BEST PRACTICE

Information Security Management with ITIL® V3

Jacques A. Cazemier
Paul Overbeek
Louk Peters

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT management,
- Architecture (Enterprise and IT),
- Business management and
- Project management

VHP is also publisher on behalf of leading companies and institutions:
The Open Group, IPMA-NL, PMI-NL, CA, Getronics, Quint, ITSqc, LLC, The Sox Institute and ASL BiSL Foundation

Topics are (per domain):

IT (Service) Management / IT Governance
ASL
BiSL
CATS
CMMI
CobiT
ISO 17799
ISO 27001
ISO 27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL® V2
ITIL® V3
ITSM
MOF
MSF
ABC of ICT

Architecture (Enterprise and IT)
Archimate®
GEA®
TOGAF™

Business Management
EFQM
ISA-95
ISO 9000
ISO 9001:2000
SixSigma
SOX
SqEME®
eSCM

Project/Programme/ Risk Management
A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP™
PMBOK® Guide
PRINCE2™

For the latest information on VHP publications, visit our website: www.vanharen.net.

Information Security Management with ITIL® Version 3

Jacques A. Cazemier,
Paul Overbeek,
Louk Peters

Van Haren PUBLISHING

Colophon

Title:	Information Security Management with ITIL® V3
Series:	Best Practice
Authors:	Jacques A. Cazemier, Paul Overbeek, Louk Peters
Editor:	Jane Chittenden
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 552 0
Print:	First edition, first impression, January 2010
Design and Layout:	CO2 Premedia, Amersfoort-NL
Copyright:	© Van Haren Publishing, 2010
Printer:	Wilco, Amersfoort – NL

For any further enquiries about Van Haren Publishing, please send an e-mail to: info@vanharen.net

Contents

About the authors

Ing. Jacques A. Cazemier is Management Consultant at Verdonck, Klooster & Associates (VKA), an independent consulting company in the Netherlands.

Dr. ir. Paul Overbeek RE is partner with OIS Information Risk & Security Management and lectures at the universities of Amsterdam, Rotterdam and Tilburg.

Drs. Louk Peters is senior business consultant for Getronics Consulting, one of the founding organizations for ITIL.

Acknowledgements

In theory, there is no difference between theory and practice. In practice there is.

This book has been written to show theory and practice of dealing with Information Security Management. We share our experiences of aiding organizations in incorporating information security management. Those experiences would not have been possible without the continuous contributions from people who – just like us – are dealing with information risks on a daily basis.

We would like to thank the reviewers who provided valuable comments on the texts we had written. In alphabetical order they are:
Dr Gary Hinson, IsecT Ltd
David Jones, Pink Elephant UK
David Lynas, SABSA Foundation
Paul Peursum, DNV-CIBIT, The Netherlands
Rita Pilon, EXIN International
Dr Gad J Selig, University of Bridgeport, USA
Dr Abbas Shahim, Atos Consulting, The Netherlands
Takanori Tsukada, Hitachi Software Engineering Co., Ltd., Japan
Xander van der Voort, vanderVoort Projects, The Netherlands

Executive summary

Challenges

In recent years there have been developments that require more confidence in information and information processing. Those developments range from regulations and directives to pressure from stakeholders and from changes in use of technology to increased liability.

As organizations have become increasingly dependent on electronic delivery of services, the importance of maintaining high standards for information technology (IT) performance is increased as well. Information is one of the most important assets for business; sharing of information with other organizations adds to that importance.

Information is also becoming more vulnerable: it can deteriorate, it may fall in the hands of an unauthorized person, it may be corrupted, and it might not be available when needed. It is increasingly threatened by deliberate attack and by unintentional security incidents such as the loss of huge numbers of personal records stored electronically.

In addition, legislation and regulations mandate governance and compliance. Information security provides the basis for these aspects: assurance that information is reliable and information processing is sound. Information has to be provided to prove compliance. Add to that the need to manage IT costs and it is clear that maintaining the required level of information security is a major challenge.

Solutions

For IT, information and the power to process this essential asset is the core of its existence. Endangering information or its processing will immediately threaten the business. For that reason, securing information as well as the IT that processes it is an important subject.

