

RUSTENBURG LOCAL MUNICIPALITY



RLM INFORMATION SECURITY MANAGEMENT STRATEGY

TABLE OF CONTENTS

INTRODUCTION.....	2
PURPOSE AND OBJECTIVES.....	2
SCOPE.....	3
VALUE TO THE MUNICIPALITY.....	4
POLICIES, PRINCIPLES AND BASIC CONCEPTS.....	4
SECURITY GOVERNANCE.....	8
PROCESS ACTIVITIES, METHODS AND TECHNIQUES.....	9
TRIGGERS, INPUTS, OUTPUTS AND INTERFACES.....	12
INFORMATION MANAGEMENT.....	15

1. INTRODUCTION

Information security is a management process within the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved. It further ensures that the information security risks are appropriately managed and that enterprise information resources are used responsibly. Information security management provides a focus for all aspects of IT security and manages all IT security activities.

In this context, the term 'information' is used as a general term and includes data stores, databases and metadata.

Information security is a critical part of the warranty of a service. If the security of a service's information and information processing cannot be maintained at the levels required by the municipality, then the municipality will not experience the value that has been promised. Without information security the utility of the service cannot be accessed.

Information security management needs to be considered within the overall corporate governance framework. Corporate governance is the set of responsibilities and practices exercised by council and executive management with the goal of providing strategic direction, ensuring the objectives are achieved, ascertaining the risks are being managed appropriately and verifying that the enterprise's resources are used effectively.

2. PURPOSE AND OBJECTIVES

The purpose of the information security strategic plan is to align IT security with institution security and ensure that the confidentiality, integrity and availability of the municipal assets, information, data and IT services always matches the agreed needs of the municipality.

The objective of information security management is to protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity and availability.

For RLM, the security objective is met when:

- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is complete, accurate and protected against unauthorized modification (integrity)
- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)
- Municipal transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation).

3. SCOPE

The information security management process shall be the focal point for all IT security issues, and must ensure that an information security policy is produced, maintained and enforced that covers the use and misuse of all IT systems and services. Information security management needs to understand the total IT and municipality security environment, including the:

- Municipality security policy and plans
- Current municipality operation and its security requirements
- Future municipality plans and requirements
- Legislative and regulatory requirements
- Obligations and responsibilities with regard to security contained within SLAs
- The municipality and IT risks and their management.

Understanding all of this to ensure that all the current and future security aspects and risks of the municipality are cost-effectively managed.

Prioritization of confidentiality, integrity and availability must be considered in the context of municipality and municipality processes. The primary guide to defining what must be protected and the level of protection has to come from the municipality. Security Strategy addresses the entire municipality processes from end to end and cover the physical and technical aspects.

The information security management process include:

- The production, maintenance, distribution and enforcement of an information security policy and supporting security policies
- Understanding the agreed current and future security requirements of the municipality and the existing municipality security policy and plans
- Implementation of a set of security controls that support the information security policy and manage risks associated with access to services, information and systems
- Documentation of all security controls, together with the operation and maintenance of the controls and their associated risks
- Management of suppliers and contracts regarding access to systems and services, in conjunction with supplier management
- Management of all security breaches, incidents and problems associated with all systems and services
- The proactive improvement of security controls, and security risk management and the reduction of security risks
- Integration of security aspects within all other ITSM processes.

To achieve effective information security governance, IT function will establish and maintain an information security management system (ISMS) to guide the development and management of a comprehensive information security programme that supports the municipality objectives.

4. VALUE TO THE MUNICIPALITY

Information security management ensures that an information security policy is maintained and enforced that fulfils the needs of the municipality security policy and the requirements of corporate governance. It raises awareness of the need for security within all IT services and assets throughout the organization, ensuring that the policy is appropriate for the needs of the organization. It manages all aspects of IT and information security within all areas of IT and service management activity.

