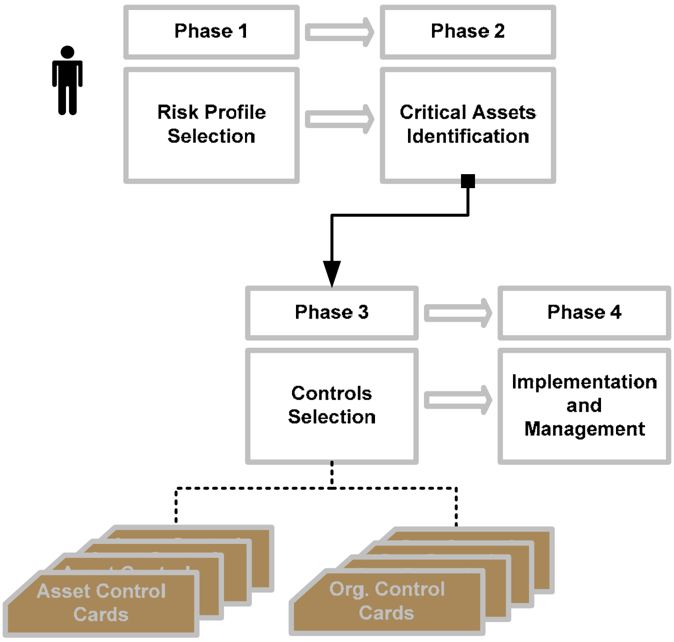
Risk Management
&
IT Security

for
Micro and Small Businesses

CONTENTS

How to proceed with Information Security



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.

Decision makers can initiate risk assessment on their environment and trigger the introduction of suitable measures to face unacceptable risks. This is the precondition for the management of information security. In performing this, a variety of approaches may be followed concerning the staffing of such an effort (also known as a “make-or-buy” decision).

We differentiate between three approaches:

- **In-sourcing of risk assessment**
- **Partial outsourcing of risk assessment**
- **Full outsourcing of risk assessment**

In-sourcing

Questions for the decision maker	Answer	
	☺ YES	☹ NO
Is your business small? Does it have a flat or simple hierarchical structure?		
Do you have **internal know-how in IT Systems and Networks?**		
Does your business have qualified and available human resources?		
Do your business activities have a low dependency on IT systems and are they uninvolved in storing or processing customer data of a sensitive nature and has your organization been involved in similar activities, i.e. quality improvement processes?		
Can you find a group of three to five people who have a broad and deep understanding of the business and also possess most of the following skills? • problem-solving ability • analytical ability • ability to work in a team • leadership skills • **Ability to understand the firm's business processes and the underlying infrastructure of the business** • ability to spend a few days working on this method		
Do you have a relatively simple information technology infrastructure that is well-understood by at least one individual in your organization?		

A majority of "YESs" will typically mean that the business should be able to develop their own policies internally.

In-sourcing of risk assessment: the risk assessment and the identification of necessary measures is performed by internal staff. The assessment is based on a risk assessment approach that has been selected by the business (e.g. a good practice, a known standard, etc.). This will help the business to master the assessment approach for recurring executions

