Information Security: Implementation Methodologies

LROBBERTZE[1], J.H.P. ELOFF[2]

[1]*lrobbertze@deloitte.co.za*
RAU Standard Bank Academy for Information Technology
Rand Afrikaans University, Johannesburg, South Africa
[2]*eloff@rkw.rau.ac.za*
RAU Standard Bank Academy for Information Technology
Rand Afrikaans University, Johannesburg, South Africa
July 2002
Tel: +27 11 489-2842 Fax: +27 11 489-2138

Key words: Information Security Management, Awareness, Accountability, Measurement, Reporting, Revision

Abstract: Information used by organisations is a valuable asset and has to be protected from the loss of integrity, confidentiality and availability. Information protection can be achieved through effective management, with meaningful board oversight. In an attempt to identify a generic methodology for the implementation of an information security management system, existing methodologies were investigated. This investigation highlighted the different aspects that would form an essential part of such a generic methodology.

1. INTRODUCTION

As the entire economy depends on the continuous operation of information technology, most organisations today share a common goal: The mitigation of risk to the Integrity, Confidentiality and Availability of their Information Resources.

In order for this goal to be reached and sustained in the minimum time and with the efficient use of a minimum amount of resources, a carefully structured methodology should be used. Much too often an ad-hoc approach is followed which will never reach its goal.

The chosen methodology should also be flexible enough so as to ensure that it can be adapted for any organisational circumstances.

The aim of this study is to find a generic methodology, which can be used by any organisation to ensure their information resources is secured in a sustainable way.

The remainder of the article is structured as follows:

2. A summary of the different existing methodologies.
   2.1 The BS7799 methodology
   2.2 The GAO methodology
   2.3 The Deloitte & Touché methodology
3. Generic methodology
4. Conclusion

2. EXISTING METHODOLOGIES WITH WHICH TO IMPLEMENT INFORMATION SECURITY IN AN ORGANISATION.

2.1 The BS7799 Methodology [BS7799]

2.1.1 Introduction

BS7799 (British Standard) – Part 2, specifies that an information security management system should be established through which the information assets of an organisation can be protected to the degree of assurance required.

The different steps in the framework have the goal of identifying, documenting, implementing and maintaining applicable controls and control objectives for the specific environment.

BS7799 presents the following framework as the minimum requirement to be used by any organisation wishing to implement an information security management system in their organisation.