Information security management provides assurance of municipality processes by enforcing appropriate security controls in all areas of IT and by managing IT risk in line with municipality and corporate risk management processes and guidelines.

5. POLICIES, PRINCIPLES AND BASIC CONCEPTS

IT processes and initiatives must align with municipality processes and objectives. All processes within the IT organization must include security considerations.

Executive management is ultimately responsible for the organization's information and is tasked with responding to issues that affect its protection. In addition, Council is expected to make information security an integral part of corporate governance. IT function must ensure that they have a comprehensive information security management policy(s) and the necessary security controls in place to monitor and enforce the policies.

5.1 Policies

Information security management activities shall be focused on and driven by an overall information security policy and a set of underpinning specific security policies. The information security policy shall have the full support of top executive IT management and ideally the support and commitment of top executive municipality management. The policy shall cover all areas of security, be appropriate, meet the needs of the municipality and should include:

- Overall information security policy
- Use and misuse of IT assets policy
- Access control policy
- Password control policy
- Email policy
- Internet policy
- Anti-virus policy
- Information classification policy
- Document classification policy

- Remote access policy
- Policy with regard to supplier access to IT service, information and components
- Copyright infringement policy for electronic material
- Asset disposal policy
- Records retention policy.

These policies shall be widely available to all customers and users, and their compliance should be referred to in all SLRs, SLAs, OLAs, underpinning contracts and agreements.

The policies should be authorized by top executive management within the municipality and IT, and compliance with them should be endorsed on a regular basis. All security policies shall be reviewed - and, where necessary, revised - on at least an annual basis.

5.2 Risk assessment and management in information security management

Formal risk assessment and management relating to security of information and information processing is fundamental.

The information security management process shall frequently collaborate not only with the municipality but also with the ITSCM and availability management processes to conduct risk assessments at various levels. IT Unit with assistance of the Chief Risk Officer shall performing accurate assessment of risk and active management of risk to acceptable levels.

5.2 Information security management system

The information security management process will have a formal system to establish policy and objectives.

This system consist of:

- Information security policy and specific security policies that address each aspect of strategy, controls and regulation
- Security management information system (SMIS), containing the standards, management procedures and guidelines supporting the information security policies
- Comprehensive security strategy, closely linked to the municipality objectives, strategies and plans
- Effective security organizational structure
- Set of security controls to support the policy
- Management of security risks
- Monitoring processes to ensure compliance and provide feedback on effectiveness

- Communications strategy and plan for security
- Training and awareness strategy and plan.

The information security management system (ISMS) provides a basis for the development of a cost-effective information security programme that supports the municipality objectives. It will involve the four Ps of people, process, products (technology) and partners (suppliers) to ensure high levels of security are in place wherever it is appropriate.

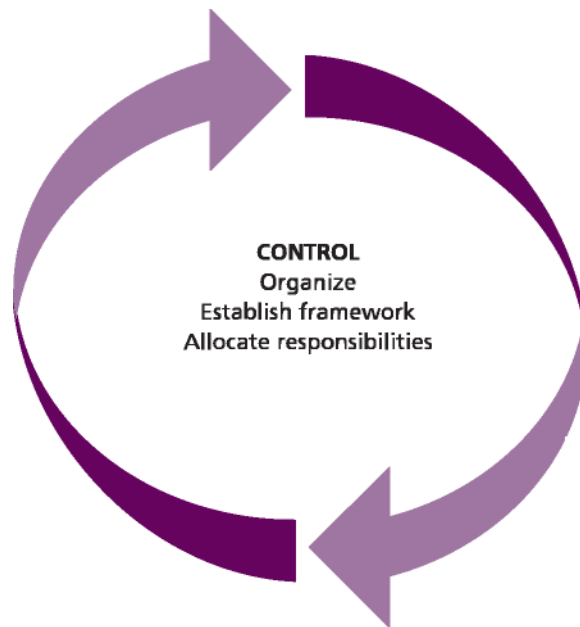
ISO/IEC 27001 is the formal standard against which RLM will seek independent certification of the ISMS (meaning the frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations).