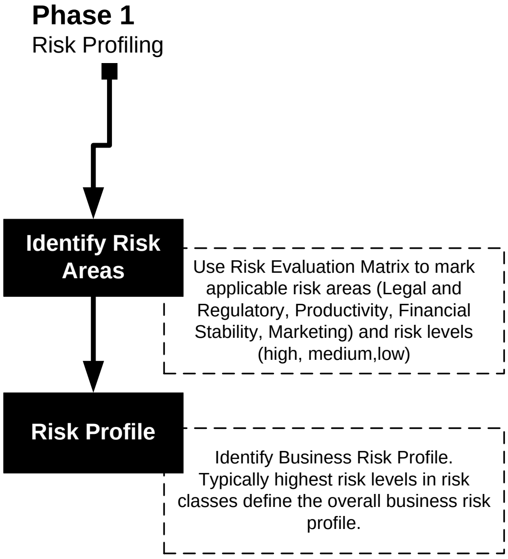
Partial Outsourcing

Questions for the decision maker	**Answer**	
	☺ **YES**	☹ **NO**
Do you deem it necessary to retain an increased focus on core competencies and strategic business processes but also improve internal information security awareness and competency in information security matters?		
Is it likely you can make available one to two people in your organisation who have a broad and deep understanding of the organization and also possess most of the following skills? • **Ability to understand the business processes and the underlying infrastructure of the organization** • problem-solving ability • analytical ability • ability to work in a team • leadership skills • ability to spend a few days working on this method • they are going to be on a longer term employment		
Do you have a complex and a relatively large IT infrastructure but a relatively simple business model?		
Do your business and service offerings include financial transactions?		
Do you operate a business that is highly subject to strict EU or Domestic Legal and Regulatory constraints and/or mandates?		
The more questions that have been answered with a "YES" the better is the MSB suited for this risk assessment implementation approach		
Partial outsourcing of risk assessment: this approach assumes that the initial risk assessment is performed by an external company. The assessment will be based on a risk assessment approach that is known to the MSB. Hence, further risk assessments can be performed by internal personnel. The initial assessment performed by the outsourcer serves as know-how transfer to the MSB's internal personnel.		

Full Outsourcing

Questions for the decision maker	Answer	
	☺ YES	☹ NO
Do you deem it necessary to **retain an increased focus** on core competencies and strategic business processes?		
Would you **find it hard to make available two to five people** who have a broad and deep understanding of the organization and also possess most of the following skills? • **Ability to understand the business processes and the underlying infrastructure of the organization** • problem-solving ability • analytical ability • ability to work in a team • leadership skills • ability to spend a few days working on this method		
Do you have a **highly complex and a relatively large IT infrastructure**?		
Does you business and service offerings include **financial transactions**?		
Do you **operate a business which is highly subject to strict EU or Domestic Legal and Regulatory constraints and/or mandates**?		
Do you have a relatively simple information technology infrastructure which is well-understood by at least one individual in your organisation?		
The more "YES" answers that appear for the business, the better outsourcing is suited to its needs.		
Full outsourcing of risk assessment: according to this approach, the entire risk assessment is performed by an external contractor. The assessment is based on a risk assessment approach that is chosen by the external contractor. The contractor can also undertake recurring future assessments. No know-how transfer to internal personnel is foreseen for the entire life cycle of the risk assessment/risk management of the MSB.		

Phase 1 -Risk Profile Selection


Phase 1
Risk Profiling
Identify Risk Areas
Use Risk Evaluation Matrix to mark applicable risk areas (Legal and Regulatory, Productivity, Financial Stability, Marketing) and risk levels (high, medium,low)
Risk Profile
Identify Business Risk Profile. Typically highest risk levels in risk classes define the overall business risk profile.

Consider the business risk aspects of information protection that can:

(a) result in legal and regulatory non-compliance,

(b) decrease productivity.

(c) create financial loss

(d) directly or indirectly affect or damage reputation and customer confidence,

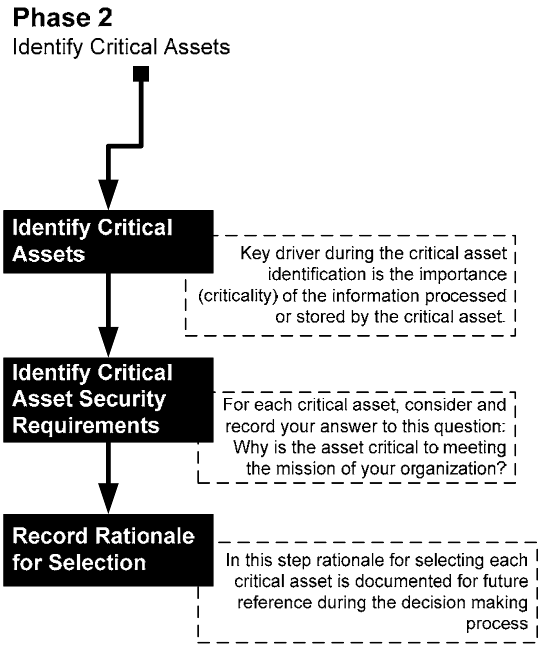
Select an appropriate risk level for each risk area using the risk profile evaluation table. The specified areas are the following: Legal and Regulatory, Productivity, Financial Stability, Reputation and Loss of Customer Confidence. As shown above, the phase involves two steps.

