member details.
    b. **Web Site** – used by members and the public to access information.
    c. **Sage Accounts software**– holds all the financial information for Pilot 2.

The organisation has numerous other assets, which would also potentially provide risks to the data held by Pilot 2. These assets include the Internet connection, other applications, networking devices and cabling. However the risks associated with these are deemed to be lower than those listed above, and the impact of any disruption caused by failures of these is considered to be lower.

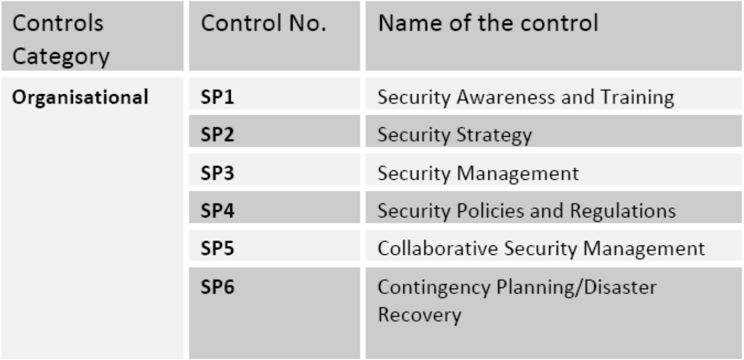
For the organisation to have a comprehensive risk management strategy we would recommend that these assets are reviewed in the future once the high risk assets have been properly examined.

This review will focus primarily on the most critical assets identified above.

5. Control Card Selection

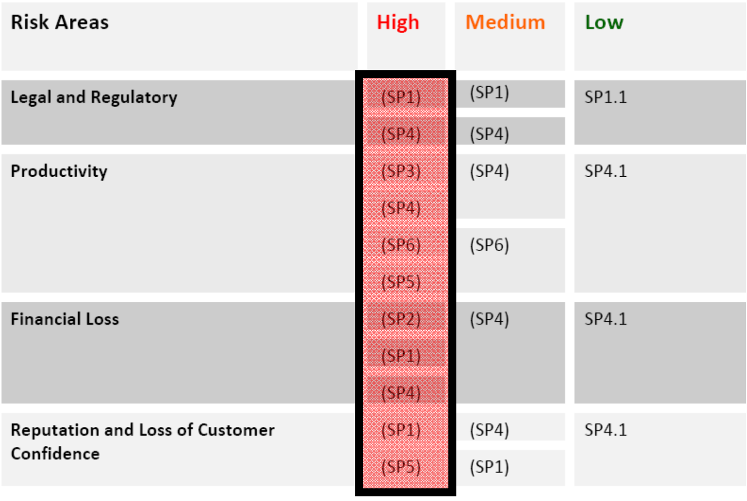
a. Organisational Controls

From the risk profile and asset identification processes above we can now select the appropriate controls that PILOT 2 need to apply in order to mitigate respective risks to the organisation. There are six possible control cards for the organisation as a whole:



Controls Category	Control No.	Name of the control
Organisational	**SP1**	Security Awareness and Training
	SP2	Security Strategy
	SP3	Security Management
	SP4	Security Policies and Regulations
	SP5	Collaborative Security Management
	SP6	Contingency Planning/Disaster Recovery

From the risk profile analysis above, we can see that PILOT 2 are classified overall as a high risk organisation. The control cards that need to be applied are therefore as follows:

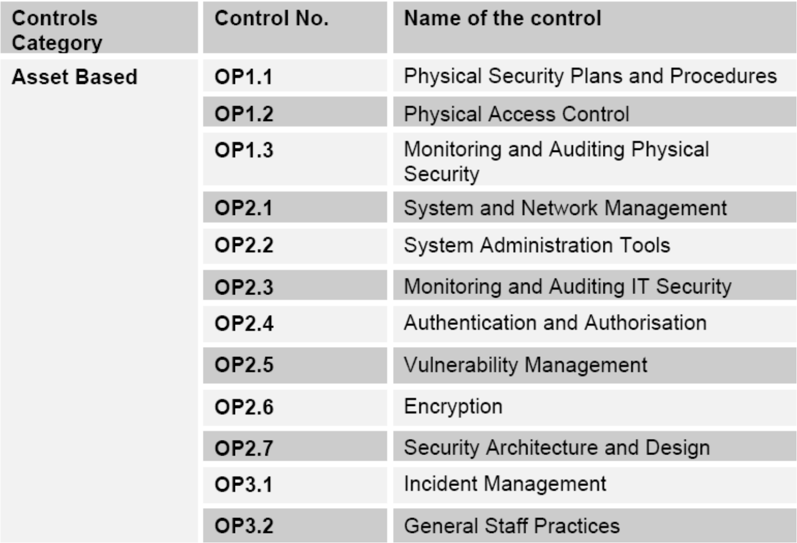


Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Productivity	(SP3) (SP4) (SP6) (SP5)	(SP4) (SP6)	SP4.1
Financial Loss	(SP2) (SP1) (SP4)	(SP4)	SP4.1
Reputation and Loss of Customer Confidence	(SP1) (SP5)	(SP4) (SP1)	SP4.1

This means that SP1, SP2, SP3, SP4, SP5 and SP6 need to be applied to Pilot 2.

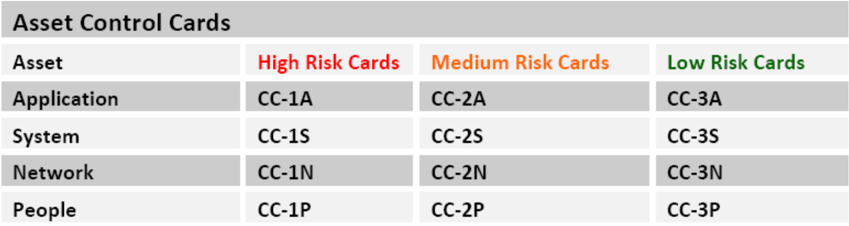
b. Asset Based Controls

There are twelve different asset based controls that can be used.



Controls Category	Control No.	Name of the control
Asset Based	OP1.1	Physical Security Plans and Procedures
	OP1.2	Physical Access Control
	OP1.3	Monitoring and Auditing Physical Security
	OP2.1	System and Network Management
	OP2.2	System Administration Tools
	OP2.3	Monitoring and Auditing IT Security
	OP2.4	Authentication and Authorisation
	OP2.5	Vulnerability Management
	OP2.6	Encryption
	OP2.7	Security Architecture and Design
	OP3.1	Incident Management
	OP3.2	General Staff Practices

The controls for each asset are decided based upon the risk level of the organisation and the type of asset concerned.



Asset Control Cards			
Asset	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

As previously identified – PILOT 2 are a high risk organisation. From our identification of assets and risk levels the following controls need to be applied:

Asset	Asset Category	Control Card Used
Data Server and Storage	System	CC-1S
Archiving and Backup	System	CC-1S
Workstation	System	CC-1S
Wireless Access Points	Network	CC-1N
Third Party Contractors	People	CC-1P
Key Applications	Application	CC-1A

6. Risk Management and Implementation

The following pages list the various controls required by Pilot 2.

Each individual control has been reviewed by PILOT 2 to identify whether they believe they are complying with that control.

Those highlighted in Green show that they believe they are currently complying.

Those highlighted in Orange show that there is a system in place, but that this needs to be reviewed and possibly updated.

Those highlighted in red show that they currently do not comply.

This gap analysis is based entirely on the responses given by Pilot 2. No verification of these responses has been carried out by PEM IT Services. If the client wishes, PEM IT Services can undertake a separate full review of the existing controls and policies. This is outside the scope of this review.

Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.2	There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.
SP1.3	Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes these topics:
	security strategies, goals, and objectives
	security regulations, polices, and procedures
	policies and procedures for working with third parties
	contingency and disaster recovery plans
	physical security requirements
	users' perspective on
	system and network management
	system administration tools
	monitoring and auditing for physical and information technology security
	authentication and authorization
	vulnerability management
	encryption
	architecture and design
	incident management
	general staff practices
	enforcement, sanctions, and disciplinary actions for security violations
	how to properly access sensitive information or work in areas where sensitive information is accessible
	termination policies and procedures relative to security

Security Strategy (SP2)

Security Strategy (SP2)	
SP2.1	The organization's business strategies routinely incorporate security considerations.
SP2.2	Security strategies and policies take into consideration the organization's business strategies and goals.
SP2.3	Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.

Security Management (SP3)

Security Management (SP3)	
SP3.1	Management allocates sufficient funds and resources to information security activities.
SP3.2	Security roles and responsibilities are defined for all staff in the organization.
SP3.3	The organization's hiring and termination practices for staff take information security issues into account.
SP3.4	The required levels of information security and how they are applied to individuals and groups are documented and enforced.
SP3.5	The organization manages information security risks, including
	assessing risks to information security both periodically and in response to major changes in technology, internal/external threats, or the organization's systems and operations
	taking steps to mitigate risks to an acceptable level
	maintaining an acceptable level of risk
	using information security risk assessments to help select cost-effective security/control measures, balancing implementation costs against potential losses
SP3.6	Management receives and acts upon routine reports summarizing the results of
	review of system logs
	review of audit trails
	technology vulnerability assessments
	security incidents and the responses to them
	risk assessments
	physical security reviews
	security improvement plans and recommendations

Security Policies and Regulations (SP4)

Security Policies and Regulations (SP4)	
SP4.1	The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including
	security strategy and management
	security risk management
	physical security
	system and network management
	system administration tools
	monitoring and auditing
	authentication and authorization
	vulnerability management
	encryption
	security architecture and design
	incident management
	staff security practices
	applicable laws and regulations
	awareness and training
	collaborative information security
	contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including
	creation
	administration (including periodic reviews and updates)
	communication
SP4.3	The organization has a documented process for periodic evaluation (technical and non-technical) of compliance with information security policies, applicable laws and regulations, and insurance requirements.
SP4.4	The organization has a documented process to ensure compliance with information security policies, applicable laws and regulations, and insurance requirements.
SP4.5	The organization uniformly enforces its security policies.
SP4.6	Testing and revision of security policies and procedures is restricted to authorized personnel.

Collaborative Security Management (SP5)

Collaborative Security Management (SP5)	
SP5.1	The organization has documented, monitored, and enforced procedures for protecting its information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners).
SP5.2	The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.
SP5.3	The organization documents, monitors, and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or is used by its own personnel.
SP5.4	The organization provides and verifies awareness and training on applicable external organizations' security polices and procedures for personnel who are involved with those external organizations.
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access. These procedures are communicated and coordinated with the external organization.

Contingency Planning/Disaster Recovery (SP6)

Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented
	business continuity or emergency operation plans
	disaster recovery plan(s)
	contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are
	aware of the contingency, disaster recovery, and business continuity plans
	understand and are able to carry out their responsibilities

Notes on Organisational Controls

1. PILOT 2 currently outsource the support of their IT infrastructure to a third party – Rock IT. As such some of the controls are carried out by the third party on behalf of the organisation.

2. Some guidance on IT Security is given to staff in the staff handbook, but there is no process for ongoing reminders or training.

3. The IT strategy of PILOT 2 is currently being reviewed and as such IT Security will form part of this process.

System - Server

🔴 ⚪ ⚪

Asset Based Control Card ID	**CC-1S**									
Risk Profile	**High**									
Asset Category	**System**									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented

.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

System – Archiving and Backup

Asset Based Control Card ID	**CC-1S**
Risk Profile	**High**
Asset Category	**System**

Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented

.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

System – Workstations

🔴 ⚪ ⚪

Asset Based Control Card ID	**CC-1S**
Risk Profile	**High**
Asset Category	**System**

Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		**2.1.3** **2.1.4** **2.1.5** **2.1.9**			**2.4.1** **2.4.6**		**2.6.1**			
Integrity		**2.1.4** **2.1.5** **2.1.8** **2.1.9** **2.1.10**			**2.4.1** **2.4.3** **2.4.6**			**2.7.1** **2.7.2**		
Availability		**2.1.6** **2.1.7** **2.1.9**			**2.4.6**					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented

.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Network – Wireless Access Points

● ○ ○

Asset Based Control Card ID	**CC-1N**									
Risk Profile	**High**									
Asset Category	**Network**									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality					2.4.6	2.5.3	2.6.1			
Integrity	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Availability	1.1.4				2.4.6					

A high risk profile implies threats that occur in network vulnerabilities that can lead to external attacks or internal unauthorised access to certain network areas of high interest or risk.

Lack of Network security has an immediate and direct effect in applications running and information flow.

Network-based confidentiality controls for a high risk organizational profile should protect critical and internal information from potential loss or misuse. Furthermore, information stored in network must be available and easily accessed and separated according to criticality level.

Essential Controls for the safeguard of confidentiality, integrity and availability in a network are the following:

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

OP2.1.1 Control requires that there are documented security plan(s) for safeguarding the systems and networks.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP 2.5.3 Control requires that technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.

OP1.1.4 Control requires that there are documented policies and procedures for managing visitors, including sign in, escort, access logs, reception and hosting.

People - Contractors

● ○ ○

Asset Based Control Card ID	**CC-1P**
Risk Profile	**High**
Asset Category	**People**

Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality										**3.2.1 3.2.2 3.2.3**
Integrity	**1.1.4 1.3.2**									**3.2.1 3.2.2 3.2.3**
Availability										

A high risk profile implies threats that occur in management of people and in human resources in general. The level of staff commitment on using the appropriate security controls on network resources determines level of protection that can be achieved.

The manipulation of information and the reuse of older records with high value for the organization is a critical aspect. Internal or confidential information from staff should be treated respectfully. Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP3.2.3 Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

OP1.3.2 Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for.