MAINTAIN

- Learn
- Improve
- Plan
- Implement

PLAN

- Service level agreements
- Underpinning contracts
- Operational level agreements
- Policy statements



EVALUATE

- Internal audits
- External audits
- Self-assessments
- Security incidents

IMPLEMENT

- Create awareness
- Classification and registration
- Personnel security
- Physical security
- Networks, applications, computers
- Management of access rights
- Security incident procedures

The five elements within this structure are as follows:

CONTROL

The objectives of the control element of the ISMS are to:

- Establish a management framework to initiate and manage information security in the organization
- Establish an organizational structure to prepare, approve and implement the information security policy
- Allocate responsibilities
- Establish and control documentation.

PLAN

The objective of the plan element of the ISMS is to devise and recommend the appropriate security measures, based on an understanding of the requirements of the organization.

The requirements will be gathered from such sources as municipality and service risk, plans and strategies, SLAs and OLAs and the legal, moral and ethical responsibilities for information security. Other factors such as the amount of funding available and the prevailing organization culture and attitudes to security must be considered.

The information security policy defines the organization's attitude and stance on security matters. This shall be an organization-wide document, not just applicable to the IT function. Responsibility for the upkeep of the document rests with the information security manager.

IMPLEMENT

The objective of the implementation element of the ISMS is to ensure that appropriate procedures, tools and controls are in place to underpin the information security policy.

Measures include:

- Accountability for assets - service asset and configuration management and the CMS are invaluable here
- Information classification - information and repositories should be classified according to the sensitivity and the impact of disclosure.

The successful implementation of the security controls and measures is dependent on a number of factors:

- The determination of a clear and agreed policy, integrated with the needs of the municipality
- Security procedures that are justified, appropriate and supported by senior management

- Effective marketing and education in security requirements
- Mechanism for improvement.

EVALUATE

The objectives of the evaluate element of the ISMS are to:

- Supervise and check compliance with the security policy and security requirements in SLAs and OLAs, and in underpinning contracts in conjunction with supplier management
- Carry out regular audits of the technical security of IT systems
- Provide information to external auditors and regulators, if required.

MAINTAIN

The objectives of this maintain element of the ISMS are to:

- Improve security agreements as specified in, for example, SLAs and OLAs
- Improve the implementation of security measures and controls.

This will be achieved using a PDCA (Plan-Do- Check-Act) cycle, which is a formal approach suggested by ISO/IEC 27001 for the establishment of the ISMS.

6. SECURITY GOVERNANCE

Information security governance shall provide six basic outcomes:

- Strategic alignment:
 - Security requirements should be driven by enterprise requirements
 - Security solutions need to fit enterprise processes
 - Investment in information security should be aligned with the enterprise strategy and agreed-on risk profile
- Value delivery:
 - A standard set of security practices, i.e. baseline security requirements following best practices
 - Properly prioritized and distributed effort to areas with greatest impact and municipality benefit
 - Institutionalized and commoditized solutions

- Complete solutions, covering organization and process as well as technology
- A culture of continual improvement
- Risk management:
 - Agreed-on risk profile
 - Understanding of risk exposure
 - Awareness of risk management priorities
 - Risk mitigation
 - Risk acceptance/deference
- Performance management:
 - Defined, agreed and meaningful set of metrics
 - Measurement process that will help identify shortcomings and provide feedback on progress made resolving issues
 - Independent assurance
- Resource management:
 - Knowledge is captured and available
 - Documented security processes and practices, including explicitly defined the interfaces between ISM and other processes
 - Developed security architecture(s) to efficiently utilize infrastructure resources
- Municipality process assurance.

7. PROCESS ACTIVITIES, METHODS AND TECHNIQUES

7.1 Process activities

The information security management process will ensure that the security aspects with regard to services and all service management activities are appropriately managed and controlled in line with municipality needs and risks.