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.

To identify the current or potential risk level, highlight the risk area and read the description in each column. Risk areas that are closer to the business profile are chosen. The process is followed for every risk area. At the end there should be a MATRIX highlighting the applicable risk level in each risk area.

This page left blank

Phase 2 Critical Assets Identification


Phase 2
Identify Critical Assets
Identify Critical Assets
Key driver during the critical asset identification is the importance (criticality) of the information processed or stored by the critical asset.
Identify Critical Asset Security Requirements
For each critical asset, consider and record your answer to this question: Why is the asset critical to meeting the mission of your organization?
Record Rationale for Selection
In this step rationale for selecting each critical asset is documented for future reference during the decision making process

Phase 2 requires decisions that shape the remainder of the evaluation—selecting the business critical assets. Depending upon the size of the business, the number of information assets identified during this phase could easily exceed a hundred. To make the analysis manageable, MSBs 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 will be analysed during later activities. As depicted in figure one the phase involves three steps.

Step 1. Select your organisation's five most critical assets

When critical assets are selected, teams are not limited to choosing only five. Five assets are normally enough to enable organizations to develop a good set of mitigation plans during phase 4. However, analysis team members must use their judgement whether to use more or fewer than five. During the selection process of critical assets, team members should consider which assets will result in a large adverse impact on the organization in one of the following scenarios:

- **Disclosure** of information to unauthorized people
- **Modification** of information without authorization
- **Loss or destruction** of the asset
- **Interrupted access** to the asset or to the 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

Security Requirements Selection

Step 2. Identify Critical Asset security requirements

In general, when describing a security requirement for an asset, you need to understand what aspect of the asset is important. For information assets, security requirements will focus on the confidentiality, integrity, and availability of the information.

Security requirements can vary for different categories of assets within an MSB, but careful selection of requirements is critical for the controls selection task that follows. In other words, high availability requirements impose high availability controls etc.

You should use the **requirements selection criteria** as provided in order to identify most important security requirements. **Asset security requirements will be used later during the asset control card selection.**

The security requirements evaluation criteria have been developed as a simple and practical guide for evaluating the security requirements in terms of confidentiality, integrity and availability of the critical assets selected. The evaluation highlights the importance of the asset security attributes and indicates the appropriate controls for their protection.

As an output, you should have **a table listing critical assets along with a short description of their importance for the accomplishment of the business mission, its basic elements, and the security requirements**.

Asset Category	Confidentiality	Integrity	Availability
Systems	A system with confidentiality requirements often handles information with corporate proprietary information (R&D), customer base information, sensitive customer information of medical or personal nature.	Systems with integrity requirements typically handle transactions of financial nature, procurement of goods or e-commerce.	Availability requirements are encountered in systems that are critical to daily business operations and where downtime usually incurs costs and overheads in terms of resource allocation.
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 and shared metropolitan 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 organizational proprietary and confidential information that when disclosed can damage the organization's brand name and customer base.	Integrity requirements when people are concerned address shared secrets like cryptographic keys or 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 proprietary information (R&D), customer base information, sensitive customer information of medical or personal nature.	Applications with integrity requirements typically handle transactions of financial nature, procurement of good or e-commerce.	Availability requirements are met in applications that are critical to the business daily operations and where downtime usually incurs costs and overheads in terms of resource allocation.