Application - Database

🔴 ⚪ ⚪

Asset Based Control Card ID	**CC-1A**									
Risk Profile	**High**									
Asset Category	**Application**									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		**2.1.3**			**2.4.2**	**2.5.1**	**2.6.1**			
Integrity		**2.1.4**			**2.4.2**	**2.5.1**	**2.6.1**			
Availability		**2.1.6**								

Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

Application – Website

● ○ ○

Asset Based Control Card ID					**CC-1A**					
Risk Profile					**High**					
Asset Category					**Application**					
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		**2.1.3**			**2.4.2**	**2.5.1**	**2.6.1**			
Integrity		**2.1.4**			**2.4.2**	**2.5.1**	**2.6.1**			
Availability		**2.1.6**								

Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

Application – Sage Accounts

🔴 ⚪ ⚪

<table>
<tr><td colspan="5"><b>Asset Based Control Card ID</b></td><td colspan="7"><b>CC-1A</b></td></tr>
<tr><td colspan="5"><b>Risk Profile</b></td><td colspan="7"><b>High</b></td></tr>
<tr><td colspan="5"><b>Asset Category</b></td><td colspan="7"><b>Application</b></td></tr>
<tr><td><b>Security Requirements</b></td><td><b>Physical Security</b></td><td><b>System and Network Management</b></td><td><b>System Administration Tools</b></td><td><b>Monitoring and Auditing IT Security</b></td><td><b>Authentication and Authorization</b></td><td><b>Vulnerability Management</b></td><td><b>Encryption</b></td><td><b>Security Architecture and Design</b></td><td><b>Incident Management</b></td><td><b>General Staff Practices</b></td></tr>
<tr><td><b>Confidentiality</b></td><td></td><td>2.1.3</td><td></td><td></td><td>2.4.2</td><td>2.5.1</td><td>2.6.1</td><td></td><td></td><td></td></tr>
<tr><td><b>Integrity</b></td><td></td><td>2.1.4</td><td></td><td></td><td>2.4.2</td><td>2.5.1</td><td>2.6.1</td><td></td><td></td><td></td></tr>
<tr><td><b>Availability</b></td><td></td><td>2.1.6</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

7. Summary of findings

PILOT 2 are a high risk organisation with regard to information security, because they hold personal information including qualifications and results, therefore requiring a high degree of accuracy. The risk to their reputation if data is found to be incorrect or incomplete is also high, and could directly affect the continuation of the business.

This review has highlighted a number of areas for action by PILOT 2 to minimise the risks associated with Information Security in their organisation. Whilst they have already put in place a number of steps to mitigate the risks there remain several areas that should be addressed, including:

- Documenting the current security procedures and policies, and making these available to staff.
- Ensuring that the roles of third parties are clearly defined, and that appropriate checks are in place to control third party access to information.
- Documenting the process for review and compliance with security policies.
- Implementing and documenting a full Disaster Recovery plan, and making this information available to all staff.

Key issues raised during the review that need to be addressed are:

- Change procedures for third parties need to be agreed, particularly for the web site. A recent upgrade left the web site inoperative, and PILOT 2 were unaware any upgrade was planned.
- Reviewing the use of administrator accounts on the network, and ensuring passwords are managed properly. The current administrator password may not have been changed since previous employees left who knew the password. It is recommended the password is changed immediately, and then at regular intervals in the future.
- Some workstations may not have the local administrator password set, allowing users the possibility of logging on to workstations locally with full administrator rights. This would potentially allow users to bypass some of the security controls on the network.
- Carrying out test restores of data from the backup tapes to ensure that data can be recovered in the event of an issue. This should be done immediately, and then test restores carried out at regular intervals in the future.
- There are currently no controls to limit installation of software by employees onto their machines. A software audit should be carried out to verify the software currently installed, and any unlicensed or unnecessary software removed. System policies should also be set up to prevent the unauthorised installation of software by users in the future.
- Users do not log onto the database application, and there appear to be no controls to restrict access and log activity based on individual user accounts. This should be checked with the database developers, and if necessary procedures put in place to control access by username and password.
- A review of the web site needs to be carried out to establish what procedures are in place for backing up the information on the site, and how information is secured on the site. The web shop currently appears to collect information via an unsecured web page, before transferring to a secure web site for payment details to be taken.

PILOT 2 are currently undertaking a review of their policies and processes. This includes a plan to document processes related to information security and business continuity. It is therefore recommended that once that process is completed a follow up IT Risk Management review is conducted to assess progress against this report.

PEM IT Services

A division of Peters Elworthy & Moore

Salisbury House
Station Road
Cambridge
CB1 2LA

Email: it@pem.co.uk
Tel: 01223 728222
Fax: 01223 461424
www.pemit.co.uk

Risk Management Review

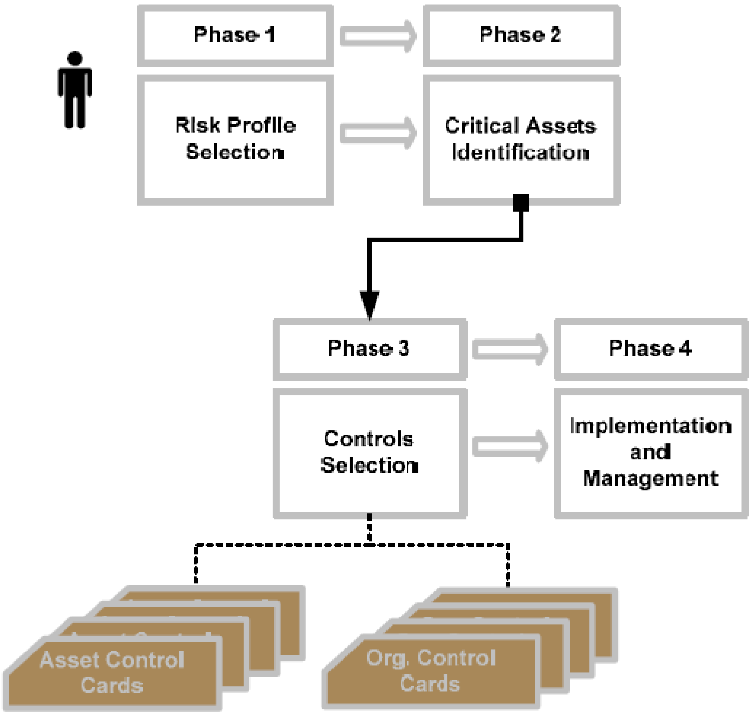
A review
for the
Pilot 3

Proposal of IT Services

This document is a review of the Risk Management and IT Security requirements for the Pilot 3.

Contents

1. Objective of this review



Part of the responsibility of MSB Managers is to provide for the security of their business environment. According to most applicable legal requirements, liability for breaches of security lies with them.

Just as they must provide a safe and secure physical environment, they must also make sure that information is protected. Given the fact, however, that computers are not “fix and forget” devices, the protection of information is a permanent concern.

This review provides an overview of the key information security risks for the organisation. It then provides a gap analysis to show the areas which are currently covered by internal procedures and policies, and highlights the areas that still need to be addressed or re-visited.

2. Who should carry out this review?

There are three alternative ways in which this review can be approached:

- In-sourcing of risk assessment – all reviews carried out by in-house staff.

- Partial outsourcing of risk assessment –initial review done by external advisor, then ongoing reviews carried out internally.

- Full outsourcing of risk assessment – entire review process is carries out by an external contractor.

Having considered the guidelines from ENISA, the Pilot 3 has decided to take the outsourcing option. This is based on the following criteria:

- The organisation is under 10 employees, and has a relatively simple IT infrastructure.

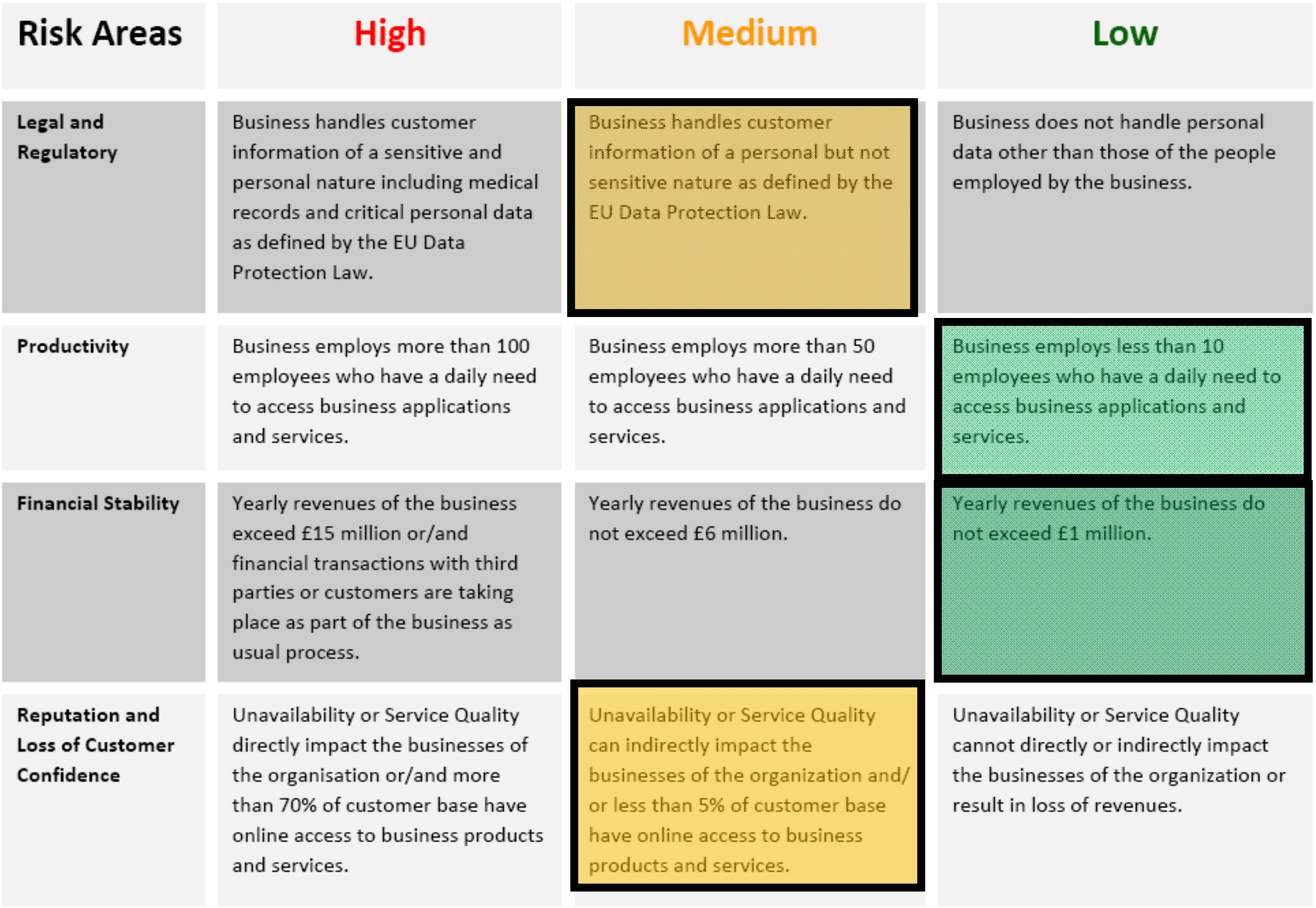
- The organisation does not currently have the time or resources to allocate to the project.

- Staff are working on other projects that have a higher priority, including a Business Continuity project.

- The questions in the assessment appear quite complex to the organisation, and therefore are difficult to understand and answer without guidance.

3. Risk Profile Analysis

The organisation’s risk profile has been considered from four separate angles, to identify the level of risk the organisation places on its information security.



Risk Areas	High	Medium	Low
Legal and Regulatory	Business handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	Business handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	Business does not handle personal data other than those of the people employed by the business.
Productivity	Business employs more than 100 employees who have a daily need to access business applications and services.	Business employs more than 50 employees who have a daily need to access business applications and services.	Business employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues of the business exceed £15 million or/and financial transactions with third parties or customers are taking place as part of the business as usual process.	Yearly revenues of the business do not exceed £6 million.	Yearly revenues of the business do not exceed £1 million.
Reputation and Loss of Customer Confidence	Unavailability or Service Quality directly impact the businesses of the organisation or/and more than 70% of customer base have online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/or less than 5% of customer base have online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

The Pilot 3 handle personal information for their members, but most of this is not of a highly sensitive nature. They do process some Credit Card payments. Therefore their risk for Legal and Regulatory non-compliance is MEDIUM.

The Pilot 3 employs 10 people who have a daily need to access business applications and services. However if the systems are down some work can still be done. Therefore the risk to Productivity is LOW.

The Pilot 3 has an annual turnover under £1 Million. Therefore the financial risk is LOW.