The key activities within the information security management process are:

- Production and maintenance of an overall information security policy and a set of supporting specific policies
- Communication, implementation and enforcement of the security policies, including:
 - Provision of advice and guidance to all other areas of the municipality and IT on all information security-related issues

- Assessment and classification of all information assets and documentation
- Implementation, review, revision and improvement of a set of security controls and risk assessment and responses, including:
 - Assessment of the impact of all changes on information security policies, controls and measures
 - Implementation of proactive measures to improve information security wherever it is in the municipality interest and cost-justifiable to do so
- Monitoring and management of all security breaches and major security incidents
- Analysis, reporting and reduction of the volumes and impact of security breaches and incidents
- Schedule and completion of security reviews, audits and penetration tests.

The developed information security management process, together with the procedures, methods, tools and techniques, constitute this security strategy. The security manager shall ensure that technologies, products and services are in place and that the overall policy is developed and well published. The security manager is also responsible for security architecture, authentication, authorization, administration and recovery.

Training and awareness shall be conducted every trimester.

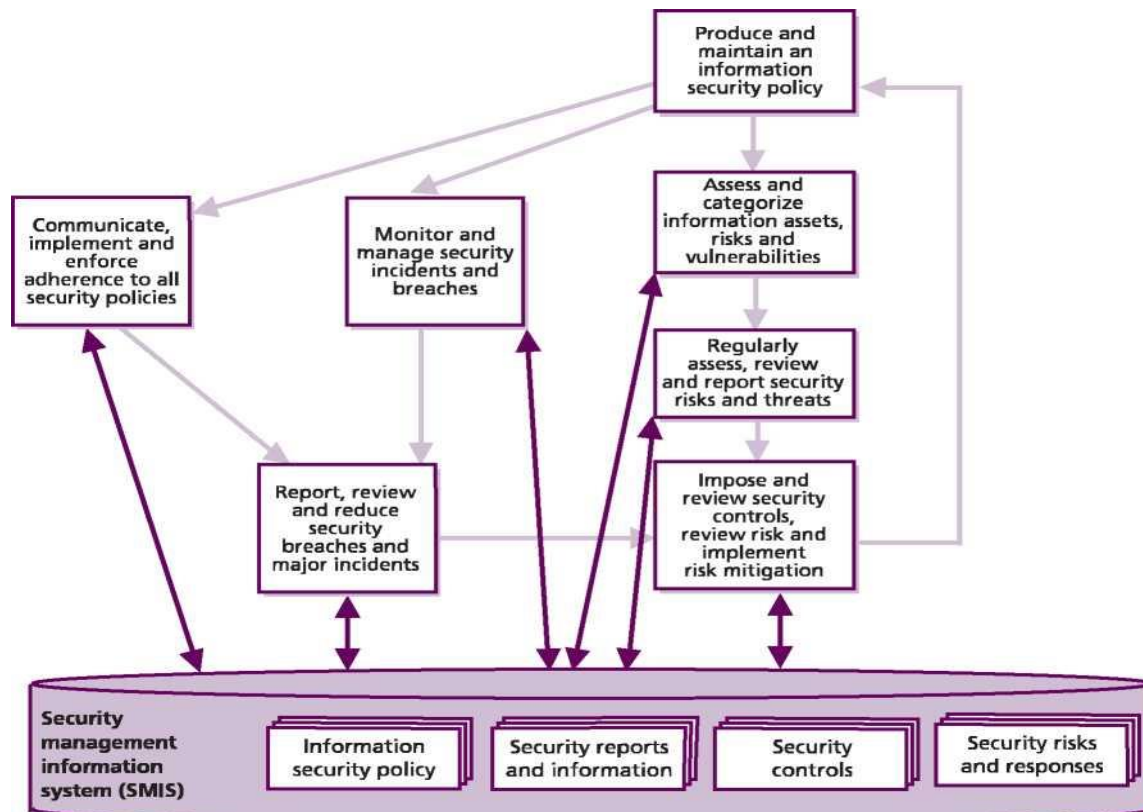


Figure: Information security management process

The set of security controls is designed to support and enforce the information security policy and to minimize all recognized and identified threats. The controls will be considerably more cost-effective if included within the design of all services. This will ensure the continued protection of all existing services and that new services and access to them are in line with the policy. The security controls and associated procedures for granting and preventing access to services by individuals will typically be executed on a day-to-day basis through the access management process.