Just maintaining the required level of information security is not sufficient. It is essential to have continuous security improvement to the level where risks are still acceptable. This does not stop at building more technology to repel threats or strengthening procedures. It also means managing the required level of security.

This book provides the background to enable adequate information security. It is an update of ITIL® (IT Infrastructure Library) version 2 Security Management book [CAZ] and fits within the ITIL version 3 service lifecycle. It also makes reference to international standards like ISO/IEC 20000 and ISO/IEC 27001. ITIL® is a registered trademark of the UK Office of Government Commerce.

This book describes Information Security Management with ITIL version 3 and builds on the ITIL version 3 processes and activities that are required to manage IT effectively.

Results

The benefits of sufficiently secure information extend to the entire business, from corporate image and position in the market to effectiveness and efficiency. It provides inherent flexibility: because information and IT security is controlled, robustness and reliability are ensured. Demonstrable compliance and continuous adherence to regulations form the basis for all business processes that require use of information and information processing.

Information Security Management gives IT resilience to survive, whatever the storms that threaten the business.

1 Introduction

1.1 This book

Information security is one of the subjects with wide coverage on the Internet. Texts on improving security, as well as breaching security, are just a few clicks away. This phenomenon is one of the reasons that maintaining information security is such an important subject: ignorance of your own information security is an open invitation to serious problems in everything that your information is used for. Without continuous effort to maintain an adequate level of protection, all investments in reliable information processing will lose their value and processes dependent on trustworthy information will fail.

Information security is an essential requirement for organizations that use and rely upon information since information is a volatile corporate asset. Commonplace security risks to information assets include:

- fraudsters inside or outside your organization who exploit missing or weak process controls for personal advantage
- theft or unauthorized disclosure of proprietary or personal data (e.g. industrial espionage, inappropriate web publication)
- human errors and omissions by information users, system/network administrators and operators (e.g. inaccurate or incomplete data entry, mis-configuration of technical security controls)
- malware – malicious software such as network worms and Trojan horse programs
- hackers who deliberately attempt unauthorized access to systems
- technical vulnerabilities arising from programming errors and design flaws in computer software, firmware and hardware (bugs and so forth)
- physical damage or loss of IT equipment and information storage media arising from storms, floods, lightning, sabotage, accidents and thefts.

In the ITIL context, many of these risks are likely to affect the organization's provision of IT services unless suitable information security controls are in place. However, information security controls require resources to design, implement, manage and utilise, hence management needs to strike a balance based on the costs and benefits of security.

Management effort is required in order to maintain the required level of security. Since information security is not limited to one aspect of technology, personnel or process, management will need to have relationships with all processes in the organization. The consequence is that Information Security Management needs to be part of every process. In this book, Information Security Management is shown to be present in all phases of the lifecycle of ITIL version 3.

1.1.1 Context

This book is an update of the ITIL book Security Management, which is a title in the ITIL version 2 series. The reason for this update is twofold: it reflects the updates of ITIL version 3 and it adds new developments and changes to the previous version.

The update consists of:
- explaining the most important changes of ITIL version 3, as far as information security management is concerned
- incorporating the changes to Information Security Management as a result of updated standards and best practices
- describing new trends in information security and its management
- highlighting the increased importance of outsourcing and service orientation
- focusing on business aspects and practices.

In this book, Information Security Management is covered from setting the initial security objectives to implementation and maintenance. It shows the relationships to all processes and activities that interface with information.

Information Security Management is a management process. It is not restricted to information technology. It is not sufficient to limit information security management to computers, networks and software. Information on other media – like paper – will have to be protected as well. It is not restricted to people; and it is not restricted to processes. For example, countermeasures for threats to information security will be found in areas as diverse as organizational architecture, human resources, computer hardware and software, physical access to buildings and supply of electrical power.

Taking ITILv3 as the starting point also gives some limitations. The focus of Information Security Management in this context is more on information, IT and business alignment and less on topics that are also relevant for security including legal aspects, organizational change, HR management and facilities.

Target audience
This book is intended for IT managers and business managers who are looking for practical directions to maintain Information Security Management. It may also be useful to business process managers to understand what Information Security Management is about.