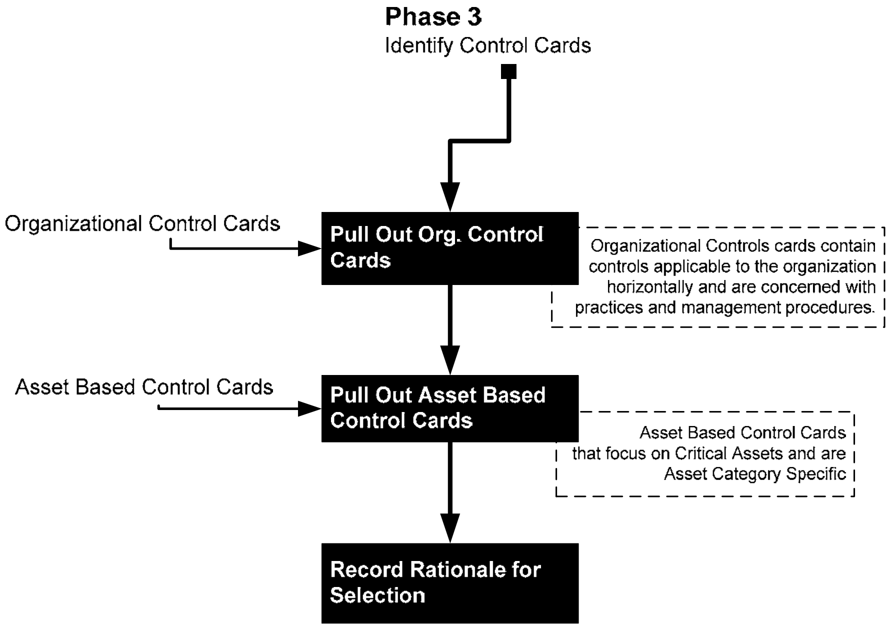
Step 3. Record the Rationale for selecting each Critical Asset

While selecting critical assets in step 1, a number of issues related to these assets are discussed. In this step the rationale for selecting each critical asset is documented for future reference during the decision making process. In addition, understanding why an asset is critical can better enable the definition of the security requirements during the next step. For each critical asset, the following questions should be considered and answers recorded:

- Why is the asset critical to meeting the mission of the organization?
- Who controls it?
- Who is responsible for it?
- Who uses it?
- How is it used?

These questions focus on how assets are used and why they are important. If answers to all of these questions are not provided, people in the organization who can provide the answers must be located and included in the analysis team. The information that is generated by answering these questions will be useful later in this process. In this regard, information gathered here must be carefully recorded.

Phase 3 - Control Cards Selection


Phase 3
Identify Control Cards
Organizational Control Cards
Pull Out Org. Control Cards
Organizational Controls cards contain controls applicable to the organization horizontally and are concerned with practices and management procedures.
Asset Based Control Cards
Pull Out Asset Based Control Cards
Asset Based Control Cards that focus on Critical Assets and are Asset Category Specific
Record Rationale for Selection

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**).

The following table assigns organisational controls to the risk profiles. Controls listed below are recommended in order to mitigate respective organisational risks.

There are 6 Organisational Control Cards as shown in the table to the right.

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

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

Asset-Based Control Cards Selection

Based on the risk profile and the asset security requirements MSBs assessment teams can use asset the control cards table below to identify the controls appropriate for the protection of critical assets.

Asset control cards are essentially grouped in three categories, corresponding to organisation risk profile, asset category and security requirement. For example assessment teams facing a high risk organisation profile will have different security requirements than medium or low risk profiles. Each control card involves a number of asset controls to address the complete range of risks and security requirements as needed in the particular profile and dictated by the selected security requirements.

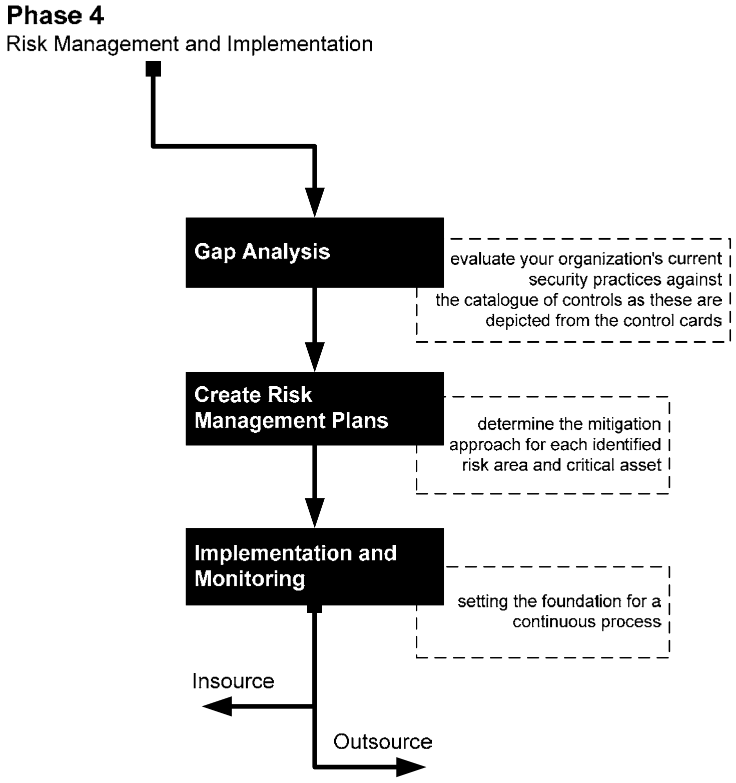
Assessment teams, using the previously identified security requirements and the control card can subsequently identify more specific controls (e.g. the controls for availability, confidentiality or integrity). It has to be noted that in cases where more than one requirement is selected, the controls that apply to the asset are the sum of the controls for each requirement.