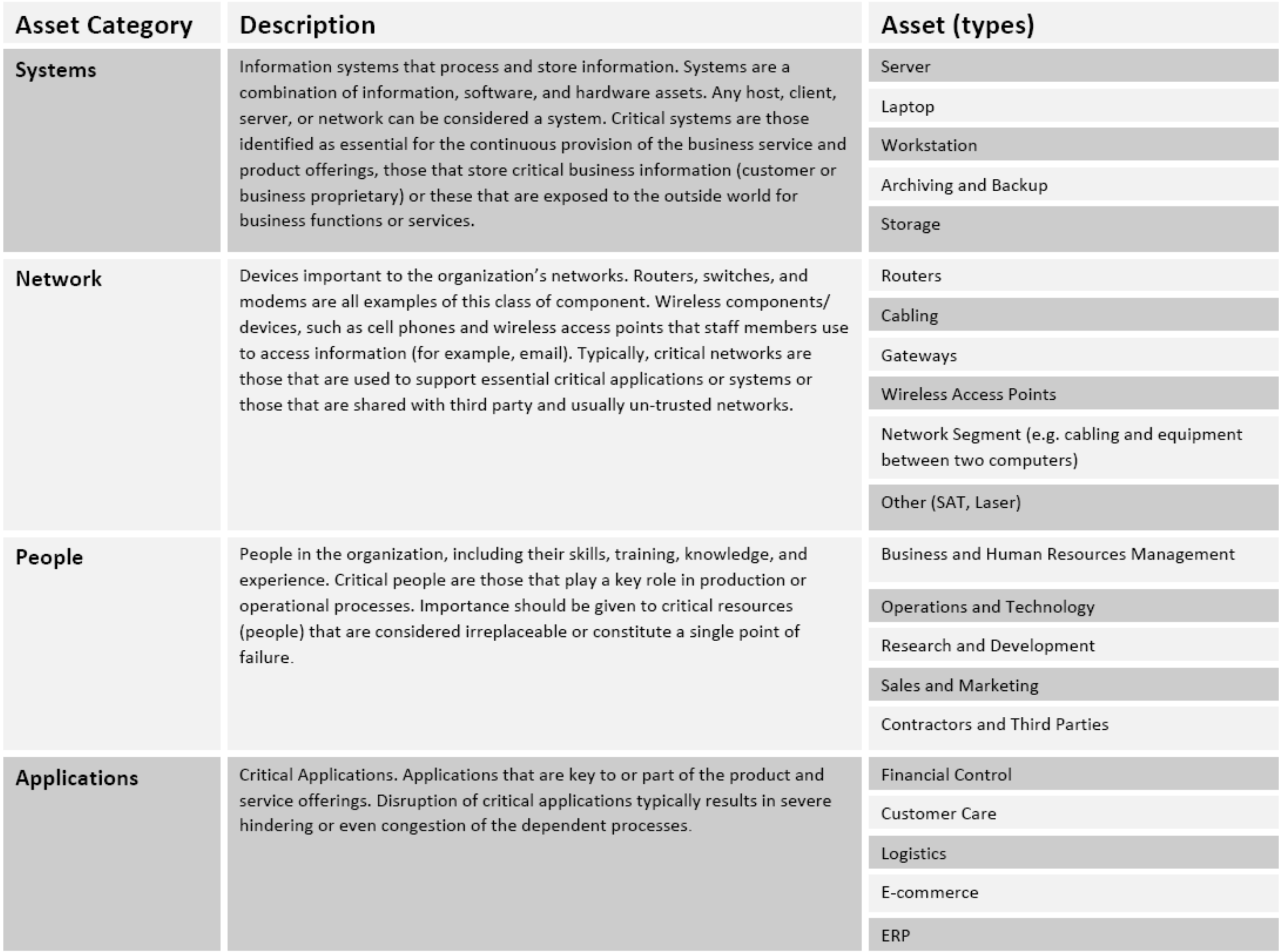
The Pilot 3 employees rely on their computer systems for much of their work. The timely production of publications is important to maintain the reputation of the organisation. This has improved markedly over the last few years, leading to increased numbers of submissions for publication. This needs to be protected. Therefore the risk to reputation or loss of customer confidence is MEDIUM.

It is therefore established that the overall risk level for the Pilot 3 is MEDIUM.

4. Identification of Critical Assets

It is important for the organisation to identify the key assets which the organisation has, from an information security perspective. These need to be identified on the basis of the adverse impact they are likely to have on the organisation in the event of the following:

- Disclosure of information to unauthorised people.
- Modification of information without authorisation.
- Loss or destruction of the asset.
- Interrupted access to the asset or information stored.



Asset Category	Description	Asset (types)
Systems	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information (customer or business proprietary) or these that are exposed to the outside world for business functions or services.	Server Laptop Workstation Archiving and Backup Storage
Network	Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of component. Wireless components/ devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with third party and usually un-trusted networks.	Routers Cabling Gateways Wireless Access Points Network Segment (e.g. cabling and equipment between two computers) Other (SAT, Laser)
People	People in the organization, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes. Importance should be given to critical resources (people) that are considered irreplaceable or constitute a single point of failure.	Business and Human Resources Management Operations and Technology Research and Development Sales and Marketing Contractors and Third Parties
Applications	Critical Applications. Applications that are key to or part of the product and service offerings. Disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.	Financial Control Customer Care Logistics E-commerce ERP

Based on the criteria above, the following assets have been identified as the most critical assets to the Pilot 3 :

1. **Data server and storage**. The Pilot 3 are an information business. The information they hold is important for the running of the organisation. If that data is lost completely there would be a major impact on the organisation. Therefore the servers holding this information are a critical asset.

2. **Archiving and Backup**. Should there be any loss of data from the server, it is critical to the Pilot 3 that the data can be recovered quickly with minimal loss.

3. **Workstations**. Staff at the Pilot 3 use their workstations to access data on the network, and therefore management of these is important to the organisation

4. **Production staff.** These are the staff who edit and produce the publications for the Pilot 3. Their role is key to the accurate and timely delivery of publications to market.

5. **Financial Team**. These staff are responsible for managing the finances of the society. This includes raising invoices and collecting money from membership and publication sales, as well as managing payments for suppliers.

6. **Key Applications**. There are three key applications which are crucial to the running of the Pilot 3:
    a. **3B2** – used to produce and generate the final documents for publication.
    b. **Office Accelerator** – holds all membership details.
    c. **Sage Accounts software**– holds all the financial information for the society.

The organisation has numerous other assets, which would also potentially provide risks to the data held by the Pilot 3. These assets include the Internet connection, other applications, networking devices and cabling. However the risks associated with these are deemed to be lower than those listed above, and the impact of any disruption caused by failures of these is considered to be lower.

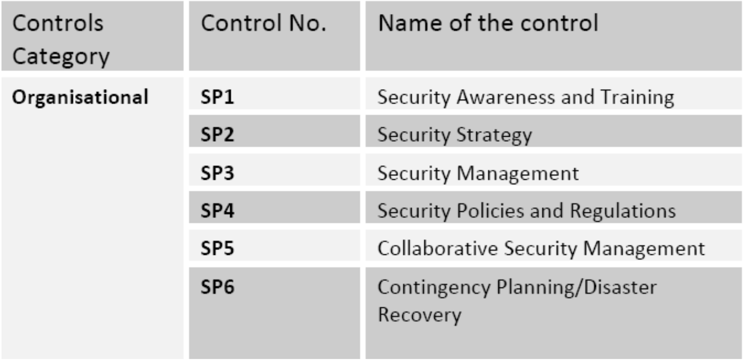
For the organisation to have a comprehensive risk management strategy we would recommend that these assets are reviewed in the future once the high risk assets have been properly examined.

This review will focus primarily on the most critical assets identified above.

5. Control Card Selection

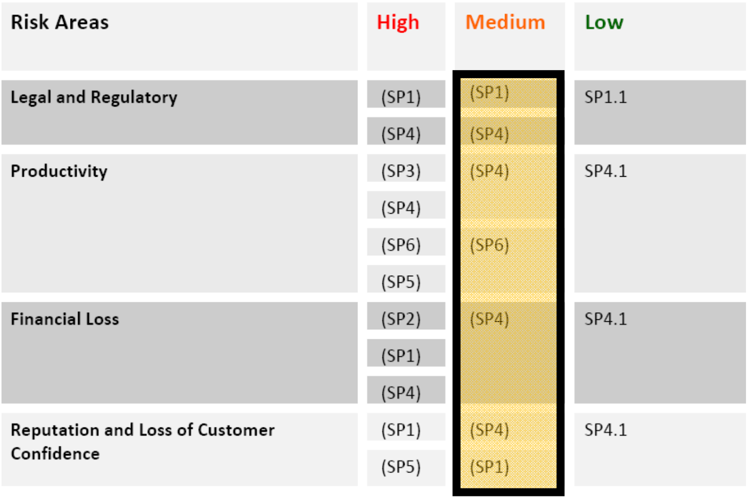
a. Organisational Controls

From the risk profile and asset identification processes above we can now select the appropriate controls that the Pilot 3 need to apply in order to mitigate respective risks to the organisation. There are six possible control cards for the organisation as a whole:



Controls Category	Control No.	Name of the control
Organisational	**SP1**	Security Awareness and Training
	SP2	Security Strategy
	SP3	Security Management
	SP4	Security Policies and Regulations
	SP5	Collaborative Security Management
	SP6	Contingency Planning/Disaster Recovery

From the risk profile analysis above, we can see that the Pilot 3 are classified overall as a medium risk organisation. The control cards that need to be applied are therefore as follows:

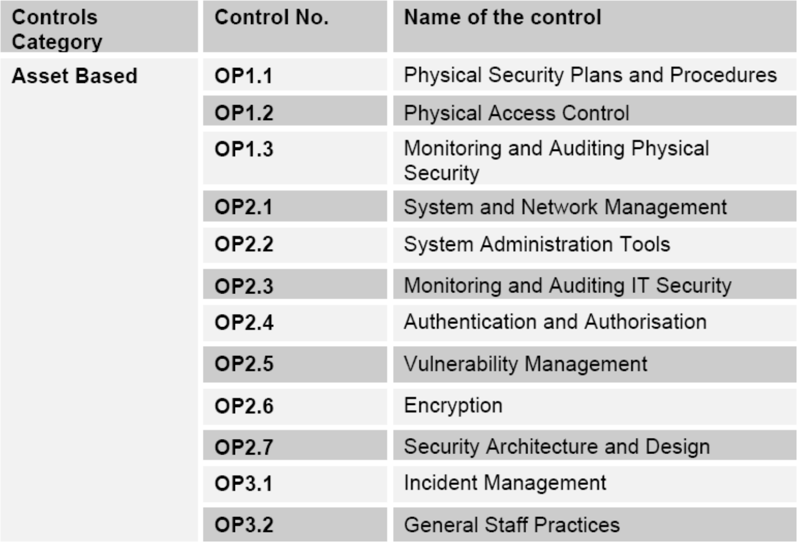


Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1)	(SP1)	SP1.1
	(SP4)	(SP4)	
Productivity	(SP3)	(SP4)	SP4.1
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Financial Loss	(SP2)	(SP4)	SP4.1
	(SP1)		
	(SP4)		
Reputation and Loss of Customer Confidence	(SP1)	(SP4)	SP4.1
	(SP5)	(SP1)	

This means that SP1, SP4, and SP6 need to be applied to the Pilot 3.

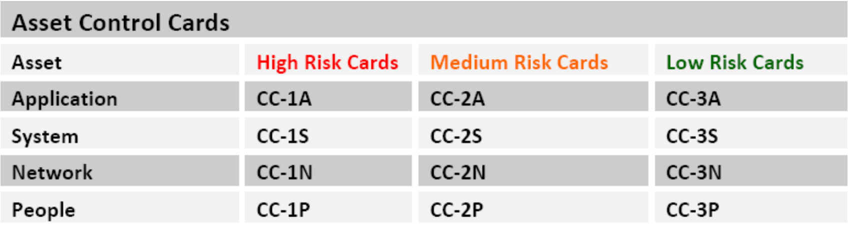
b. Asset Based Controls

There are twelve different asset based controls that can be used.



Controls Category	Control No.	Name of the control
Asset Based	OP1.1	Physical Security Plans and Procedures
	OP1.2	Physical Access Control
	OP1.3	Monitoring and Auditing Physical Security
	OP2.1	System and Network Management
	OP2.2	System Administration Tools
	OP2.3	Monitoring and Auditing IT Security
	OP2.4	Authentication and Authorisation
	OP2.5	Vulnerability Management
	OP2.6	Encryption
	OP2.7	Security Architecture and Design
	OP3.1	Incident Management
	OP3.2	General Staff Practices

The controls for each asset are decided based upon the risk level of the organisation and the type of asset concerned.



Asset Control Cards			
Asset	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

As previously identified – the Pilot 3 are a medium risk organisation. From our identification of assets and risk levels the following controls need to be applied:

Asset	Asset Category	Control Card Used
Data Server and Storage	System	CC-2S
Archiving and Backup	System	CC-2S
Workstation	System	CC-2S
Production Team	People	CC-2P
Financial Team	People	CC-2P
Key Applications	Application	CC-2A

6. Risk Management and Implementation

The following pages list the various controls required by the Pilot 3.

Each individual control has been reviewed by the Pilot 3 to identify whether they believe they are complying with that control.

Those highlighted in Green show that they believe they are currently complying.

Those highlighted in Orange show that there is a system in place, but that this needs to be reviewed and possibly updated.

Those highlighted in red show that they currently do not comply.

This gap analysis is based entirely on the responses given by the Pilot 3. No verification of these responses has been carried out by PEM IT Services. If the client wishes, PEM IT Services can undertake a separate full review of the existing controls and policies. This is outside the scope of this review.

Security Awareness and Training (SP1)

Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.2	There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.
SP1.3	Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes these topics:
	security strategies, goals, and objectives
	security regulations, polices, and procedures
	policies and procedures for working with third parties
	contingency and disaster recovery plans
	physical security requirements
	users’ perspective on
	system and network management
	system administration tools
	monitoring and auditing for physical and information technology security
	authentication and authorization
	vulnerability management
	encryption
	architecture and design
	incident management
	general staff practices
	enforcement, sanctions, and disciplinary actions for security violations
	how to properly access sensitive information or work in areas where sensitive information is accessible
	termination policies and procedures relative to security

Security Policies and Regulations (SP4)

Security Policies and Regulations (SP4)	
SP4.1	The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including
	security strategy and management
	security risk management
	physical security
	system and network management
	system administration tools
	monitoring and auditing
	authentication and authorization
	vulnerability management
	encryption
	security architecture and design
	incident management
	staff security practices
	applicable laws and regulations
	awareness and training
	collaborative information security
	contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including
	creation
	administration (including periodic reviews and updates)
	communication
SP4.3	The organization has a documented process for periodic evaluation (technical and non-technical) of compliance with information security policies, applicable laws and regulations, and insurance requirements.
SP4.4	The organization has a documented process to ensure compliance with information security policies, applicable laws and regulations, and insurance requirements.
SP4.5	The organization uniformly enforces its security policies.
SP4.6	Testing and revision of security policies and procedures is restricted to authorized personnel.