2.1.2 Diagrammatic Representation

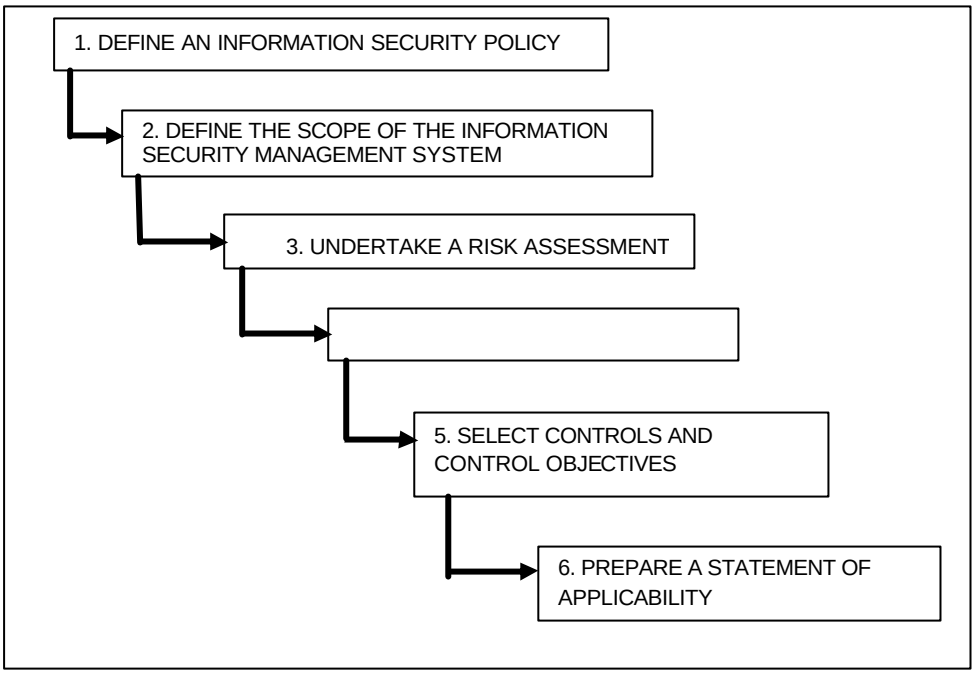


Fig 1: BS7799 Information Security Management System

2.1.3 Explanation

- DEFINE THE POLICY

The framework starts by defining an information security policy. Through this policy management will provide direction, and show support and commitment to the implementation of an information security program across the organisation. It is intended for this policy to be communicated throughout the organisation in a form that is accessible and understandable to the employees.

- DEFINE THE SCOPE OF THE ISMS

The next step establishes the scope of the information security management system for the particular organisation. An information security infrastructure is defined within the organisation. This infrastructure should comprise of the necessary fora through which to initiate and control the implementation of information security across the organisation.

The boundaries for the ISMS should also be defined in terms of all information assets, technologies and business units included. This would allow an organisation to reduce the complexity of information security management, by concentrating its security efforts on a predefined subset of their information resources.

- UNDERTAKE A RISK ASSESSMENT

The organisation should undertake a risk assessment to identify the threats to, and vulnerabilities of, the assets specified in the scope of this information security management system. The impact that these threats and vulnerabilities will have on the confidentiality, integrity and availability of the assets shall determine the degree of risk faced by the organisation.

- MANAGE THE RISK

The high-risk areas are now identified and the degree of assurance required for each of these areas is established – based on the defined information security policy.

- SELECT CONTROL OBJECTIVES AND CONTROLS TO BE IMPLEMENTED

Appropriate control objectives and controls must now be selected by the organisation from BS7799 – Part 1. The selection of controls should be justified.

- PREPARE A STATEMENT OF APPLICABILITY

The selected control objectives and controls, and the reasons for their selection shall be documented in the statement of applicability.

This document should also contain verification for controls (as specified in BS7799 – Part 1) that are excluded.

2.1.4 Comments

This is a typical top-down approach to information security management. Although this provides a very thorough way to manage information security in an organisation, a lot of time would lapse before the information assets of the organisation is secured. Technical activities, which could provide quick fixes, are only considered in step 5.

The only guidance given to maintaining the secure environment is the specification of records that should be kept. These records should indicate the organisational compliance to the selected controls. No guidance is given as to when a re-iteration of the whole framework would be required or how to establish the success of the control implementation.

The framework is specified only to serve as a guide for information security management and can therefore be adapted to organisational specific circumstances.

As this is a very high-level framework for an information security management system, organisations would still need expert advice on the implementation thereof.

2.2 **The GAO (United States General Accounting Office) Methodology.** [GAO]

2.2.1 Introduction

This methodology was derived from a study into the management practices of eight non-federal organizations in the United States that has been recognized as having strong information security programs.