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**

There are 12 Asset-Based Control Cards as shown in the table below.

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

Phase 4 -Risk Management and Implementation


Phase 4
Risk Management and Implementation
Gap Analysis
evaluate your organization's current security practices against the catalogue of controls as these are depicted from the control cards
Create Risk Management Plans
determine the mitigation approach for each identified risk area and critical asset
Implementation and Monitoring
setting the foundation for a continuous process
Insource
Outsource

During Phase 4 the MSB identifies actions and recommends an action list, setting forth the direction for security improvement. Essential for the successful implementation is the establishment of Senior Management (Decision Makers) sponsorship for the ongoing security improvement.

Step 1. Gap Analysis

Gap analysis is essential in order to improve how an organization handles information security, and establish the current state of security, that is, what is currently done well and where improvement is needed.

In this step, analysis teams are occupied with the evaluation of the organization's current security practices against the controls as these are depicted from the control cards. Analysis teams read carefully selected control cards and elicit detailed information about the organization's current security policies, procedures, and practices, thus providing a starting point for improvement.

During the Gap Analysis process teams use the control cards as the “requirements” and assess the gaps between these and current security practices both at an organizational and critical asset level. Analysis teams should carefully document output in two distinct plans – **(1) one for the organizational improvement** and **(2) one for the asset protection**.

The output from this process can form the basis for the planning activity that follows next. It is separated into two categories: **(a) Organizational Controls**, where the analysis teams should identify what they do and don’t do and define actions for improvement at an organizational level and **(b) Asset Based controls** where analysis teams assess existing protection measures for the identified critical assets.

Step 2. Create Risk Mitigation Plans

In this step MSBs have already identified critical assets, their organisation risk profile, the security requirements and have further selected appropriate controls and are about to determine the mitigation approach for each identified risk area and critical asset.

By taking these initial steps toward improvement, businesses can start to build the momentum needed to implement its protection strategy.

The output of this activity is the risk mitigation plan, which **leads to a series of steps** that a business can take to raise or maintain its existing level of security. Its objective is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern. Since a mitigation plan provides organisational direction with respect to information security activities, we suggest structuring it around the selected (phase 3) control cards (organisational and critical-asset-based).

Step 3. Implementation, Monitoring and Control

One of the principles of the risk assessment method is setting the foundation for a continuous process. This principle addresses the need to implement the results of an information security risk evaluation, providing the basis for security improvement. **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 in any improvement activity is maintaining the momentum generated during an evaluation. However, practical considerations will prevent most organizations from immediately implementing all of the initiatives after the evaluation. MSBs will likely have limited funds and staff members available to implement the protection strategy.

In **this step analysis teams prioritise the activities and then focus on implementing the highest-priority activities.**

Two distinct options are provided:

- **Risks accepting**. When a risk is accepted, no action to reduce the risks is taken and the consequences should the risk materialise are accepted.
- **Risks mitigating**. When a risk is mitigated, actions designed to counter the threat and thereby reduce the risk are identified and enforced.

Now that specific action items have been identified, analysis team members need to assign responsibility for completing them as well as set a completion date. Answers -- for each action item -- to the following questions must be reordered:

- Who will be **responsible** for each action item?
- What can management do **to facilitate** the completion of this action item?
- How much will it **cost**?
- **How long** will it take?
- **Can we do it ourselves?**
- **Do we need external assistance?**

NOTE:

The last two questions are critical **to whether a business can handle implementation** of the **necessary controls internally**. The answers to these are equally important and very hard to establish since both (outsource or in-source) have benefits and disadvantages.