Contingency Planning/Disaster Recovery (SP6)

Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented
	business continuity or emergency operation plans
	disaster recovery plan(s)
	contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are
	aware of the contingency, disaster recovery, and business continuity plans
	understand and are able to carry out their responsibilities

Notes on Organisational Controls

1. Many of the controls are carried out but not normally documented. The Society are currently in the process of carrying out a full review of their policies and procedures and documenting them. This includes Job Descriptions and identifying roles of key individuals in the organisation.
2. The review of policies and procedures includes the design of a new Business Continuity Plan for the Society, therefore several issues highlighted above will be addressed by this.
3. The Society currently outsource the support of their IT infrastructure to a third party – PEM IT Services. As such some of the controls are carried out by the third party on behalf of the Society.

System – Server and Storage

Asset Based Control Card ID	**CC-2S**									
Risk Profile	**Medium**									
Asset Category	**System**									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		**2.1.6** **2.1.7**			**2.4.1**					
Integrity		**2.1.9**			**2.4.1**					
Availability		**2.1.6** **2.1.7**								

A medium risk profile implies moderate level threats that occur in system instabilities leading to unavailability of business service for a short period of time. Systems are unable to support applications or functions properly.

System based controls for medium risk organizational profiles involve methods that ensure proper configuration and functionality of the system for appropriate access.

Essential Control for the protection of confidentiality, integrity and availability in systems is the following:

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.1.6 Control requires that there is a documented data backup plan which is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

System - Archiving and Backup

○ ● ○

Asset Based Control Card ID	**CC-2S**										
Risk Profile	**Medium**										
Asset Category	**System**										
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**	
Confidentiality		**2.1.6** **2.1.7**			**2.4.1**						
Integrity		**2.1.9**			**2.4.1**						
Availability		**2.1.6** **2.1.7**									

A medium risk profile implies moderate level threats that occur in system instabilities leading to unavailability of business service for a short period of time. Systems are unable to support applications or functions properly.

System based controls for medium risk organizational profiles involve methods that ensure proper configuration and functionality of the system for appropriate access.

Essential Control for the protection of confidentiality, integrity and availability in systems is the following:

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.1.6 Control requires that there is a documented data backup plan which is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

System - Workstations

○ ● ○

Asset Based Control Card ID	**CC-2S**
Risk Profile	**Medium**
Asset Category	**System**

Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality		**2.1.6** **2.1.7**			**2.4.1**					
Integrity		**2.1.9**			**2.4.1**					
Availability		**2.1.6** **2.1.7**								

A medium risk profile implies moderate level threats that occur in system instabilities leading to unavailability of business service for a short period of time. Systems are unable to support applications or functions properly.

System based controls for medium risk organizational profiles involve methods that ensure proper configuration and functionality of the system for appropriate access.

Essential Control for the protection of confidentiality, integrity and availability in systems is the following:

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.1.6 Control requires that there is a documented data backup plan which is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

People – Production Team

Asset Based Control Card ID	CC-2P									
Risk Profile	Medium									
Asset Category	People									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management (OP2.5)**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality										3.2.1 3.2.2
Integrity										3.2.1 3.2.2
Availability	1.1.4									

A medium risk profile implies threats that occur in management of human resources of medium size enterprises when current security practices could lead to business problems of moderate impact.

Incidents from improper use of passwords or access rights can lead to information leakage. A medium level of confidentiality of information determines the risk level or the money loss for the organization.

Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

People – Financial Team

○ ● ○

Asset Based Control Card ID	**CC-2P**										
Risk Profile	**Medium**										
Asset Category	**People**										
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management (OP2.5)**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**	
Confidentiality										**3.2.1** **3.2.2**	
Integrity										**3.2.1** **3.2.2**	
Availability	**1.1.4**										

A medium risk profile implies threats that occur in management of human resources of medium size enterprises when current security practices could lead to business problems of moderate impact.

Incidents from improper use of passwords or access rights can lead to information leakage. A medium level of confidentiality of information determines the risk level or the money loss for the organization.

Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

Application – 3B2

Asset Based Control Card ID	**CC-2A**									
Risk Profile	**Medium**									
Asset Category	**Application**									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality					2.4.2		2.6.1			
Integrity					2.4.2					
Availability		2.1.6 2.1.7								

A medium risk profile implies storage and processing of internal or moderate-value proprietary information that would typically incur a generic threat profile involving external malicious entities intending to violate or compromise specific and moderate-value information confidentiality. Application-based confidentiality controls for a medium risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information life-cycle. Application-based integrity controls for a medium risk organizational profile define the level of accuracy of information of an application while availability refers to the level of accessibility.

Essential Controls for the protection of confidentiality, integrity and availability in applications are the following:

OP2.4.2 Control requires that there are documented information-use policies and procedures for individual and group access to establish the rules for granting the appropriate level of access, establish an initial right of access, modify the right of access, terminate the right of access and periodically review and verify the rights of access.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires all staff understand and is able to carry out their responsibilities under the backup plans.

Application – Office Accelerator

Asset Based Control Card ID	**CC-2A**									
Risk Profile	**Medium**									
Asset Category	**Application**									
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality					2.4.2		2.6.1			
Integrity					2.4.2					
Availability		2.1.6 2.1.7								

A medium risk profile implies storage and processing of internal or moderate-value proprietary information that would typically incur a generic threat profile involving external malicious entities intending to violate or compromise specific and moderate-value information confidentiality. Application-based confidentiality controls for a medium risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information life-cycle. Application-based integrity controls for a medium risk organizational profile define the level of accuracy of information of an application while availability refers to the level of accessibility.

Essential Controls for the protection of confidentiality, integrity and availability in applications are the following:

OP2.4.2 Control requires that there are documented information-use policies and procedures for individual and group access to establish the rules for granting the appropriate level of access, establish an initial right of access, modify the right of access, terminate the right of access and periodically review and verify the rights of access.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires all staff understand and is able to carry out their responsibilities under the backup plans.

Application – Sage Accounts

○ ● ○

Asset Based Control Card ID					**CC-2A**					
Risk Profile					**Medium**					
Asset Category					**Application**					
Security Requirements	**Physical Security**	**System and Network Management**	**System Administration Tools**	**Monitoring and Auditing IT Security**	**Authentication and Authorization**	**Vulnerability Management**	**Encryption**	**Security Architecture and Design**	**Incident Management**	**General Staff Practices**
Confidentiality					**2.4.2**		**2.6.1**			
Integrity					**2.4.2**					
Availability		**2.1.6** **2.1.7**								

A medium risk profile implies storage and processing of internal or moderate-value proprietary information that would typically incur a generic threat profile involving external malicious entities intending to violate or compromise specific and moderate-value information confidentiality. Application-based confidentiality controls for a medium risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information life-cycle. Application-based integrity controls for a medium risk organizational profile define the level of accuracy of information of an application while availability refers to the level of accessibility.

Essential Controls for the protection of confidentiality, integrity and availability in applications are the following:

OP2.4.2 Control requires that there are documented information-use policies and procedures for individual and group access to establish the rules for granting the appropriate level of access, establish an initial right of access, modify the right of access, terminate the right of access and periodically review and verify the rights of access.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires all staff understand and is able to carry out their responsibilities under the backup plans.

7. Summary of findings

The Pilot 3 are a medium risk organisation with regard to information security, because they hold personal information but not of a highly sensitive nature. They also have a high reliance on the availability of their data to be able to complete their primary task of preparing journals for publication.

This review has highlighted a number of areas for action by the Pilot 3 to minimise the risks associated with Information Security in their organisation. Whilst they have already put in place a number of steps to mitigate the risks there remain several areas that should be addressed, including:

- Documenting the current security procedures and policies, and making these available to staff.
- Ensuring staff understand their role in terms of IT security, and are aware of the main risks to the Society from this area.
- Documenting the process for review and compliance with security policies.
- Implementing and documenting a full Disaster Recovery plan, and making this information available to all staff.

Key issues raised during the review that need to be addressed are:

- Staff sharing passwords so other users can access emails when they are away. This should be stopped and appropriate permissions set on mailboxes to allow staff controlled access to mailboxes of others members of staff.
- All users in Sage Accounts have the same password. Each user should set their own unique password for the application.
- Some workstations may not have the local administrator password set, allowing users the possibility of logging on to workstations locally with full administrator rights. This would potentially allow users to bypass some of the security controls on the network.

As mentioned earlier, the Pilot 3 are currently undertaking a review of their policies and processes. This includes documentation of processes related to information security and business continuity. It is therefore recommended that once that process is completed a follow up IT Risk Management review is conducted to assess progress against this report. The Society also plan to implement a new Membership database system in the coming months and this should be subjected to a similar review once in place.

ENISA Information Security Risk Management Pilot
Prepared for

Pilot 4
July 2008

Index

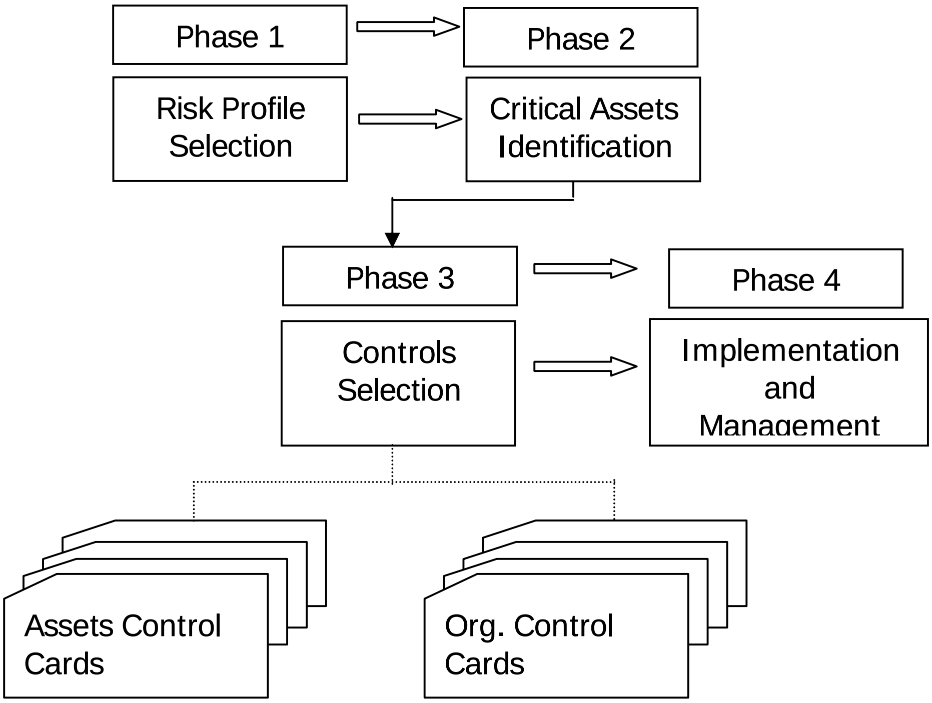
Introduction

Part of the responsibility of business owners is to provide for the security of their business environment, most applicable legal requirements, and liability for breaches of security lies with you.

Just as you must provide a safe and secure physical environment you must also ensure that information is suitably protected. This protection of information should be of permanent concern in that computer systems are not a fix and forget device, they constantly evolve as new technologies are applied within the normal working environment.

The precondition for the management of information security is to carry out a risk assessment on the business environment and assets with a view of triggering the introduction of suitable measures to address risks which are viewed as unacceptable.

ENISA Methodology



Current position

The following short summary has been compiled from an interview between Ian Sumbler of Morris Owen and xxx, Company Director of Pilot 4 on 14 July 2008.

The Company has a single server in a first floor office in Marlborough Wiltshire, with 7 networked desktop machines spread throughout the 2 storey building. In addition to the Marlborough set up, there are 2 further locations from which staff operate, but only 1 of those sites, Cardiff, has remote access into the company network. This facility has a dedicated line into Marlborough and is used by a single employee. The 2 Directors also have remote access from their home.

Remote access is controlled using a Virtual Private Network (VPN) with authentication routines in place to validate the remote user.

All users are required to enter a password to log onto the network, but there are no further access controls within the network. Email and Internet access is granted to all staff, with virus software deployed across all network PC's and also protecting the remote user devices. Email accounts for 90% of all correspondence with customers and suppliers and involves the transfer of information using Word and Excel. Password protection is used in some cases to protect unauthorised access to the information being transferred i.e. payroll data exchange between the company and the payroll bureau.

Information held electronically represents commercially sensitive information to Blue Chip Companies. There is no personal data held on either customers or their customers . Personnel records remain paper based held within cabinets within the Directors office, although as already mentioned, electronic means are used to pass staff details between the company and the payroll bureau. Some personal details are therefore going to be held electronically albeit temporarily.

Accounting and Financial information is maintained on a single PC on the network and can only be accessed by using that PC. This PC is located on the ground floor of the premises within a general office. A back up file is created daily and stored on the server in order that the network back up picks up the accounting data.

Licences are held for all applications used by the organisation, although there are no controls in place to prevent unauthorised applications from being deployed. The Company runs on a trust basis with respect to employee activities when using the Network, no acceptable use or general I.T. policy is in place.

The company is registered under the Data Protection Act.

The company regard their system as “mission critical” to the successful running of the company operations therefore the company has a server maintenance contract in place, and backups are performed daily to tape which are retained onsite.

There has been some consideration in the past regarding a Disaster Recovery or Business Continuity Plan, but this has yet to be put in place.

Phase 1 - Risk Profile Selection

The business risk aspects of information can

- Result in legal and regulatory non compliance
- Decrease productivity
- Create financial loss
- Directly or indirectly affect or damage reputation and customer confidence

Appropriate measures need to be taken to mitigate risk to an acceptable level.

Following the review with you of the current business, the I.T. set up and the market in which the company operates I have assessed the company against each of these factors in accordance with the ENISA risk profile factors.