2.2.2 Diagrammatic Representation

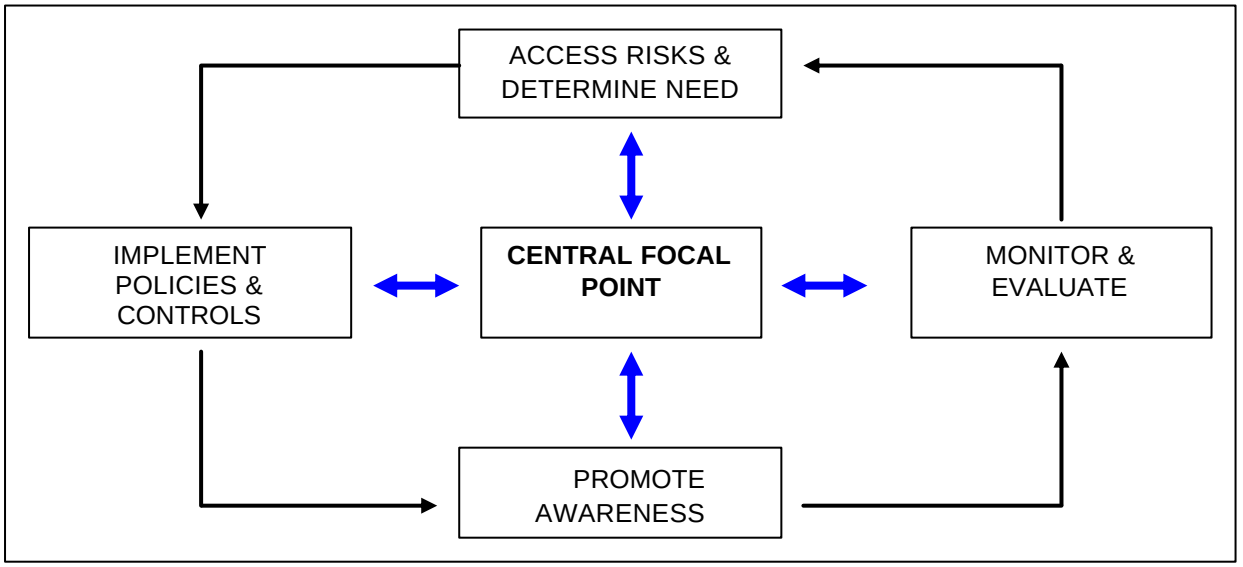


Fig 2: General Accounting Office Information Security Management

2.2.3 Explanation

Five management principles (phases) were identified and linked in a cycle of activity in order to ensure that information security policies addressed current risks on an ongoing basis.

- ASSESS RISK AND DETERMINE NEED

People with knowledge of business operations and technical aspects of systems should be involved in this phase. The result of this assessment should not be to exactly quantify risk, but rather to identify any control deficiencies needed in a business unit to mitigate the prevailing risks.

Business unit leaders should make a cost-benefit decision on whether to accept the risks responsibility or to implement the controls.

This gathered information could then also be used to educate management not only on needed resources, but also on how security can be used as a business enabler.

This is not a once off phase and should be repeated in an effort to identify new risks in the ever-changing environment.

- ESTABLISH A CENTRAL MANAGEMENT FOCAL POINT

A central group is designated to carry out the key activities of the security program. Their responsibilities stretches through all levels of the organisation and would include the following:

  - To independently voice security concerns to senior executives. This would ensure that management have thoroughly understood and considered all security risks, before the decision to tolerate /mitigate the risk, is made.
  - To ensure a consistent approach to security is followed throughout the organisation.
  - To define responsibilities for all groups involved and to dedicate staff to accept those responsibilities.
  - To ensure that the technical skills of all security managers and specialists are periodically updated.
  - To identify problem areas in the organisation and ensure that a weakness in one area doesn't place the whole organisation at risk.

- To ensure that all staff are aware of security risks and to clear up any policy misunderstandings.

- IMPLEMENT POLICIES AND CONTROLS

Policies are seen as a way for management to communicate their views on and requirements for specific business risk mitigation to all personnel. It should always be current and at a high enough level to be understood by all. It is the foundation of the security program and should form the basis for adopted procedures and technical controls.

Policies should be developed and distributed to all personnel by the Central Security Group.

- PROMOTE AWARENESS

The Central Security Group should continually educate all personnel on Information Security Risks and the related Policies using user-friendly techniques.

- MONITOR AND EVALUATE CONTROL EFFECTIVENESS

Monitoring is done to ensure that all Policies are still appropriate and that controls accomplish their purpose. The effectiveness of the controls defined by the Security Program will be monitored. Measurement results can be obtained from audit reports, network penetration tests and the use of specialised tools.

The results will be used to hold managers accountable and to direct the future efforts of the Security Program.

2.2.4 Comments

This methodology continuously revisits four security phases to ensure that all current risks are addressed. The management focal point ensures that the four cyclic activities are coordinated and focused.

The cycle of activities starts with a risk assessment and can therefore be time consuming when implemented for the first time. Resources are managed effectively through the use of the central management focal point.