Outsourcing is the **"make or buy" decision applied to the resource in question**. If it is done right, outsourcing can offer definite advantages. The main objectives for outsourcing are, besides support functions, cost-cutting, downsizing, and a desire to focus on the business (core competence). The lack of IT competence in the business can also be a reason for IT outsourcing. As IT is getting more important, companies frequently confront a wide disparity between the capabilities and skills necessary to realize the potential of information technology and the reality of their own in-house technology expertise.

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.

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.

System

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

Asset Based Control Card ID	CC-3S										
Risk Profile	Low										
Asset Category	System										
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		2.1.9			2.4.1						
Integrity					2.4.1						
Availability		2.1.6									

A low risk profile implies minimum level threats that entail potential system instabilities leading to unavailability of business service for a short period of time.

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

Impact of system unavailability does not affect organization reputation as information is neither private nor critical to the organization.

Unavailability of system does not affect quality of service or product.

Essential Control for the protection of confidentiality and availability in systems are 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 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.

OP2.1.9 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.

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.

Network

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, use of public key infrastructure, 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 in security advisories.

Network

Asset Based Control Card ID	CC-3N									
Risk Profile	Low									
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										
Availability										

A low risk profile implies threats that occur in minor network vulnerabilities or unavailability of information due to wrong or poorly-implemented network architecture. The impact however could be considered insignificant since information is not of great interest nor highly confidential for the organization. Therefore potential financial loss for the organization is small.

Nevertheless, security controls that address encrypted transferred information are recommended.

Essential Controls for the safeguard of confidentiality 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, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

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.

People

○ ● ○

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

○ ○ ●

Asset Based Control Card ID	**CC-3P**
Risk Profile	**Low**
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										
Integrity										
Availability	**1.1.4**									

A low risk profile implies potential threats with low impact on management of human resources when current security practices could lead to business problems but with a minimum risk for the organization.

Criticality of information is not of a high level. Thus, impact in financial terms is low and money loss can be considered as insignificant.

However, monitoring of staff policies even on such procedures further ensures the confidentiality, integrity and availability of information.

Essential Control for securing the confidentiality, integrity and availability of information in combination with people is the following:

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

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.

Application

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

○ ○ ●

Asset Based Control Card ID	CC-3A									
Risk Profile	Low									
Asset Category	Application									
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					2.4.2					
Integrity										
Availability										

A low risk profile implies storage and processing of public or internal information but with no critical level of importance that would entail more than a minimal loss of money. Organization reputation is not at stake. However, controls that would prevent even that kind of information leakage and that can secure the information life-cycle should be applied.

Furthermore, even if there is no confidentiality impact, information integrity and availability to every authorized user must be secured.

An essential control for confidentiality in the application asset is 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.

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.

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.

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

Action Checklist

☑	**Risk Profile Selection**	Consider the business risk aspects of information protection that can: (a) result in legal and regulatory non-compliance, (b) decrease productivity. (c) create financial loss (d) directly or indirectly affect or damage reputation and customer confidence,
☑	**Identify your Critical Assets**	Systems
		Network
		People
		Applications
☑	**Select Controls**	Assets
		Organisational
☑	**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 consider implementing passwords at the BIOS level on laptops.
☑	**Virus, Worms & Trojans**	Use anti-virus software 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 can be built into your operating system, or included as part of your router, make sure that yours is actually switched on and working.
☑	**Patches**	Keep all of 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 or CD
		Remotely via the Internet
☑	**Wireless Networks**	Ensure that the security is “turned on” so that unauthorised users can not access your network.

☑	**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 can not be read. Consider implementing this for laptops.
☑	**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. If you want to!
☑	**Remote Workers**	Increasingly remote workers are provided with PCs, and access to the corporate system via the internet. Ensure the data on their PCs is backed up and remote access is via a secure channel.
☑	**E-commerce**	If you have a web site that allows customers to order and pay for products ensure that this is secure.
☑	**Data Protection Act**	Understand your responsibilities under the DPA
☑	**Physical Security**	Don't forget that you probably 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. For it to be successful it is inevitable that some form of off site storage will be required.
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.		