Risk Areas	High	Medium	Low
Legal & Regulatory			✓
Productivity			✓
Financial Stability			✓
Reputation and loss of customer confidence		✓	

The Risk profile for the remainder of this assessment will be judged against the highest risk score from the above table ie. medium. This has been viewed as an appropriate level of concern due to the commercially sensitive data that you may be holding and the profile of your customer client base.

Phase 2 – Critical Assets Identification

The number of assets identifiable within any organisation could easily number in excess of 100. To make the process manageable we need to narrow the focus of the evaluation by selecting the few assets that are most critical to achieving their mission and meeting the objectives of the business. These are the only assets that are therefore analysed in the later phases of the report.

When critical assets are selected 5 assets are normally enough to enable organisations to develop a good set of mitigation plans during phase 4. The selection process has considered which assets will result in the largest adverse impact on the organisation in one of the following scenarios:

- Disclosure – of information to unauthorised people
- Modification – of information without authorisation
- Loss or destruction – of the asset
- Interrupted access – to the asset or the information stored

Assets to be identified have been considered against the following table

Asset category	Description
System	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information.
Network	Devices important to the organisation's networks, routers, switches, and modems. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications.
People	People in the organisation, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes. Importance should be given to critical resources (people) that are considered irreplaceable or constitute a single point of failure
Applications	Critical Applications. Applications that are key to or part of the product and service offerings. Disruption of critical applications typically result in severe hindering or even congestion of the dependent processes.

When evaluating security requirements for a business, or indeed the individual assets, you need to understand what aspect of the asset is important. Security requirements will focus on confidentiality, integrity and availability of the information. The evaluation highlights the importance of the asset security attributes and indicates the appropriate controls for their protection.

Result from discussion

Critical asset	Importance	Basic element	Security requirement
Server	Central to all data held	Server hardware 4 years old	Needs to meet all 3 elements of confidentiality, integrity and availability criteria
Back Up	Recovery purposes in the event of data loss	Single tape drive with multiple tapes in use	Needs to meet all 3 elements of confidentiality, integrity and availability criteria
Telecoms	Ability to communicate with customers and suppliers	Internet connection	Confidential and availability criteria
Accounts PC	Financial data	Single PC	Confidential and integrity criteria
Cabling	Access to central information to users	CAT 5 Cabling	Availability criteria

For each critical asset

1. Why is the asset critical
2. Who controls it
3. Who is responsible for it
4. Who uses it
5. How is it used

Note – Software has not been classified as critical as the major applications in use (Microsoft Exchange, Microsoft Office, Adobe Acrobat) can all be easily and quickly replaced.

Asset category	Confidentiality	Integrity	Availability
Systems	A system with confidentiality requirements often handles information with corporate information, customer base information, sensitive customer information	Systems with integrity requirements typically handle transactions of financial nature.	Availability requirements are encountered in systems that are critical to daily business operations and where downtime incurs costs and overheads
Network	A network with confidentiality requirements typically covers communications and information exchange over insecure and un-trusted environments.	Network integrity requirements are typically necessary when transactions that take place over public network or telecommunication providers	Availability requirements are especially necessary when the network is used as part of customer care, or service and product offerings.
People	Confidentiality requirements are typically encountered when people handle organisational proprietary and confidential information that when disclosed can damage the organisation's brand name and customer base.	Integrity requirements when people are concerned address share passwords. Possession of such knowledge introduces human factor threats that should be addressed with respective controls	Availability requirements for people assets are especially important when these people are critical resources for the continuous operations of the service or product offerings.
Applications	Applications with confidentiality requirements often handle information with corporate information , customer base information, sensitive customer information	Applications with integrity requirements typically handle transactions of financial nature.	Availability requirements are met in applications that are critical to the business daily operations and where downtime usually incurs costs and overheads

The important factors relating to your own organisation and the assets which have been identified as critical have been picked out in blue text.

Implementation, Monitoring and Control

One of the principles of risk management is setting the foundation for a continuous process. The principle addresses the need to implement the results as a basis for security improvements. If a business fails to implement the results of an evaluation it will also fail to improve its security position.

One of the most difficult tasks facing any improvement activity is maintaining momentum generated following an evaluation. Many practical considerations will potentially prevent organisations from immediately implementing all (or any) of the initiatives. Limited funds, staff and time will all impact on the organisation.

A step analysis can prioritise the activities to focus on implementing the highest priority solutions first.

- Risk acceptance - when a risk is accepted no action to reduce is taken and the consequences accepted
- Risk mitigation – actions designed to counter the threat are enforced
  - Who will be responsible
  - What is the cost
  - How long to deploy
  - Need to involve external expert help

Phase 3 Controls

From the medium risk profile ascribed to the business the following controls may be considered to mitigate the risks the organisation is currently exposed to at an organisational level.

The risks have been coloured coded according to the degree of exposure

Red	Requires immediate action
Amber	Secondary actions
Green	Represents a low level of risk, or risk is already covered by controls

Security Awareness and Training (SP1)	
SP1	Security Awareness and Training Control includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel. Staff understanding and roles should be clearly documented and conformance should be periodically verified.
Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.3	Security awareness, training, and periodic reminders are provided for all personnel. Training includes these topics:
	security regulations, polices, and procedures
	policies and procedures for working with third parties
	contingency and disaster recovery plans
	physical security requirements
	general staff practices, acceptable use
	enforcement, sanctions, and disciplinary actions for security violations
	how to properly access sensitive information or work in areas where sensitive information is accessible
	termination policies and procedures relative to security

Security Policies and Regulations (SP4)	
SP4	The Control Card requires an organization to have a comprehensive set of documented, current information security policies that are periodically reviewed and updated.
Security Policies and Regulations (SP4)	
SP4.1	The organization has a set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including
	security strategy and management
	physical security
	system and network management
	authentication and authorization
	staff security practices
	applicable laws and regulations
	awareness and training
	contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including
	Creation
	Administration
	Deletion
SP4.3	The organization has a documented process for periodic review (technical and non-technical) of compliance with information security policies, applicable laws and regulations, licenses, and insurance requirements.

Contigency Planning / Disaster Recovery (SP6)	
SP6	Continuity Planning/Disaster Recovery Control Cards incorporates security controls in order to assure continuous business operations in case of a disaster or unavailability of the information. Key elements of the control card are: business continuity or emergency operation plans, disaster recovery plan(s) and contingency plan(s) for responding to emergencies.
Contigency Planning / Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented
	business continuity or emergency operation plans
	disaster recovery plan(s)
	contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.

Asset Controls

System Control Card

Asset Based Control Card ID	CC-2S
Risk Profile	Medium
Asset Category	System

Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.6 2.1.7			2.4.1					
Integrity		2.1.9			2.4.1					
Availability		2.1.6 2.1.7								

A medium risk profile implies moderate level threats that occur in system instabilities leading to unavailability of business service for a short period of time. Systems are unable to support applications or functions properly.

System based controls for medium risk organizational profiles involve methods that ensure proper configuration and functionality of the system for appropriate access.

Essential Control for the protection of confidentiality, integrity and availability in systems is the following:

OP2.4.1	Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, specific applications and services, network connections within the organization, network connections from outside the organization.
OP2.1.6	Control requires that there is a documented data backup plan which is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups
OP2.1.7	Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.
OP2.1.9	Control requires that staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

Network Control Card

Asset Based Control Card ID	CC-2N									
Risk Profile	Medium									
Asset Category	Network									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality							2.6.1			
Integrity					2.4.3					
Availability		2.1.5								

A medium risk profile implies threats that occur in network vulnerabilities due to wrong or poorly-implemented network architecture that can lead to external attacks or internal unauthorised access to certain network areas of moderate interest and of medium organization value.

Lack of Network security has immediate and direct effect on applications running and information flow. The risk is considered medium when the system does not permit access to critical components that could directly affect organization reputation or financial health.

Essential Controls for the safeguard of confidentiality, integrity and availability in a network is the following:

OP2.6.1	Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, virtual private network technology, encryption for all Internet-based transmission.
OP2.4.3	Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.
OP2.1.5	Control requires that all systems are up to date with respect to revisions, patches, and recommendations

Phase 4 Implementation Plan

- Unique user identification is required for all information system users, including third-party users. Staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Passwords are changed on a regular basis and default accounts and default passwords have been removed from systems.

- Appropriate access controls are implemented and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, specific applications and services, network connections within the organization, network connections from outside the organization.

- The organization has a set of documented, current policies that are periodically reviewed and updated. These policies address key security areas, general staff practices and acceptable use policies for the organization.

- The organization has documented business continuity disaster recovery plan

Appendix

Quick Action Checklist

□	*Create a Security Policy*	Document
		Publish
		Review
□	*Know where your Critical Data is actually held:* • *On IT Systems* • *Paper Systems*	Documents
		Accounting Data
		Email
		Specialist Applications
□	*PC Operating Systems*	Older versions of PC Operating Systems do not necessarily have the latest security features available. Versions designed for business usually have more security features than versions designed for home users. Make sure you are using the appropriate operating system version
□	*Passwords*	Use Strong Passwords, and force regular changes
□	*Virus, Worms & Trojans*	Ensure anti-virus software is up to date and ensure that the appropriate features are enabled.
□	*Spam*	Understand how your e-mail software handles Spam, consider upgrading your anti-virus software to include this feature.
□	*Spyware*	Your anti-virus software will probably also support this, but again ensure that it is enabled.
□	*Firewalls*	Firewalls, make sure that yours is actually switched on and working.
□	*Patches*	Keep all your software up to date by enabling the automatic update features. But do ensure that you run them as soon as they are available.

□	*Backups*	Locally to tape
		Stored somewhere safely and preferably off site.
□	*Protect your IP*	When sending information electronically ensure that it is in a format that prevents the information being extracted and re-used.
□	*House Keeping*	Deleting Files – when deleting files often the file is just moved to a “deleted items” folder or the “waste bin”, ensure you “empty” them regularly.
		CDs – If you have application software that was provided on CD then ensure that those CDs, with authorisation codes are stored somewhere safely and preferably off site.
□	*Encrypt Data*	Business versions of PC operating systems will allow you to encrypt the data, that way if the PC is stolen the data cannot be read. Consider implementing this for laptops if they are introduced into the business
□	*Browser Software*	The latest versions of your browser software will support things like anti-phishing. Ensure your browser software is up to date and that the feature is switched on.
□	*Removable Devices*	There are an increasing number of devices that can be connected to your PC and allow for the exchange of data. USB memory sticks, but also PDAs, mobile phones, i-pods and cameras. Your PC sees all of these as external storage and you can easily move files between them. Consider the security implications and establish a policy for proper and acceptable use.

□	*Remote Workers*	Ensure any data on their PC is backed up and remote access is via a secure channel.
□	*Data Protection Act*	Understand your responsibilities under the DPA.
□	*Physical Security*	Don't forget that you still have lots of business critical information on paper. Ensure that it is kept securely as well.
□	*Disaster Recovery & Business Continuity*	Even the smallest business should have a basic plan.

Whilst the above list is comprehensive it is not exhaustive. All businesses are different and if you have any doubts at all then you are advised to take independent advice before implementing a Strategy.

RISK MANAGEMENT & IT SECURITY REVIEW

[redacted]

7 July 2008

Table of Contents

Introduction

WKH is taking part in a pilot study for the European Network & Information Security Agency (ENISA) of its Risk Management & IT Security programme for small and medium sized businesses. The pilot study is being coordinated by the International Association of Accountants Innovation Technology Consultants (IAAITC) of which WKH is a member.

WKH have been asked to carry out the testing on a small business and to report to

- That business the findings and to report, and
- ENISA on the experiences of using the programme.

The business on which the testing has been carried out is [redacted]

Executive Summary

- An IT Security Policy is currently in the process of being written and it is vital that this is completed and issued.

- There are currently no procedures in place covering Disaster Recovery and is an area that needs to be assessed on and fully documented.

- Procedures need to be put in place for protecting information when working with external organisations.

- Although there is a documented data back up plan, it is not routinely tested. A plan needs to be put into place so that restores are regularly tested and back up procedures need to be fully covered in the IT Security Policy.

- Appropriate security controls should be in place to protect sensitive information while in storage and during transmission. E.g. at present there is no encryption of back ups.

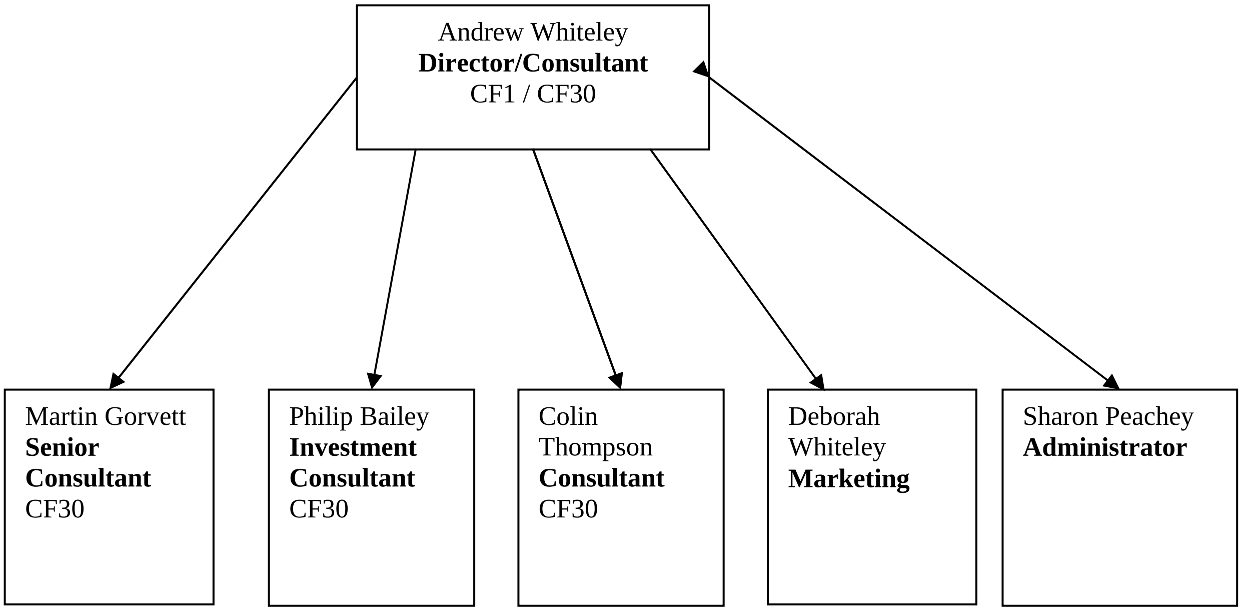
Business Overview

[redacted] is a financial services company providing independent financial planning advice, including:

- Life, critical illness and sickness insurance
- Stakeholder and personal pensions
- Pre and post retirement planning
- Group pension planning & Employee Benefits packages
- Self Invested Personal Pensions (SIPP) and Small Self Administered Schemes (SSAS) for directors
- ISA’s, PEP’s and direct investments into Unit Trusts
- Trustee & Corporate investments
- Capital Gains Tax and Income Tax mitigation schemes
- Inheritance Tax planning
- Mortgages

The company was formed in 2003, consists of 4 consultants and 2 administrators and is regulated by the Financial Services Authority.