1.1.2 Best practice
The value of this book lies in its character as best practice. It integrates current standards and best practices. It is not a standard that would be used for a certification process, it is not a regulation to be followed to the letter. It provides ideas and experiences that may or may not be appropriate in your situation. We believe that the overall advice in this book is useful in the majority of cases; however, it may need to be adapted to your organization's situation.

The book enables comparison of experiences and informed discussions about implementation of Information Security Management. In addition, it may serve as a benchmark when organizations are comparing their efforts in this field.

1.1.3 The subject
Information security management is the process to ensure that both information and information processing is (and remains) reliable, confidential and available when and for whom it is required. It limits access to information and information processing to authorized people and functions.

Information Security Management deals with establishing and maintaining all that is needed to keep that required level of information security.

The basis for this required level is the specification of information security in the Service Level Agreement that has been agreed between the business and the service provider.

The goal of Information Security Management is to provide confidence and assurance to the business that the business assets are protected and the overall security process supports the business mission. Security has long been seen as a subject for the IT department, with much emphasis on technology. Solving business problems was never considered as a reason for security measures. Although the introduction of the standard BS7799 (later ISO/IEC 27002) made it clear that security is about more than technology alone, in practice we still see a silo approach towards security, so that security restricts business processes and even sometimes becomes a showstopper or restraint.

With a 'guard-dog' attitude, IT departments used to think that a secure IT infrastructure could only be established by just enforcing more rules, more and longer passwords, more limitations on access, more firewalls and the like. This approach has given security a bad reputation, sometimes called 'the business prevention department'.

Security is not an end in itself but a property relative to a specific (business) context. What is good for one organization does not necessarily have to apply to another. For others, there will be other risks. There is a definite need for 'tailored security'.

How to define and reach the required level of security – that is, how to determine which control objectives are needed and what controls are to be put in place to reach the required level of security – is one part of Information Security Management. It contains topics such as establishing the proper business requirement for information security, risk analysis, defining control objectives, the definition of the right countermeasures, creating a standard minimum level of information security, the implementation of controls and operational monitoring such as intrusion detection.

The other part of Information Security Management deals with maintaining information security at the required level and providing appropriate assurance. Security maintenance topics are incident registration and handling, trend analysis and reporting, escalation support, access management, hardening, maintaining standards, etc.

The first part, defining and reaching the required level of security, is performed first. When information security is 'in place', operational and functioning, the second part (maintaining the required level) is a continuous effort as part of the lifecycle. The activities are essentially the same as for the first part, but become progressively better informed by metrics and experience of the operational security management system. Of course, the requirements for security have to be maintained as well. These are not static since both the importance of information as well as the threats in the ever-changing IT and organizational infrastructure vary.

The Information Security Management process coordinates and directs the security activities, using a standard process management cycle.

This book's primary focus is the Information Security Management system, which resembles a normal management process like that of the ISO 9000 series of standards. This management system maintains the required level of security, reacts to problems and improves controls and countermeasures and security management itself if necessary.

Since Information Security Management has relationships with almost all other management processes and is part of many organizational activities, it is impossible to operate information security as a standalone process. The relationships to other processes and the management activities required to maintain an overview of information security are the main subjects of this book.

Managing information security has become a critical business issue. Compliance dictates demonstrable control and auditability, for which Information Security Management is mandatory. Proving that the organization is in control of its information security is high on every business's agenda – or should be.

1.1.4 Trends in information security

Information processing and the required technology are changing in ways that are increasingly rapid and complex. The Internet and its services have become part of our social and business structure. This creates challenges when implementing hardware and software infrastructure (and subsequent infrastructure), administration, management, maintenance and support. Keeping up to date with security adds to that burden. This paragraph sketches just a few of the many developments that affect information security today.

A particular challenge is created by the fact that every security flaw that is ever found is published on the Internet. Add to this the availability on the Internet of construction kits for all kinds of malicious programs to exploit these flaws. Keeping up with and responding rapidly to the continual flow of security bulletins, patches and updates are more essential than ever.

Fortunately, security awareness is improving and products are being designed with more security technology built in. Initiatives such as sourcing and Service Oriented Architectures are stimulating professionalism in service and system management and are promoting the use of tools to support Information Security Management.
Suppliers are providing more or less integrated security embedded in their management tools, which allows centralized monitoring and resolving of security aspects. Networks, databases and applications, access and asset classification management systems are increasingly integrated, leading towards enterprise wide IT management.