IT Security Check

About your business	
Type of business.	
Retail	
Service	
Distribution	
Manufacturing	
Location	
High Street	
Industrial / Commercial business park	
Countryside	
Number of employees	
Number of sites/premises	

Onsite security:

Are the access points to your building secured?			
	YES	NO	Action Required
Doors/ Gates			
Locks			
Windows			
Skylight			
Emergency exits			

Is your company guarded?			
	YES	NO	Action Required
Porter			
Security service			
Alarm system			
Visual surveillance (e.g. webcam)			

Are there any secure areas in your building?			
	YES	NO	Action Required
Document archive			
Accountancy			
Cash box			
Safe			
Server room (server)			

Access to special and secured areas for certain groups of persons			
	YES	NO	Action Required

Is access to the building or parts of it logged?			
	YES	NO	Action Required
Document archive			
Accountancy			
Cash box			
Safe			
Server room (server)			

Do you securely dispose of critical material?			
	YES	NO	Action Required
Accountancy			
Logs, printouts			
Hard copy documents in general			
Computer and spare parts			

Do you dispose of storage media?			
	YES	NO	Action Required
Discs			
Hard drives			
CD, DVD			
Tapes			
Other			

Internal networks / WLAN

Do you operate an internal network?	YES	NO

Which technology do you use:	YES	NO
Windows		
Linux		
UNIX		

Do you have documentation for?			
	YES	NO	Action Required
Network connectors			
Connected computers			
Printers			
Modems			
Other devices			

Wireless networks / WLAN			
Which type:			
	YES	NO	Action Required
Access control / encryption available			

How do you control access/ connection to the network?			
	YES	NO	Action Required
Switch / patch			
Mac addresses			
Encryption			

Do you control connection of devices / computers to the network?			
	Open	Controlled	Action Required
Activate computers			
Create users and approved devices			

Are modems attached?			
	Open	Controlled	Action Required
Function of modems			
Configuration of modems			
Administration of access data for modems			

Do you have documentation about network architecture and components?			
	YES	NO	Action Required
Documentation up to date			
Roles and responsibilities defined			

Data Backup/Data Protection/Hard Copy Documents

How may PC do you use?	
Type/manufacturer:	
Operating system:	

Do you have a central file server?			
Type/manufacturer:			
Operating system			
	Employee	Third Party	Unknown
Server installation			
Server maintenance			
Scheduled?			
Configuration documented			

Are redundant mass storage devices in place?			
	YES	NO	Action Required / Planned
RAID			
Mirror server			
Backup / test server			

Where do you store paper documents?			
	YES	NO	Action Required / Planned
Office			
Archive			
External			

Are employees instructed to save electronic data on the fileserver?			
	YES	NO	Action Required / Planned

Do you use external drives?			
	YES	NO	Action Required / Planned
USB			
CD			
DVD			
Document server			

How do you archive electronic data?			
	YES	NO	Action Required / Planned
Office			
Archive			
External			

Is access control for files and data in place?			
	YES	NO	Action Required / Planned
User name/ password			
public/ private folders			
database access control			
other			
Responsibility for access control defined			
Administration access / user / passwords defined			
Compliance with directives checked			
Backup of application data			
Daily of more often			
Monthly			
Seldom			
Backup of applications			
Purchased standard applications			
Purchased custom applications			
Self produced applications			
How are data backed up?			
Standard applications			
Backup applications			
Self-produced system			
Is there an automatic backup?			
Responsibility for backup defined			
Backup data is checked			
Documentation available			
Which backup media are used?			
Disc			
Tape / type			
CD/DVD			
External drives/ removable hard drives			
Do you do backups to external servers via secure Internet connection?			
Do you do backups to external servers via secure Internet connection?			
Do you store backup media externally?			
External storage of backup media			
Access to external backup media			
Do you label backup media?			
Do you overwrite backup media according to a schedule (cyclical)?			
Storage of original media of licensed software			
External backup available			
Access to original media			
Access to original media is			

logged			
Installation of original media			
Licensed software			
Compatible to new hardware			
Check of license agreements			
Is there a regular re-check?			
Is the re-check documented?			
Backups older than 12 months			
Can they still be read			
Are they tested regularly			
Are they copied to new media			
Is the use of portable storage media like USB sticks or removable hard drives authorised?			
Do you have an emergency plan?			
emergency plan tested regularly			

Laptop / Mobile Devices

Do you use mobile devices?