Staff Organisation Chart



IT Support

The IT function of [redacted] is support by [redacted] all programs and data are held on the servers of [redacted] and a charge is made for this service to be provided.

Although the day to day IT support is believed to be sufficient there are concerns expressed by the director over:

- Disaster Recovery planning
- Status of the data held by third parties and accessed via the internet.

Phase 1 – Risk Profile Selection

Consideration was given to the business risks affecting information that can result in:

- Legal and regulatory non- compliance
- Decrease in productivity
- Financial loss
- Damaged reputation and customer confidence

Using a risk profile evaluation table the appropriate risk level was selected for each area as follows:

Legal & Regulatory	High
Productivity	High
Financial stability	Medium
Reputation & Loss of customer confidence	Medium

From the evaluation of the risk profile testing was undertaken on Organisational Controls - those concerned with business practices and management procedures. The full list of questions applied to the Organisational Controls can be found at Appendix 1. There are five areas of Organisational Controls with comments and recommendations as follows:

Security Awareness & Training

Staff members understand their security roles and responsibilities and these are adequately documented in the staff handbook.

An IT Security Policy in currently in the process of being written and it is vital that this is completed and issued.

Security Management

All questions covered by this section have been answered in an acceptable manner with no issues arising.

Security Policies and Regulations

This area will be covered by the introduction of the IT Security Policy.

Collaborative Security Management

This area covers procedures for protecting information when working with external organisations. This whole area needs to be addressed and included in the IT Security Policy.

Contingency planning & Disaster recovery

There are currently no procedures in place covering Disaster Recovery and is an area that needs to be planned and fully documented.

Phase 2 – Critical Assets identification and security requirements

Critical assets are those most critical to achieving the objectives of the business. The critical assets for [redacted] are identified as follows:

Systems	Servers Data back up
Network	Cabling, routers and internet connection
People	Operational staff
Applications	Advisor Office Watermark

When describing a security requirement for an asset it is important to understand which aspect of the asset is critical. For assets affecting information security the requirements will focus on Confidentiality (C), Integrity (I), and Availability (A) of the information. Each of these apply to the critical assets identified as follows:

Server	C/I/A
Data Back Up	C/I/A
Cabling, routers & Internet connection	A
Operations	C/I/A
Advisor office	C/I/A
Watermark	C/I/A

Given the nature of the business of [redacted] and the identification of various risk levels in phase 1, it is appropriate to apply a high risk profile to all aspects of the testing of the critical assets.

Detailed asset based controls have been applied to all the assets listed above. A complete list of the question applied is contained in Appendix 2.

This report only focuses on areas where a weakness has been identified and an action is required.

System and Network Management

Although there is a documented data back up plan, it is not routinely tested and verification of the ability to restore from a back up is only tested when there is a problem and a restore actually has to be performed. A plan needs to be put into place so that restores are regularly tested, back up procedures need to be fully covered in the IT Security Policy.

Authentication and Authorisation

Testing suggest that access rights to the network should be recorded by individual. There is a record in place as to who has access to all programs so this is considered to be adequate for [redacted] purposes.

Testing also suggests that authentication mechanisms should be in place to protect the integrity of sensitive information using digital signatures and biometrics. Again this is not considered to be appropriate given the size of the business.

Encryption

Appropriate security controls should be in place to protect sensitive information while in storage and during transmission. E.g. at present there is no encryption of back ups and this should be implemented.

APPENDIX 1

Organisational Controls

The selection of the organisational control cards is performed in a fairly straightforward manner:

Organisation Controls are available for every risk profile (defined in the risk profiling matrix created in **Phase 1 Risk Profile Selection**).

Security Awareness and Training (SP1)

SP1 Security Awareness and Training Control Card includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel. Staff understanding and roles should be clearly documented and conformance should be periodically verified.

Security Strategy (SP2)

SP2 Security Strategy Control Card includes controls that require the organization's business strategies to routinely incorporate security considerations. Equally, security strategies and policies must take into consideration the organization's business strategies and goals.

Security strategies, goals, and objectives should be documented and are routinely reviewed, updated, and communicated to the organization.

Security Management (SP3)

SP3 Security Management Control Card includes controls that require a security management process to be implemented and enforced. The process must continuously assess the required levels of information security and define appropriate and cost/risk balanced controls that should be applied and documented.

Security Policies and Regulations (SP4)

SP4 The Control Card requires an organization to have a comprehensive set of documented, current information security policies that are periodically reviewed and updated.

Collaborative Security Management (SP5)

SP5 Collaborative Security Management Control Cards includes security controls that enforce documented, monitored, and enforced procedures for protecting the organization's information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners).

Contingency Planning/Disaster Recovery (SP6)

SP6 Continuity Planning/Disaster Recovery Control Cards incorporates security controls in order to assure continuous business operations in case of a disaster or unavailability of the information. Key elements of the control card are:

- business continuity or emergency operation plans,
- disaster recovery plan(s) and
- contingency plan(s) for responding to emergencies.

Organisational Control Cards

Security Awareness and Training (SP1)

Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and
SP1.2	There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This
SP1.3	Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes
	security strategies, goals, and objectives
	security regulations, polices, and procedures
	policies and procedures for working with third parties
	contingency and disaster recovery plans
	physical security requirements
	users' perspective on
	system and network management
	system administration tools
	monitoring and auditing for physical and information technology security
	authentication and authorization
	vulnerability management
	encryption
	architecture and design
	incident management
	general staff practices
	enforcement, sanctions, and disciplinary actions for security violations
	how to properly access sensitive information or work in areas where sensitive
	termination policies and procedures relative to security

Organisational Control Cards

Security Strategy (SP2)

Security Strategy (SP2)	
SP2.1	The organization's business strategies routinely incorporate security considerations.
SP2.2	Security strategies and policies take into consideration the organization's business strategies
SP2.3	Security strategies, goals, and objectives are documented and are routinely reviewed,

Security Management (SP3)

Security Management (SP3)	
SP3.1	Management allocates sufficient funds and resources to information security activities.
SP3.2	Security roles and responsibilities are defined for all staff in the organization.
SP3.3	The organization's hiring and termination practices for staff take information security issues
SP3.4	The required levels of information security and how they are applied to individuals and
SP3.5	The organization manages information security risks, including
	assessing risks to information security both periodically and in response to major changes in technology, internal/external threats, or the organization's systems and
	taking steps to mitigate risks to an acceptable level
	maintaining an acceptable level of risk
	using information security risk assessments to help select cost-effective security/
SP3.6	Management receives and acts upon routine reports summarizing the results of
	review of system logs
	review of audit trails
	technology vulnerability assessments
	security incidents and the responses to them
	risk assessments
	physical security reviews
	security improvement plans and recommendations

Security Policies and Regulations (SP4)

Security Policies and Regulations (SP4)	
SP4.1	The organization has a comprehensive set of documented, current policies that are
	security strategy and management
	security risk management
	physical security
	system and network management
	system administration tools
	monitoring and auditing
	authentication and authorization
	vulnerability management
	encryption
	security architecture and design
	incident management
	staff security practices
	applicable laws and regulations
	awareness and training
	collaborative information security
	contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including
	creation
	administration (including periodic reviews and updates)
	communication
SP4.3	The organization has a documented process for periodic evaluation (technical and non-technical) of compliance with information security policies, applicable laws and regulations,
SP4.4	The organization has a documented process to ensure compliance with information security
SP4.5	The organization uniformly enforces its security policies.
SP4.6	Testing and revision of security policies and procedures is restricted to authorized personnel.

Organisational Control Cards

Collaborative Security Management (SP5)

Collaborative Security Management (SP5)	
SP5.1	The organization has documented, monitored, and enforced procedures for protecting its information when working with external organizations (e.g., third parties, collaborators,
SP5.2	The organization has verified that outsourced security services, mechanisms, and technologies
SP5.3	The organization documents, monitors, and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or
SP5.4	The organization provides and verifies awareness and training on applicable external organizations' security polices and procedures for personnel who are involved with those
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access. These procedures are communicated and

Contingency Planning/Disaster Recovery (SP6)

Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented
	business continuity or emergency operation plans
	disaster recovery plan(s)
	contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are
	aware of the contingency, disaster recovery, and business continuity plans
	understand and are able to carry out their responsibilities

System

● ○ ○

Asset Based Control Card ID	CC-1S
Risk Profile	High
Asset Category	System

Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented.
OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Network

Asset Based Control Card ID	CC-1N									
Risk Profile	High									
Asset Category	Network									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality					2.4.6	2.5.3	2.6.1			
Integrity	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Availability	1.1.4				2.4.6					

A high risk profile implies threats that occur in network vulnerabilities that can lead to external attacks or internal unauthorised access to certain network areas of high interest or risk.

Lack of Network security has an immediate and direct effect in applications running and information flow.

Network-based confidentiality controls for a high risk organizational profile should protect critical and internal information from potential loss or misuse. Furthermore, information stored in network must be available and easily accessed and separated according to criticality level.

Essential Controls for the safeguard of confidentiality, integrity and availability in a network are the following:

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

OP2.1.1 Control requires that there are documented security plan(s) for safeguarding the systems and networks.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP 2.5.3 Control requires that technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.

OP1.1.4 Control requires that there are documented policies and procedures for managing visitors, including sign in, escort, access logs, reception and hosting.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.

People

● ○ ○

Asset Based Control Card ID	CC-1P									
Risk Profile	High									
Asset Category	People									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										3.2.1 3.2.2 3.2.3
Integrity	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Availability										

A high risk profile implies threats that occur in management of people and in human resources in general. The level of staff commitment on using the appropriate security controls on network resources determines level of protection that can be achieved.

The manipulation of information and the reuse of older records with high value for the organization is a critical aspect. Internal or confidential information from staff should be treated respectfully. Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP3.2.3 Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

OP1.3.2 Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for.

Application

● ○ ○

Asset Based Control Card ID					CC-1A					
Risk Profile					High					
Asset Category					Application					
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

IAAITC Asset-Based Controls

Physical Security (OP1)	
Physical Security Plans and Procedures (OP1.1)	
OP1.1.1	There are documented facility security plan(s) for safeguarding the premises, buildings, and any restricted areas.
OP1.1.2	These plans are periodically reviewed, tested, and updated.
OP1.1.3	Physical security procedures and mechanisms are routinely tested and revised.
OP1.1.4	There are documented policies and procedures for managing visitors, including
	· sign in
	· escort
	· access logs
	· reception and hosting
OP1.1.5	There are documented policies and procedures for physical control of hardware and software, including
	· workstations, laptops, modems, wireless components, and all other components used to access information
	· access, storage, and retrieval of data backups
	· storage of sensitive information on physical and electronic media
	· disposal of sensitive information or the media on which it is stored
	· reuse and recycling of paper and electronic media
Physical Access Control (OP1.2)	
OP1.2.1	There are documented policies and procedures for individual and group access covering
	· the rules for granting the appropriate level of physical access
	· the rules for setting an initial right of access
	· modifying the right of access
	· terminating the right of access
	· periodically reviewing and verifying the rights of access
OP1.2.2	There are documented policies, procedures, and mechanisms for controlling physical access to defined entities. This includes
	· work areas
	· hardware (computers, communication devices, etc.) and software media
OP1.2.3	There are documented procedures for verifying access authorization prior to granting physical access.
OP1.2.4	Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.
Monitoring and Auditing Physical Security (OP1.3)	
OP1.3.1	Maintenance records are kept to document the repairs and modifications of a facility's physical components.
OP1.3.2	An individual's or group's actions, with respect to all physically controlled media, can be accounted for.
OP1.3.3	Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.