The world of digital communication, the Internet and doing business through networks is now part of our society. Unfortunately, the criminal world has discovered that substantial profits can be made by fraudulently manipulating business on the Internet. Identity theft is a new form of robbery. Cyber crime is rising. Pressure on information security countermeasures is increasing. This means that Information Security Management – to maintain the required level of security – is becoming ever more important.

In line with the increased focus on governance, control of information security is becoming much more important as a management issue. At the same time, the legal aspects of information security are receiving more attention. Management needs to be in control, and that has to be demonstrated; as a result, monitoring is being given more attention. Starting with monitoring the security operations, attention evolves towards Information Security Management monitoring. Performance 'dashboards' provide information on security status, tuned to the needs of different levels of management.

The world is evolving into an environment where all kinds of information systems are connected. Organizations operate in networks, which has an impact on information security. 'The chain is only as strong as the weakest link' is a very valid expression. In particular, the IT interfaces between organizations are well known as weak points. Too often, this is treated as a technological problem. The human aspect is vulnerable to social engineering [MIT] and adequate processes to manage the connections across these borders are known to be weak links. Indeed, Information Security Management across the borders of organizations will be the main challenge for many years to come.

Information systems are linked not only through professionally managed corporate networks, but also through 'user managed' or amateur home networks, private media centers, vending machines, etc. Technically, household appliances can be controlled using the Internet. This implies that information security has to be integrated in all those functions. The idea that information security is limited to fencing the company's owned infrastructure is obsolete. Information is accessible via an increasing number of channels, some controlled by the organization itself, some managed by a third party or even by the users itself. This is described by the Jericho Forum [JER] as the problem of de-perimeterization or perimeter erosion. The huge explosion in business collaboration and commerce on the Web means that today's traditional approaches to securing a network boundary are at best flawed, and at worst ineffective. Examples include:

- business transactions that tunnel through perimeters or bypass them altogether
- IT products that cross the boundary, encapsulating protocols within Web protocols
- security exploits that use email and Web to get through the perimeter.

Information security increasingly requires attention from more than just IT – not only technology, but also public and political acceptance of the use of technology.

Identity theft has increased dramatically over the last few years. This includes 'phishing' attacks, which are aimed at obtaining personal information for fraudulent activities (e.g. whose fictitious premise might lead to the closing of a given bank). Similarly, attacks may deploy other types of fraudulent activity with an economic impact, such as emails that promise easy access to funding for mortgages or refinancing. All types of organizations, profit or non-profit, have to deal with these new types of crime. Millions of Internet users have their identities stolen each year. The consequences of identity theft can be traumatic. For identity theft victims it may cost a great deal of money and many days repairing the damage to their good name and credit record. For organizations facing fraud it means direct and indirect financial loss or loss of public image. It also may mean that information stored in customer databases may become corrupted.

Identity management systems may be considered, but there are trade-offs. On the one hand, access rights and separation of duties are easier to manage centrally; on the other, it may increase vulnerability by having a centralized access point to identity information and processing.

Online and real-time auditing and vulnerability monitoring are now possible. Combined with upcoming techniques for monitoring and filtering, more effective Information Security Management is possible to a much greater extent than previously. Supporting standards, like ISO/IEC27004, help to provide more awareness of the status of information security.

Governments depend on technology to implement policies. For example, public sector organizations are using biometrics and radio frequency identification (RFID) tags in passports, centralized records and administration and chip cards for identification, payment, authentication procedures and storage of certificates. Unfortunately, there are many examples of too much haste during implementation, subsequently revealing the results of ad hoc solutions.

Long-term vision is required to achieve the right balance of the effects of timely implementation and incorporating lasting security. Transparency, the scope of use, access rights to the underlying system and democratic control are but a few of the aspects that will have to be considered. The requirements for information security have never been so important as now. Failure to integrate security could have major political impact.

There is also the explosion of malware variants, where malware consists of malicious software designed to infiltrate or damage a computer system: recent attacks include new strains of malware that consist of millions of distinct threats that propagate as a single, core piece of malware. This creates an unlimited number of unique malware instances.