	YES	NO	Action Required / Planned
Laptop			
PDA/ handheld			
Telephone with data interface			
Camera devices (mobile, PDA)			

Where do you use these mobile devices?

	YES	NO	Action Required / Planned
Office			
Home office			
On the go			

Is access control implemented?

	YES	NO	Action Required / Planned
User / password			
Encryption			
Mechanical access control			

What data is stored on mobile devices?

	YES	NO	Action Required / Planned
Copies of server data			
Private data			
Client information, etc..			

Documentation and registration of mobile devices and their usage

	YES	NO	Action Required / Planned
Hardware			
Software			

Internet connection

	YES	NO	Action Required / Planned
Do you have Internet connection?			
Responsibility for router defined			
Type of Internet connection			
Dial in			
DSL based broadband solution			
Cable-TV based broadband solution			
Wireless connection to provider			
Dedicated line			

Do you operate a firewall?			
	YES	NO	Action Required / Planned
Type / manufacturer:			
	Employee	Third Party	Unknown
Who has installed the firewall			
Who maintains the firewall			
	YES	NO	Action Required / Planned
Configuration documentation available			

Do you run your own mail server?			
	YES	NO	Action Required / Planned
Type / manufacturer:			
	Employee	Third Party	Unknown
Who has installed the mail server			
Who maintains the mail server			
	YES	NO	Action Required / Planned
Configuration documentation available			
Do you secure the mail server			

Do you use a proxy?			
	YES	NO	Action Required / Planned
Proxy filter installed?			
Do you run a web server?			

Malware

Operating System			
	Open	Controlled	Action Required / Planned
administrator rights on computer and server			
	Employee	Third Party	Unknown
Who is responsible for operating system updates?			
Regular updates			
	YES	NO	Action Required / Planned
Responsibility for license management			
Responsibility for installation and updates			

Applications			
	Open	Controlled	Action Required / Planned
	Employee	Third Party	Unknown
Who is responsible for application updates?			
Regular updates			
	YES	NO	Action Required / Planned
Responsibility for license management			
Responsibility for installation and updates			
Do you use security settings for applications			

Which anti-virus software do you use?			
	Open	Controlled	Action Required / Planned
	Employee	Third Party	Unknown
Regular updates			
	YES	NO	Action Required / Planned
Responsibility for license management			
Responsibility for installation and updates			
Are protocols analysed and discussed regularly			

Against what kind of malware is the system protected?			
	YES	NO	Action Required / Planned
Spyware/adware			
Server side protection against spyware possible?			
Spam			

Written Documentation of Directives / Protocol

	YES	NO	Action Required / Planned
Usage of computers in the company			
Treatment of data (personal)			
Hard copy documents			
Electronic documents			
Email correspondence			
	Open	Controlled	Action Required / Planned
What contents may be sent via email			
For which purpose may email be used			
Access to the Internet			
	Open	Controlled	Action Required / Planned
Who may use the Internet for what purpose			
How is private usage defined and authorised			
	YES	NO	Action Required / Planned
installation and configuration of computer systems documented			
How is compliance with directives checked			
Procedures for leaving employees			
Rules of conduct for employees e.g. if viruses occur			

Other

	YES	NO	Action Required / Planned
Is employee personal data treated according to the Data Protection Act			
Is client / supplier data treated according to Data Protection Act			

Software Application Checklist			
	YES	NO	Action Required / Planned
Internet Security Suite			
Operating system			
Anti-virus scanner			
Firewall/spyware/spam filter			
Office products			
Other software			

Notes

This guide has been developed by the International Association of Accountants Innovation & Technology Consultants (IAAITC) in co-operation with the European Network and Information Security Agency (ENISA), the Micro Entrepreneurs Acceleration Institute (MEA-I), and WKO- Information and Consulting Division.

The material in this guide reflected acknowledged best practice as at December 2007. This document is for educational and informational purposes only. Neither the IAAITC nor other contributing parties makes any warranties, express or implied, in this document.

Readers should consider taking appropriate professional advice before acting on any issue raised.