IAAITC Asset-Based Controls

Information Technology Security (OP2)	
System and Network Management (OP2.1)	
OP2.1.1	There are documented security plan(s) for safeguarding the systems and networks.
OP2.1.2	Security plan(s) are periodically reviewed, tested, and updated.
OP2.1.3	Sensitive information is protected by secure storage, such as
	· defined chains of custody
	· backups stored off site
	· removable storage media
	· discard process for sensitive information or its storage media
OP2.1.4	The integrity of installed software is regularly verified.
OP2.1.5	All systems are up to date with respect to revisions, patches, and recommendations in security advisories.
OP2.1.6	There is a documented data backup plan that
	· is routinely updated
	· is periodically tested
	· calls for regularly scheduled backups of both software and data
	· requires periodic testing and verification of the ability to restore from backups
OP2.1.7	All staff understands and is able to carry out their responsibilities under the backup plans.
OP2.1.8	Changes to IT hardware and software are planned, controlled, and documented.
OP2.1.9	IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.
	· Unique user identification is required for all information system users, including third-party users.
	· Default accounts and default passwords have been removed from systems.
OP2.1.10	Only necessary services are running on systems – all unnecessary services have been removed.
System Administration Tools (OP2.2)	
OP2.2.1	New security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.
OP2.2.2	Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are
	· data integrity checkers
	· cryptographic tools
	· vulnerability scanners
	· password quality-checking tools
	· virus scanners
	· process management tools
	· intrusion detection systems
	· secure remote administrations
	· network service tools
	· traffic analyzers

	· incident response tools
	· forensic tools for data analysis
Monitoring and Auditing IT Security (OP2.3)	
OP2.3.1	System and network monitoring and auditing tools are routinely used by the organization.
	· Activity is monitored by the IT staff.
	· System and network activity is logged/recorded.
	· Logs are reviewed on a regular basis.
	· Unusual activity is dealt with according to the appropriate policy or procedure.
	· Tools are periodically reviewed and updated.
OP2.3.2	Firewall and other security components are periodically audited for compliance with policy.
Authentication and Authorization (OP2.4)	
OP2.4.1	Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to
	· information
	· systems utilities
	· program source code
	· sensitive systems
	· specific applications and services
	· network connections within the organization
	· network connections from outside the organization
OP2.4.2	There are documented information-use policies and procedures for individual and group access to
	· establish the rules for granting the appropriate level of access
	· establish an initial right of access
	· modify the right of access
	· terminate the right of access
	· periodically review and verify the rights of access
OP2.4.3	Access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.
OP2.4.4	Access control methods/mechanisms are periodically reviewed and verified.
OP2.4.5	Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner.
OP2.4.6	Authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are
	· digital signatures
	· biometrics

Vulnerability Management (OP2.5)	
OP2.5.1	There is a documented set of procedures for managing vulnerabilities, including
	· selecting vulnerability evaluation tools, checklists, and scripts
	· keeping up to date with known vulnerability types and attack methods
	· reviewing sources of information on vulnerability announcements, security alerts, and notices
	· identifying infrastructure components to be evaluated
	· scheduling of vulnerability evaluations
	· interpreting and responding to the results
	· maintaining secure storage and disposition of vulnerability data
OP2.5.2	Vulnerability management procedures are followed and are periodically reviewed and updated.
OP2.5.3	Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.
Encryption (OP2.6)	
OP2.6.1	Appropriate security controls are used to protect sensitive information while in storage and during transmission, including
	· data encryption during transmission
	· data encryption when writing to disk
	· use of public key infrastructure
	· virtual private network technology
	· encryption for all Internet-based transmission
OP2.6.2	Encrypted protocols are used when remotely managing systems, routers, and firewalls.
OP2.6.3	Encryption controls and protocols are routinely reviewed, verified, and revised.
Security Architecture and Design (OP2.7)	
OP2.7.1	System architecture and design for new and revised systems include considerations for
	· security strategies, policies, and procedures
	· history of security compromises
	· results of security risk assessments
OP2.7.2	The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

IAAITC Asset-Based Controls

Staff Security (OP3)	
Incident Management (OP3.1)	
OP3.1.1	Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations, including
	· network-based incidents
	· physical access incidents
	· social engineering incidents
OP3.1.2	Incident management procedures are periodically tested, verified, and updated.
OP3.1.3	There are documented policies and procedures for working with law enforcement agencies.
General Staff Practices (OP3.2)	
OP3.2.1	Staff members follow good security practice, such as
	· securing information for which they are responsible
	· not divulging sensitive information to others (resistance to social engineering)
	· having adequate ability to use information technology hardware and software
	· using good password practices
	· understanding and following security policies and regulations
	· recognizing and reporting incidents
OP3.2.2	All staff at all levels of responsibility implements their assigned roles and responsibility for information security.
OP3.2.3	There are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where the information resides. This includes
	· employees
	· contractors, partners, collaborators, and personnel from third-party organizations
	· systems maintenance personnel
	· facilities maintenance personnel

ENISA Information Security Risk Management Pilot

Prepared for

[redacted]

September 2008

Index

Introduction

Part of the responsibility of business owners is to provide for the security of their business environment. According to most applicable legal requirements, liability for breaches of security lies with you. Just as you must provide a safe and secure physical environment you must also ensure that information is suitably protected.

The business therefore needs to have in place a security strategy that identifies the risk areas and puts in place the appropriate controls necessary to protect against the risk of a breach.

Executive Summary

A risk assessment was conducted with the aim of identifying where the risks of a breach in security are and what controls are needed.

The form of risk considered were as follows:-

Legal & Regulatory – i.e. the risk of legal and regulatory non-compliance.
Productivity - i.e. the risk of a decrease in productivity.
Financial Stability - i.e. the risk that of a financial loss.
Reputation/Loss of customer confidence - i.e. the risk, directly or in-directly, that adversely affects or damage reputation and customer confidence.

The agreed risk profile determined for [redacted] is summarised as follows:-

Legal & Regulatory	High
Productivity	Medium
Financial Stability	Medium
Reputation/Loss of customer confidence	High

The overall risk profile of the business is judged at the highest rating achieved and therefore the business has a high risk profile.

Immediate action points

The critical controls required to be put in place appropriate to this risk profile are detailed in the following pages but in summary the issues requiring immediate action are as follows:-

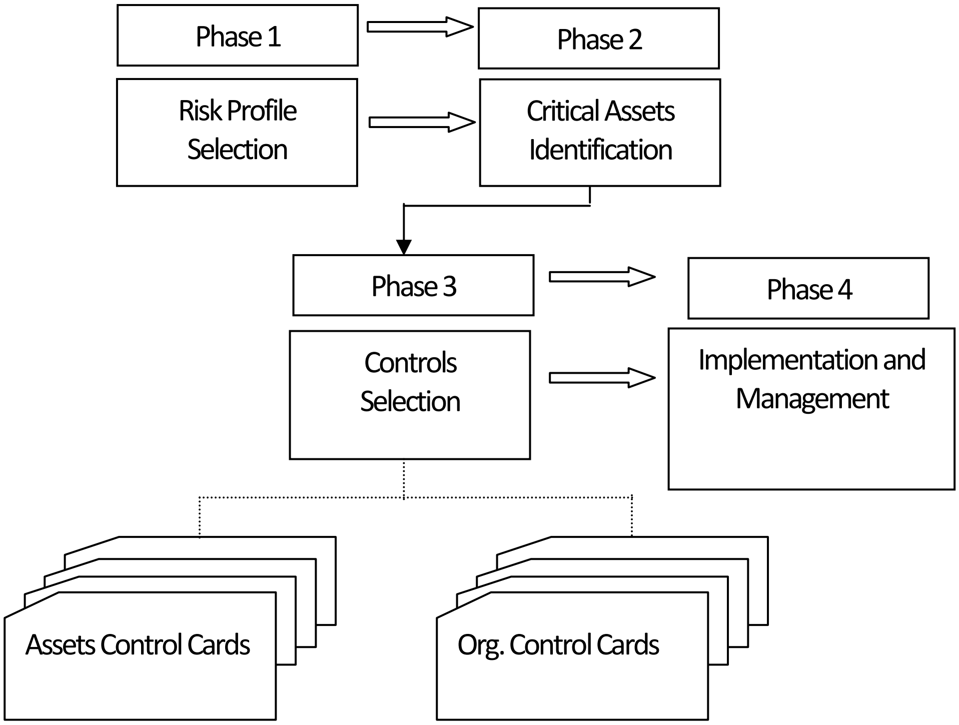
- Develop and document a Security strategy which addresses key security area and is incorporated into the overall business strategy.
- Develop and implement security awareness training.
- Develop and implement physical security access controls to the main server and portable devices.

- Develop and document a business continuity and disaster recovery plan.
- Develop and document a proven data backup plan where data is encrypted and critical software and licence information is stored off-site.
- Document the enterprise-wide security architecture and network topology.
- Develop a strategy to ensure compliance with NHS regulations for storing and accessing patient information electronically.

ENISA Methodology – summary

The following methodology was applied:-

Phase 1	identify risk areas and risk profile for the business.
Phase 2	select business critical assets.
Phase 3	select appropriate organisational and assets based controls.
Phase 4	identify actions and implement the strategy.



Current position

The following short summary has been compiled from an interview conducted between [redacted] Paul Holborow and Stephen Slater, RMT Technology Ltd.

About the business

[redacted] provides physiotherapy services in 4 clinics, in GP surgeries and in commercial workplace environments. There are approximately 78 staff with 55 clinicians and 23 in administration. There are 2 leased administration offices and services are provided in over 70 different workplace and clinical and surgery settings.

Onsite security

Access points to premises used to deliver services and store information are generally speaking secured although there is an obvious reliance on 3rd party security arrangements. Access to premises is not logged. Critical material is disposed of securely although computer parts are not kept in a secure manner.

Internal Networks

The Company operates one Windows Small Business Server 2003 Premium edition. Access on the network is controlled through domain authentication and user group permissions. First line server and user support is provided by Gosforth IT, a local IT company. There is no control over access to the network and all ports are open. There is little documentation of the IT infrastructure.

Data backup/Data Protection/Hard Copy documents

The backup, firewall, mail server and proxy server services are supplied and supported remotely by Clear Digital Solutions Ltd in Middlesbrough using a Linux based solution. Mass storage devices are not in use and paper documents, including patient details, are stored locally in filing cabinets in the head office and at one of the clinics. Paper records of patient details are archived at one clinic. External hard drives are used without authentication controls. Financial data (accounts and payroll) is stored on the central server but occasionally taken off site. Evidence that the backups have actually been performed is available on request from Clear Computing. Email is not backed up. There are no emergency plans.

Laptop/Mobile devices

Laptops are used in the business with some Company data being transferred to the laptop for off-line working. There are no hard drive encryption or authentication devices.

Internet Connection

Internet access is provided by Onyx Internet providing an ADSL connection. The firewall service is outsourced and the mail server is maintained by Clear Digital Solutions Ltd.

Phase 1 - Risk Profile Selection

The business risk aspects of information can

- Result in legal and regulatory non compliance
- Decrease productivity
- Create financial loss
- Directly or indirectly affect or damage reputation and customer confidence

Appropriate measures need to be taken to mitigate risk to an acceptable level.

Following the review with you of the current business, the I.T. set up and the market in which the company operates I have assessed the company against each of these factors in accordance with the ENISA risk profile factors.

RISK MATRIX			
Risk Areas	High	Medium	Low
Legal & Regulatory	✓		
Productivity		✓	
Financial Stability		✓	
Reputation and loss of customer confidence	✓		

The Risk profile for the remainder of this assessment will be judged against the highest risk score from the above table i.e. high. This has been viewed as an appropriate level of concern due to the commercially sensitive data that you may be holding and the profile of your customer client base.

Phase 2 – Critical Assets Identification

The number of assets identifiable within any organisation could easily number in excess of 100. To make the process manageable we need to narrow the focus of the evaluation by selecting the few assets that are most critical to achieving their mission and meeting the objectives of the business. These are the only assets that are therefore analysed in the later phases of the report.

When critical assets are selected 5 assets are normally enough to enable organisations to develop a good set of mitigation plans during phase 4. The selection process has considered which assets will result in the largest adverse impact on the organisation in one of the following scenarios:

- Disclosure – of information to unauthorised people
- Modification – of information without authorisation
- Loss or destruction – of the asset
- Interrupted access – to the asset or the information stored

Assets to be identified have been considered against the following table

Asset category	Description
System	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information.
Network	Devices important to the organisation's networks, routers, switches, and modems. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications.
People	People in the organisation, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes. Importance should be given to critical resources (people) that are considered irreplaceable or constitute a single point of failure
Applications	Critical Applications. Applications that are key to or part of the product and service offerings. Disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.

When evaluating security requirements for a business, or indeed the individual assets, you need to understand what aspect of the asset is important. Security requirements will focus on confidentiality, integrity and availability of the information. The evaluation highlights the importance of the asset security attributes and indicates the appropriate controls for their protection.

For each critical asset the following attributes were considered:-

1. Why is the asset critical?
2. Who controls it?
3. Who is responsible for it?
4. Who uses it?
5. How is it used?

Note – Software has not been classified as critical as the major applications in use (Microsoft Exchange, Microsoft Office, and Adobe Acrobat) can all be easily and quickly replaced.

Result from discussion

Critical asset	Importance	Basic element	Security requirement
Systems:			
Server	Central to all data held	Server hardware 4 years old	Confidential, integrity and availability criteria
Patient information	Essential for continuous provision of service	Paper based & electronic record of personal nature. Off-site paper archive	Confidential and availability criteria
Software	Essential for continued operation.	Off-site storage of replacement software CD's & licences	Confidential and availability criteria
Back Up	Recovery purposes in the event of data loss	Outsourced	Confidential, integrity and availability criteria
Network:			
Telecoms	Essential for access to critical hosted software	Internet connection	Confidential and availability criteria
People:			
Operational Directors	Key role in service development/continuity	Training, knowledge and contacts	Confidential, integrity and availability criteria
Third parties	Key role in maintaining IT systems	Skills & knowledge	Confidential, integrity and availability criteria
Applications:			
Customer care Financial	Patient booking and billing system. Accounting & Payroll	Software as a Service Installed on finance computers	Confidential, integrity and availability criteria Confidential & integrity criteria
Email	Communications	Mail server	Confidential & availability criteria

The important factors relating to your own organisation and the assets which have been identified as critical have been highlighted in ***italic text.***

Asset category	Confidentiality	Integrity	Availability
Systems	A system with confidentiality requirements often handles information with corporate information, customer base information, ***sensitive customer information***	Systems with integrity requirements typically handle ***transactions of financial nature***.	Availability requirements are encountered in ***systems that are critical to daily business operations*** and where downtime incurs costs and overheads
Network	A network with confidentiality requirements typically covers ***communications and information exchange over insecure and un-trusted environments.***	Network integrity requirements are typically necessary when transactions that take place over public network or telecommunication providers	Availability requirements are especially necessary when the network is used as part of customer care, or service and product offerings.
People	Confidentiality requirements are typically encountered when people handle ***organisational proprietary and confidential information that when disclosed can damage the organisation's brand name and customer base.***	Integrity requirements when people are concerned ***address share passwords.*** Possession of such knowledge introduces human factor threats that should be addressed with respective controls	Availability requirements for people assets are especially important when these people are critical resources for the ***continuous operations of the service*** or product offerings.
Applications	Applications with confidentiality requirements often handle information with ***corporate information , customer base information, sensitive customer information***	Applications with integrity requirements typically handle transactions of ***financial nature.***	Availability requirements are met in applications that are ***critical to the business daily operations and where downtime usually incurs costs and overheads***

Phase 3 Controls

From the high risk profile ascribed to the business the following controls may be considered to mitigate against the risks the organisation is currently exposed to at an organisational level.