Security measures will be used at a specific stage in the prevention and handling of security incidents, as illustrated. Security incidents are not solely caused by technical threats - statistics show that the large majority stem from human errors (intended or not) or procedural errors, and often have implications in other fields such as safety, legality or health.

The following stages will be identified:

At the start there is a risk that a threat will materialize. A threat can be anything that disrupts the municipality process or has negative impact on the municipality. When a threat materializes, we speak of a security incident. This security incident may result in damage (to information or to assets) that has to be repaired or otherwise corrected. Suitable measures will be selected for each of these stages. The choice of measures will depend on the importance attached to the information.

■ Preventive

Security measures will be employed to prevent a security incident from occurring:

Allocation of access rights to a limited group of authorized people

Control of access rights (granting, maintenance and withdrawal of rights), authorization (identifying who is allowed access to which information and using which tools), identification and authentication (confirming who seeking access is) and access control (ensuring that only authorized personnel can gain access).

■ Reductive

Measures will be taken in advance to minimize any possible damage that may occur. These are 'reductive' measures:

Making regular backups and the development, testing and maintenance of contingency plans.

■ Detective of security incident:

Monitoring, linked to an alert procedure, Antivirus/virus-checking software.

■ Repressive

Measures will be used to counteract any continuation or repetition of the security incident.

■ Corrective

The damages will be repaired as far as possible using corrective measures include restoring the backup, or returning to a previous stable situation (roll-back, back-out).

The documentation of all controls shall be maintained to reflect accurately their operation, maintenance and method of operation.

7.2 Management of security breaches and incidents

In the case of serious security breaches or incidents, an evaluation is necessary in due course, to determine what went wrong, what caused it and how it can be prevented in the future. However, this process is not be limited to serious security incidents. All breaches of security and security incidents need to be studied in order to gain a full picture of the effectiveness of the security measures as a whole. A reporting procedure for security incidents will be followed in order evaluate the effectiveness and efficiency of the present security measures based on an insight into all security incidents. This is facilitated by the maintenance of log files and audit files and, of course, the incident records from the incident management process. The analysis of these statistics on security issues should lead to improvement actions focused on the reduction of the impact and volume of all security breaches and incidents, in conjunction with problem management.

8. TRIGGERS, INPUTS, OUTPUTS AND INTERFACES

8.1 Triggers

Information security management activity can be triggered by many events, including:

- New or changed corporate governance guidelines
- New or changed municipality security policy
- New or changed corporate risk management processes and guidelines
- New or changed municipality needs or new or changed services
- New or changed requirements within agreements, such as SLRs, SLAs, OLAs or contracts
- Review and revision of municipality and IT plans and strategies
- Review and revision of designs and strategies
- Service or component security breaches or warnings, events and alerts, including threshold events, exception reports
- Periodic activities, such as reviewing, revising or reporting, including review and revision of information security management policies, reports and plans
- Recognition or notification of a change of risk or impact of a municipality process or VBF, an IT service or component
- Requests from other areas, particularly SLM for assistance with security issues.