This framework provides ample guidance on the implementation of a good information security management system. As this framework was

derived from those used by a few other organisations, it can be concluded that this information security management system is flexible enough to fit or to be adapted to any organisational environment.

2.3 The Deloitte and Touche Methodology

2.3.1 Introduction

This framework consists of four phases, each of which subdivided into 3 dimensions: People, Process and Technology. The four phases can be seen as a high-level cycle for activity.

Any of the four phases can be used as a starting point for information security management, as long as the other phases are visited sequentially thereafter.

2.3.2 Diagrammatic Representation

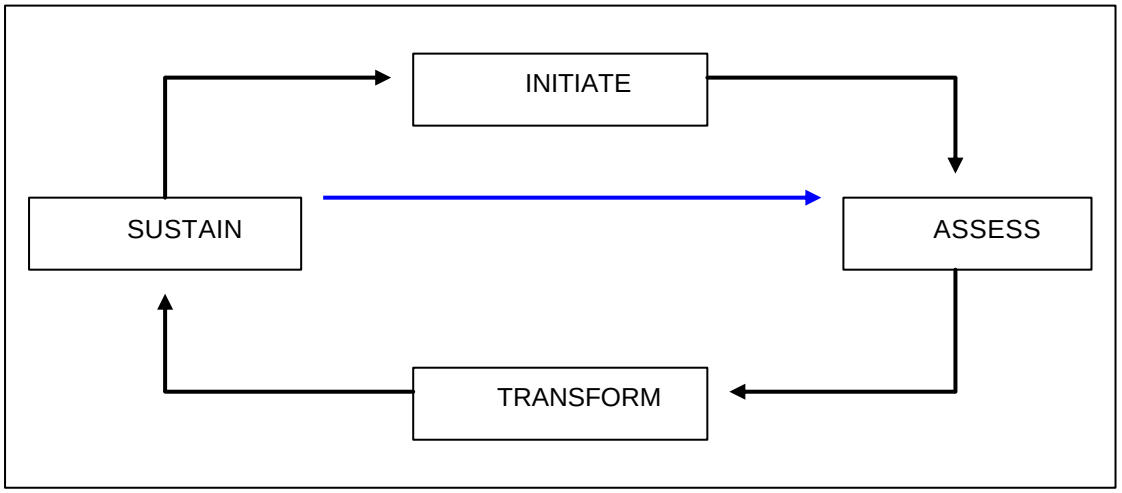


Fig 3: Deloitte & Touche Information Security Management System

2.3.3 Explanation

Activities within the different phases can be summarized as follows:

- INITIATE

This phase should establish the direction of the Security Program in the organisation. The activities listed in this phase should form the baseline for ensuring the maintenance of risk mitigation on a sustainable basis, as measurement of goal achievement is only possible with this baseline in position.

Activities for this phase should include:

- The identification of all stakeholders required for the implementation of the information security management system. This will ensure that the responsibilities and accountability for all the security activities can be allocated and monitored.
- To document the Statement of Management Intent. This will establish top management's direction on, and commitment to, information security and would take the form of a high-level information security policy.
- To establish an Information Security Forum and an Information Security Function. The Information Security Forum should review and agree on all deliverables from the Information Security Function. The Information Security Function should in turn manage information security within the organization. They would also be responsible for the coordination of training and awareness initiatives.

- ASSESS

This phase will measure the current status of Information Security within the organisation – the result of which should be the sum total of all efforts up to date. All the dimensions should be assessed in order to identify any enterprise risks that are not addressed effectively at present. In order to concentrate efforts, this assessment should only be done on the systems identified as most critical within the organisation.

Objectives for this phase should include:

- A criticality assessment with which to identify those systems that are at high risk or critical to business operations.
- An assessment of the organisational culture towards Information Security. The awareness of security issues as well the commitment to and capability for combating security risks are established.
- To do an assessment of the maturity of information security process control in the organisation.
- To determine the organisation's susceptibility to information security threats, by doing a technical vulnerability assessment.