The risks have been coloured coded according to the degree of exposure:

Red	Requires immediate action
Amber	Secondary actions
Green	Represents a low level of risk, or risk is already covered by controls

Organisational Controls

System Control Card

🔴 ⚪ ⚪

Security Awareness and Training (SP1)	
SP1	Security Awareness and Training Control includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel. Staff understanding and roles should be clearly documented and conformance should be periodically verified.

Security Awareness and Training (SP1)	
SP1.1	🟨 Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.2	🟨 There is adequate in-house expertise for all supported services, mechanisms and technologies including their secure operation.
SP1.3	🟥 Security awareness, training, and periodic reminders are provided for all personnel. Training includes these topics:
	🟥 security regulations, polices, and procedures
	🟥 policies and procedures for working with third parties
	🟥 contingency and disaster recovery plans
	🟨 physical security requirements
	🟩 general staff practices, acceptable use
	🟩 enforcement, sanctions, and disciplinary actions for security violations
	🟩 how to properly access sensitive information or work in areas where sensitive information is accessible
	🟩 termination policies and procedures relative to security

Security Strategy (SP2)	
SP2	Security Awareness and Training Control Cards includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training and periodic reminders should be provided for all personnel. Staff understanding and roles should be clearly documented and conformance should be periodically verified.
Security Strategy (SP2)	
SP2.1	The organisation's business strategies routinely incorporate security considerations.
SP2.2	Security strategies and policies take into consideration the organisation's business strategies.
SP2.3	Security strategies, goals and objectives are documented and are routinely reviewed.

Security Management (SP3)	
SP3	Security Management Control Cards include controls that require a security management process to be implemented and enforced. The process must continuously assess the required levels of information security and define appropriate cost/risk balanced controls that should be applied and documented.
Security Management (SP3)	
SP3.1	Management allocates sufficient funds and resources to information security activities.
SP3.2	Security roles and responsibilities are defined for all staff in the organisation.
SP3.3	The organisation's hiring and termination practices for staff take information security issues into consideration.
SP3.4	The required levels of information security and how they are applied to individuals are reviewed continuously.
SP3.5	The organisation manages information security risks, including Assessing risk periodically in relation to changes to technology, internal/external threats Taking steps to mitigate risks to an acceptable level Maintaining an acceptable level of risk Using risk assessments to help select cost effective security solutions
SP3.6	Management receives and acts upon routine reports summarizing the results of: Review of system logs Review of audit trails

	Technology vulnerability assessments Security incidents and responses to them Risk assessments Physical security reviews Security improvement plans and recommendations

Security Policies and Regulations (SP4)	
SP4	The Security Policies and Regulations Control Card require an organisation to have a comprehensive set of documented, current information security policies that are periodically reviewed and updated.
Security Policies and Regulations (SP4)	
SP4.1	The organisation has a set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including:
	security strategy and management
	physical security
	system and network management
	authentication and authorization
	staff security practices
	applicable laws and regulations
	awareness and training
	contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including
	Creation
	Administration
	Deletion
SP4.3	
SP4.4	The organisation has a documented process to ensure compliance with information security plans.
SP4.5	The organisation uniformly enforces its security policy

Collaborative Security Management (SP5)	
SP5	Collaborative Security Management Control Cards include security controls that enforce documented, monitored and enforced procedures for protecting the organisation's information when working with external organisation's (e.g. third parties, collaborators, subcontractors or partners).
Collaborative Security Management (SP5)	
SP5.1	The organisation has documented, monitored and enforced procedures for protecting its information when working with external organisation's (e.g. third parties, collaborators).
SP5.2	The organisation has verified that outsourced security services, mechanisms and technologies have a security strategy in place.
SP5.3	The organisation documents, monitors and enforces protection strategies for information belonging to external organisation's that is accessed from its own infrastructure.
SP5.4	The organisation provides and verifies awareness and training on applicable external organisation's security policies and procedures for those personnel involved with those third parties.
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access.

Contingency Planning/Disaster Recovery (SP6)	
SP6	Continuity Planning/Disaster Recovery Control Cards incorporates security controls in order to assure continuous business operations in case of a disaster or unavailability of the information. Key elements of the control card are: business continuity or emergency operation plans, disaster recovery plan(s) and contingency plan(s) for responding to emergencies.
Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organisation has documented
	business continuity or emergency operation plans
	disaster recovery plan(s)
	contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are aware of the contingency, disaster recovery and business continuity plans and understand and are able to carry out there responsibilities.

Asset Controls

System Control Card

🔴 ○ ○

Asset Based Control Card ID	CC-1S
Risk Profile	High
Asset Category	System

Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organisational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organisational profiles typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity.

Essential controls for the safeguard of integrity in critical assets are the following:

OP2.1.3	Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off-site, removable storage media and discard process for sensitive information or its storage media.
OP2.1.4	Control requires that the integrity of installed software is regularly verified.
OP2.1.5	Control requires that all systems are up to date with respect to revisions, patches and recommendations in security advisories.
OP2.1.6	Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups
OP2.1.7	Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.
OP2.1.8	Control requires that changes to IT hardware and software are planned, controlled, and documented
OP2.1.9	Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.
OP2.1.10	Control requires that only necessary services are running on systems – all unnecessary services have been removed.
OP2.2.1	Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organisation's security strategies.
OP2.2.2	Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.
OP2.3.1	Control requires that system and network monitoring and auditing tools are routinely used by the organisation. Activity is monitored by the IT staff, System and network activity is logged/ recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.
OP2.4.1	Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organisation, network connections from outside the organisation
OP2.4.3	Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures
OP2.4.6	Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.
OP2.6.1	Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.
OP2.7.1	Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.
OP2.7.2	Control requires that the organisation has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Asset Controls

🔴 ⚪ ⚪

Network Control Card

Asset Based Control Card ID	CC-1N									
Risk Profile	High									
Asset Category	Network									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality					2.4.6	2.5.3	2.6.1			
Integrity	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Availability	1.1.4				2.4.6					

A high risk profile implies threats that occur in network vulnerabilities that can lead to external attacks or internal unauthorised access to certain network areas of high interest or risk.

Lack of Network security has an immediate and direct effect in applications running and information flow.

Network-based confidentiality controls for a high risk organisational profile should protect critical and internal information from potential loss or misuse. Furthermore, information stored in network must be available and easily accessed and separated according to criticality level.

Essential Controls for the safeguard of confidentiality, integrity and availability in a network are the following:

OP2.6.1	This control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.
OP2.4.6	Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.
OP2.7.2	Control requires that the organisation has up-to-date diagrams that show the enterprise-wide security architecture and network topology.
OP2.1.1	Control requires that there are documented security plan(s) for safeguarding the systems and networks.
OP2.4.1	Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organisation, network connections from outside the organisation.
OP2.4.3	Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.1.10	Control requires that only necessary services are running on systems – all unnecessary services have been removed.
OP 2.5.3	Control requires that technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.
OP1.1.4	Control requires that there are documented policies and procedures for managing visitors, including sign in, escort, access logs, reception and hosting.
OP2.4.6	Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.

Asset Controls

People control card

Asset Based Control Card ID	CC-1P									
Risk Profile	High									
Asset Category	People									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										3.2.1 3.2.2 3.2.3
Integrity	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Availability										

A high risk profile implies threats that occur in management of people and in human resources in general. The level of staff commitment on using the appropriate security controls on network resources determines level of protection that can be achieved.

The manipulation of information and the reuse of older records with high value for the organisation is a critical aspect. Internal or confidential information from staff should be treated respectfully. Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1	Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.
OP3.2.2	Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.
OP3.2.3	Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organisations, systems maintenance personnel, or facilities maintenance personnel.
OP1.1.4	Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.
OP1.3.2	Control requires that an individual's or group's actions – with respect to all physically controlled media – can be accounted for.

Application

Asset Based Control Card ID	CC-1A									
Risk Profile	High									
Asset Category	Application									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Application-based confidentiality controls for a high risk organisational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2	Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.
OP2.5.1	Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.
OP2.1.3	Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.
OP2.1.4	Control requires that the integrity of installed software is regularly verified.
OP2.1.6	Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.
OP2.6.1	Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

Phase 4 Implementation, Monitoring and Control

One of the principles of risk management is setting the foundation for a continuous process. The principle addresses the need to implement the results as a basis for security improvements. If a business fails to implement the results of an evaluation it will also fail to improve its security position.

One of the most difficult tasks facing any improvement activity is maintaining momentum generated following an evaluation. Many practical considerations will potentially prevent organisations from immediately implementing all (or any) of the initiatives. Limited funds, staff and time will all impact on the organisation.

A step analysis can prioritise the activities to focus on implementing the highest priority solutions first.

- Risk acceptance - when a risk is accepted no action to reduce is taken and the consequences accepted
- Risk mitigation – actions designed to counter the threat are enforced
    - Who will be responsible
    - What is the cost
    - How long to deploy
    - Need to involve external expert help

Issues requiring immediate action.

- Security Policies and Regulations should be developed to provide a comprehensive set of documented, current information security policies that are periodically reviewed and updated. These policies address key security areas, general staff practices and acceptable use policies for the organisation.

- Security awareness training to staff incorporating security policies, procedures and disaster recovery plans needs to be provided to all staff and include working with third parties. These should be reviewed periodically and staff should understand their roles. Procedures should be clearly documented and conformance should be periodically verified.

- Appropriate access controls are implemented to restrict physical access to the server and network infrastructure both from internal staff and external contractors.

- The organisation has a set of documented, current security policies that are periodically reviewed and updated.

- The organisation has documented business continuity disaster recovery plan. Continuity Planning/Disaster Recovery incorporates impact assessment and security controls in order to assure continuous business operations in case of a disaster or unavailability of the information.

- The organisation has a documented data backup plan that is routinely updated, is periodically tested and calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups. The backup should be encrypted and software licences and disks stored off site.

- The organisation has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Summary

Implementation Plan	Gap Analysis	Risk Management Plan	Implementation/Monitoring & Control
Organisational controls	Security Awareness Training	Raise the profile of risk & develop training	In house
	Security Policies and Regulations	Formulate and communicate policies	In house
	Physical Access controls	Implement security controls to network	In house
	No formal security strategy as part of business strategy	Develop security strategy & document	Out source
	No Disaster Recovery plan	Develop DR plan and test	Out source
Asset controls	No documented back up plan	Develop and test back up plan	In house
	Diagram and documentation for systems architecture.	Document architecture	In house

Appendix

Quick Action Checklist

□	*Create a Security Policy*	Document
		Publish
		Review
□	*Know where your Critical Data is actually held:* • *On IT Systems* • *Paper Systems*	Documents
		Accounting Data
		Email
		Specialist Applications
□	*PC Operating Systems*	Older versions of PC Operating Systems do not necessarily have the latest security features available. Versions designed for business usually have more security features than versions designed for home users. Make sure you are using the appropriate operating system version
□	*Passwords*	Use Strong Passwords, and force regular changes
□	*Virus, Worms & Trojans*	Ensure anti-virus software is up to date and ensure that the appropriate features are enabled.
□	*Spam*	Understand how your e-mail software handles Spam, consider upgrading your anti-virus software to include this feature.
□	*Spyware*	Your anti-virus software will probably also support this, but again ensure that it is enabled.
□	*Firewalls*	Firewalls, make sure that yours is actually switched on and working.
□	*Patches*	Keep all your software up to date by enabling the automatic update features. But do ensure that you run them as soon as they are available.

□	*Backups*	Locally to tape
		Stored somewhere safely and preferably off site.
□	*Protect your IP*	When sending information electronically ensure that it is in a format that prevents the information being extracted and re-used.
□	*House Keeping*	Deleting Files – when deleting files often the file is just moved to a "deleted items" folder or the "waste bin", ensure you "empty" them regularly.
		CDs – If you have application software that was provided on CD then ensure that those CDs, with authorisation codes are stored somewhere safely and preferably off site.
□	*Encrypt Data*	Business versions of PC operating systems will allow you to encrypt the data, that way if the PC is stolen the data cannot be read. Consider implementing this for laptops if they are introduced into the business
□	*Browser Software*	The latest versions of your browser software will support things like anti-phishing. Ensure your browser software is up to date and that the feature is switched on.
□	*Removable Devices*	There are an increasing number of devices that can be connected to your PC and allow for the exchange of data. USB memory sticks, but also PDAs, mobile phones, i-pods and cameras. Your PC sees all of these as external storage and you can easily move files between them. Consider the security implications and establish a policy for proper and acceptable use.

□	*Remote Workers*	Ensure any data on their PC is backed up and remote access is via a secure channel.
□	*Data Protection Act*	Understand your responsibilities under the DPA.
□	*Physical Security*	Don't forget that you still have lots of business critical information on paper. Ensure that it is kept securely as well.
□	*Disaster Recovery & Business Continuity*	Even the smallest business should have a basic plan.

Whilst the above list is comprehensive it is not exhaustive. All businesses are different and if you have any doubts at all then you are advised to take independent advice before implementing a Strategy.