8.2 Inputs

Information security management will obtain input from many areas, including:

- Municipality information from the municipality strategy, plans and financial plans, and information on its current and future requirements
- Governance and security from corporate governance and municipality security policies and guidelines, risk assessment and responses
- IT information from the IT strategy and plans and current budgets
- Service information from the SLM process with details of the services from the service portfolio and the service catalogue and service level targets within SLAs and SLRs, and possibly from the monitoring of SLAs, service reviews and breaches of the SLAs
- Risk assessment processes and reports from ISM, availability management and ITSCM
- Details of all security events and breaches from all areas of IT and ITSM, especially incident management and problem management
- Change information from the change management process with a change schedule and a need to assess all changes for their impact on all security policies, plans and controls
- CMS Containing information on the relationships between the municipality, the services, supporting services and the technology
- Details of partner and supplier access from supplier management and availability management on external access to services and systems.

8.3 Outputs

The outputs produced by the information security management process are used in all areas and shall include:

- An overall information security management policy, together with a set of specific security policies
- A security management information system (SMIS), containing all the information relating to information security management
- Revised security risk assessment processes and reports
- A set of security controls, together with details of the operation and maintenance and their associated risks
- Security audits and audit reports
- Security test schedules and plans, including security penetration tests and other security tests and reports

- A set of security classifications and a set of classified information assets
- Reviews and reports of security breaches and major incidents
- Policies, processes and procedures for managing partners and suppliers and their access to services and information.

8.4 Interfaces

The key interfaces that information security management has with other processes are as follows:

- Service level management Information security management provides assistance with the determining of security requirements and responsibilities and their inclusion within SLRs and SLAs, together with the investigation and resolution of service and component security breaches.
- Access management this process performs the actions to grant and revoke access and applies the policies defined by information security management and included in the service design by availability management.
- Change management Information security management should assist with the assessment of every change for impact on security and security controls. Also ISM may provide information on unauthorized changes that resulted from security breaches.
- Incident and problem management Information security management provides assistance with the resolution and subsequent justification and correction of security incidents and problems. The incident management process must include the ability to identify and deal with security incidents. Service desk and service operations staff must 'recognize' a security incident.
- IT service continuity management Information security management works collaboratively with ITSCM on the assessment of municipality impact and risk, and the provision of resilience, failover and recovery mechanisms. Security is a major issue when continuity plans are tested or invoked. A working ITSCM plan is a mandatory requirement for ISO/IEC 27001.
- Service asset and configuration management this will give the ability to provide accurate asset information to assist with security classifications. Having an accurate CMS is therefore an extremely useful information security management input.
- Availability management if data is unavailable or lacks integrity, then the ability of the service to perform its agreed function is compromised. This makes ISM a critical enabler of availability management. ISM is the process that is accountable for ensuring compliance with security policies in all services. Availability management is responsible for ensuring security requirements are defined and incorporated within the overall availability design. ISM operates collaboratively with both availability management and ITSCM to conduct integrated risk assessment and management exercises.

- Capacity management this must consider security implications when selecting and introducing new technology. Security is an important consideration when procuring any new technology or software.
- Financial management for IT services this should provide adequate funds to finance security requirements.
- Supplier management this should assist with the joint management of suppliers and their access to services and systems, and the terms and conditions to be included within contracts concerning supplier security responsibilities.
- Legal and human resources issues these must be considered when investigating security issues. Accordingly, ISM activity should be integrated with these corporate processes and functions.

9. INFORMATION MANAGEMENT

All the information required by information security management shall be contained within the SMIS. This will include all security controls, risks, breaches, processes and reports necessary to support and maintain the information security policy and the SMIS. This information shall cover all IT services and components, and needs to be integrated and maintained in alignment with all other management information systems, particularly the service portfolio and the CMS. The SMIS will also provide the input to security audits and reviews and to the continual improvement activities so important to all SMISs. The SMIS will also provide invaluable input to the design of new systems and services.