- TRANSFORM

The goal of this phase is to modify the shortcomings in existing controls in an effort to mitigate risk effectively. A roadmap should be drawn up to guide the transition from the current, to the desired state of information security.

Objectives for this phase should include:

- To establish or revise the organisational awareness and education programmes so that every member of staff understands the importance if information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly.
- To develop or update the organisational issue-specific policies. This will ensure that top management's direction on, and commitment to, information security is documented and can be communicated to all individuals with access to the enterprise's information and systems.
- The review of current procedures / controls against best practice. This will ensure the correct and secure operation of the organisation's information processing facilities.
- To document Key Performance Indicators with which to measure the performance of the implemented information processes / controls and to identify opportunities for improvement.
- To address all identified technical vulnerabilities so as to minimise exposures to security threats.

- To document or revise current standards so as to ensure a consistent and current approach to securing network devices, applications and operating systems.

- SUSTAIN

To ensure a sustainable level of information security in an organisation the effectiveness of implemented procedures and controls should be closely monitored.

Objectives for this phase should include:

- To implement policy enforcement and monitoring mechanisms so as to ensure compliance thereto.
- To implement security tools and techniques so that security management and monitoring activities can be automated.
- To establish an Incident Response Capability that would identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

2.3.4 Comments

The division of the four phases into the different dimensions (people, process and technology) ensures that all possible issues of information security issues are addressed. It also provides a vehicle through which the activities within a certain phase can be implemented in parallel. This ensures that our goal for implementing an information security management system in the minimum amount of time, with all resources allocated efficiently, is realized.

As no specific starting point in the framework is enforced, this framework can easily be adapted to suit any organisational environment.

3. GENERIC METHODOLOGY

3.1 Introduction

This generic methodology has the following goals for the implementation of an information security management system:

- To be flexible enough so as to suit any organisational situation and requirements.
- To use the minimum amount of time
- To use the minimum amount of resources in an efficient way

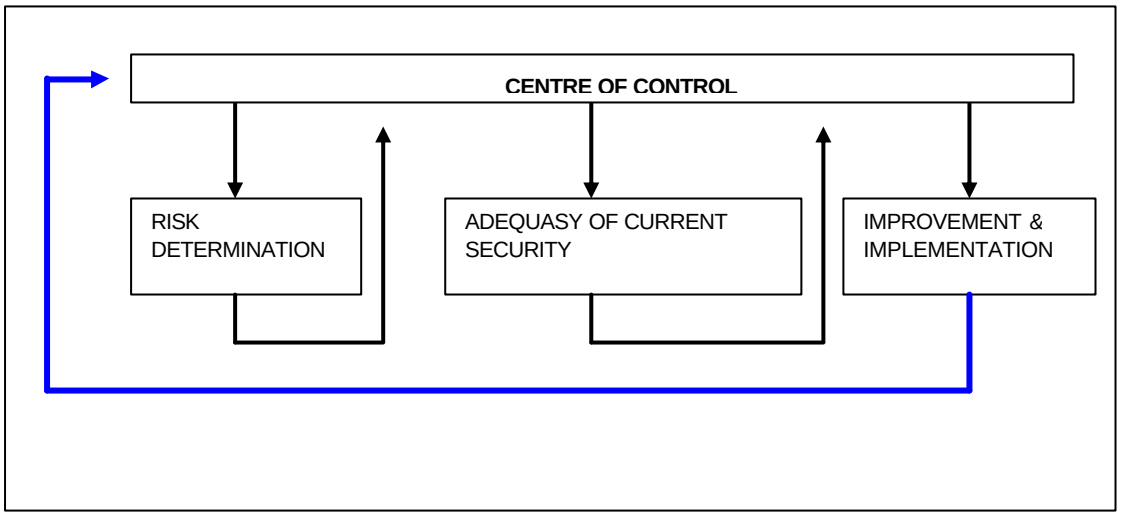
The following phases should exist within the generic methodology and should be controlled by a Centre of Control (The Centre of Control should be established when the information security management system is initialised.):

- Risk Determination
- Adequacy of Current Security
- Improvement and Implementation

The following issues have been identified as important to address:

- For an information security management system to be applied effectively across the organisation, commitment would be needed from all levels within the organisation. This can only be ensured if:
- All parties not only understand threats to information and information systems but also understand the mechanisms used to control these.
- All information security roles and responsibilities are clearly defined, and all parties have responsibilities for which they are held accountable.
- Information security controls should be proportionate to the impact that the identified risks will have on information and information systems.
- The effectiveness of the current information security management system should be frequently monitored and reported on.
- The information security management system should undergo constant revision.