9.1 Critical success factors and key performance indicators

- CSF
 - Municipality is protected against security violations
 - KPI Percentage decrease in security breaches reported to the service desk
 - KPI Percentage decrease in the impact of security breaches and incidents
 - KPI Percentage increase in SLA conformance to security clauses
- CSF
 - The determination of a clear and agreed policy, integrated with the needs of the municipality
 - KPI Decrease in the number of non-conformances of the information security management process with the municipality security policy and process

- CSF
Security procedures that are justified, appropriate and supported by senior management
 - KPI Increase in the acceptance and conformance of security procedures
 - KPI Increased support and commitment of senior management
- CSF
Effective marketing and education in security requirements, and IT staff awareness of the technology supporting the services
 - KPI Increased awareness of the security policy and its contents, throughout the organization
 - KPI Percentage increase in completeness of supporting services against the IT components that make up those services
 - KPI Service desk supporting all services
- CSF
A mechanism for improvement
 - KPI The number of suggested improvements to security procedures and controls
 - KPI Decrease in the number of security non-conformance detected during audits and security testing.
- CSF
Information security is an integral part of all IT services and all ITSM processes
 - KPI Increase in the number of services and processes conformant with security procedures and controls
- CSF
The availability of services is not compromised by security incidents
 - KPI Percentage decrease in the impact of security breaches and incidents
 - KPI Percentage reduction in the number of incidents of service unavailability linked to security breaches
- CSF
Clear ownership and awareness of the security policies among the customer community
 - KPI Percentage increase in acceptable scores on security awareness questionnaires completed by customers and users.

9.2 Challenges

Ensuring that there is adequate support from the municipality, municipality security and senior management.

IT security controls and risk assessment and management will be severely limited in what they can achieve. It is pointless implementing security policies, procedures and controls in IT if these cannot be enforced throughout the municipality. The major use of IT services and assets is outside of IT, and so are the majority of security threats and risks.

Municipality perception is that security is an IT responsibility, and therefore the municipality assumes that IT will be responsible for all aspects of IT security and that IT services will be adequately protected. However, without the commitment and support of the municipality and municipality personnel, money invested in expensive security controls and procedures will be largely wasted and they will mostly be ineffective.

If there is a municipality security process established, then the challenge becomes one of alignment and integration. Information security management must ensure that accurate information is obtained from the municipality security process on the needs, risks, impact and priorities of the municipality and that the information security management policies, information and plans are aligned and integrated with those of the municipality. Having achieved that alignment, the challenge becomes one of keeping them aligned by management and control of municipality and IT change using strict change management and service asset and configuration management control. Again, this requires support and commitment from the municipality and senior management.

9.3 Risks

Gap between the need to protect systems and services and the degree of protection applied. The gap is caused by internal and external factors, including the widespread use of technology, increasing dependence of the municipality on IT, increasing complexity and interconnectivity of systems, disappearance of the traditional organizational boundaries, and increasingly onerous regulatory requirements.

This means that there are new risk areas that could have a significant impact on critical municipality operations, such as:

- Increasing requirements for availability and robustness
- Growing potential for misuse and abuse of information systems affecting privacy and ethical values
- External dangers from hackers, leading to denial-of-service and virus attacks, extortion, industrial espionage and leakage of organizational information or private data.

Because new technology provides the potential for dramatically enhanced municipality performance, improved and demonstrated information security can add real value to the organization by contributing to interaction with trading partners, closer customer relationships, improved competitive advantage and protected reputation.

It can also enable new and easier ways to process electronic transactions and generate trust.

Other areas of major risks associated with information security management include:

- A lack of commitment from the municipality to the information security management process and procedures
- Lack of commitment from the municipality and a lack of appropriate information on future plans and strategies
- A lack of senior management commitment or a lack of resources and/or budget for the information security management process
- The processes focusing too much on technology issues and not enough on the IT services and the needs and priorities of the municipality
- Risk assessment and management being conducted in isolation and not in conjunction with availability management and ITSCM
- Information security management policies, plans, risks and information becoming out of date and losing alignment with the corresponding relevant information and plans of the municipality and municipality security
- Security policies becoming bureaucratic and/ or excessively difficult to follow, discouraging compliance
- Security policies adding no value to municipality.