3.2 Diagrammatic Representation



3.3 Explanation

This methodology is derived from all the above methodologies.

An overall requirement of this methodology is management's commitment to address information security risks.

- Management should document a Statement of Intent, which would demonstrate their commitment.
- Management should establish a Centre of Control to coordinate and report on the implementation of the information security management system across the organisation.

The phases used by this methodology comprises the following:

- RISK DETERMINATION
  - Current organisational risk and the impact thereof on the organisation's critical systems should be established by:
  - Measuring the compliance to controls already implemented to ensure risk mitigation. (Compliance should be measured against a preset benchmark value.)
  - Audit findings should be investigated
  - Risks not already assessed for impact on the organisations information and information systems should be identified.

- CENTRE OF CONTROL
  - Management should not only be informed of the compliance to the currently implemented controls but also of newly identified high-risk or problem areas.

- ADEQUACY OF CURRENT SECURITY
  - In order to decide whether additional controls should be implemented across the organisation, the effectiveness of current controls should be measured. This should be done for each of the following three levels:
  - People: The security awareness in the organisation should be established. This should highlight if roles and responsibilities have been communicated effectively and if people are held accountable for their actions.
  - Process: An analysis can be done of the maturity of the security implementation across the organisation. This should identify any processes that have not been documented and that are not measured for effectiveness.
  - Technology: A technical vulnerability assessment can be performed to identify any security holes that are not yet covered by the existing controls.

- CENTRE OF CONTROL
  - Controls needed for additional risk mitigation should now be identified and the cost of implementation calculated. This should be communicated through the centre of control to management.
  - Management should now decide whether the cost of the proposed controls is proportionate to the impact that to the organisation when the risk is realised. The goal and scope of the information security management system should be adapted accordingly.

- IMPROVEMENT AND IMPLEMENTATION
  - Policies should be revised to communicate management's decision on the implementation of revised controls.
  - Roles and Responsibilities should be revised where necessary.
  - Procedures and standards should be revised to support the implementation of the policies.
  - Metrics should be defined to measure the effectiveness of controls to be implemented. This would indicate if the security level as defined by policy is being achieved.
  - Training and awareness programs should be implemented to ensure that all personnel have the proper knowledge and skills required to take accountability for their responsibilities.
  - Once the policies, standards and procedures have been approved their implementation strategy should planned and signed-off.

- CENTRE OF CONTROL
  - The Centre of Control should coordinate the implementation of the identified controls according to the planned strategy to ensure a consistent approach towards information security management.

3.4 Comments

There should be a constant reiteration of the framework to ensure that the level of security across the organisation is improved.

All activities are guided by the Centre of Control, which will prevent ad-hoc approaches that waste time and human resources. The Centre of Control controls the time and resource usage by allowing different activities to run in parallel.

As Activities in different phases can be implemented at different time intervals, this framework can easily be adapted to suit any organisational environment.

4. CONCLUSION

An information security management system can only be implemented and enforced across an organisation if it is communicated as a management commitment.

Any information security management system will necessitate the use of different skills during the implementation of the various phases of the chosen methodology, and would therefore need the commitment from all personnel across the organisation.

To ensure that the current level of security is sustained in an organisation the used information security management system should be quantifiable and repeatable. It should also allow a sequential reiteration of the identified phases so as to enforce constant improvement.

During this study it has become apparent that security is a journey and not a destination.

5. LIST OF SOURCES CONSULTED

[BS7799] BS7799 Code of Practice for Information Security Management, BSI **1999**.

[GAO] GAO Executive Guide – Information Security Management May 1998