As the number of available Web services increases and as a large number of browsers continue to support the unsafe use of scripting languages, we can expect the number of new Web-based threats to continue to increase.

We see an increase in activity from threats related to social networking sites. These threats have involved 'phishing' for username accounts or using social context as a way to increase the 'success rate' of an online threat. Spammers, sending unsolicited junk mail (spam) in selected European, Middle Eastern and African regions have been heavily promoting social networking sites. These threats will become increasingly important for IT organizations since staff often access these tools using corporate resources.

Virtualization technology will be incorporated into security solutions to provide an environment that is isolated and protected from the chaos of a general-purpose operating system environment. This technology will provide a safe environment for sensitive transactions such as banking and protect critical infrastructure such as the security components that protect the general purpose operating environment. However, virtualization is just as much a threat as a benefit to security. Hackers are actively employing mechanisms to subvert and compromise virtual environments.

Malicious attackers have changed their approach. Examples of social engineering attacks are almost too numerous to mention, but a few of the most popular are: fake codecs, instant

messaging spreading malware (which appears to be from a known contact) contains a link to a malicious website or malicious file, malicious content on peer-to-peer networks (which claims to be a popular application, video, or music content, but is actually just malware) and so on.

With the Internet, users want services anytime, any place. With cloud computing we offer the ability to work on documents from almost anywhere. This is convenient, but also represents a potential risk to your security and privacy. If you, as a user, can access your documents and sensitive data from anywhere, then so can people with malicious or criminal intentions, if they can guess your password or find a security weakness in the Web-based application. The physical computers that these services reside on are also a very attractive target – if criminals can break into a computer room and steal some of the servers, they will potentially have access to thousands of people's information.

Last but not least, other emerging trends worth mentioning are:
- a growing focus on compliance, accountability, governance, demonstrable security, assurance and audit ability – the whole assurance question
- more emphasis on information rather than IT security
- more professional education of workers in the field through CISSP, CISA, CISM, SABSA, SANS, GIAC etc.
- designing the management of information security as a coherent, comprehensive and cost-effective management system, itself aligned if not integrated with other management systems (e.g. ISO/IEC 20000 and/or ITIL, ISO 9000 etc.)
- greater emphasis on physical, procedural, legal, compliance, policy and awareness controls etc. in addition to technical security controls
- organizations seek much more standardization and have a growing interest in certification.

1.1.5 Structure of this book

This book contains five major chapters; the annexes provide additional background information.

Chapter 2: Fundamentals of information security – to provide insight and give background about what is going to be managed. Topics such as types of security controls, business benefits and the perspectives of business, customers, partners, service providers, and auditors are covered.

Chapter 3: Fundamentals of management of information security – to explain what information security management is about and its objectives. Details are also given on implementing generic Information Security Management and the continuous effort required to maintain its quality.

Chapter 4: ITIL version 3 and Information Security Management – shows the links with the other ITIL processes. It builds on existing processes and activities as much as possible. By integrating the Information Security Management activities into existing processes and activities, the additional efforts are reduced as much as possible, keeping responsibilities where they should be. Effective Information Security Management is mainly achieved through coordination and allocation of activities within other processes.

Chapter 5: Guidelines for implementing Information Security Management – gives practical advice how to put Information Security Management into practice. From awareness in the organization via documentation required to maturity models; this chapter aims to describe best practices for realizing Information Security Management.

In the annexes of this book, more information is given about standards and other best practices. These standards all use different starting points but deal more or less with the same subject; this allows you to choose the right framework for your organization's needs.

1.1.6 Website

The websites www.itilv3ism.nl and www.vanharen.net provide additional background information on Information Security Management with ITIL v3. The websites are also available to provide feedback and share good practices.

2 Fundamentals of information security

This chapter describes information security from the perspective of the different stakeholders. These stakeholders include the business, customers, partners, regulatory parties, auditors and those responsible for oversight as well as the perspective of management of the IT infrastructure.

Information and information processing are crucial to support business processes. Nowadays IT not only supports the business but also acts as an enabler for generating new business (e.g. the opportunities offered by the Internet). Each organization has to deal with an ongoing stream of changes in the business and its environment, causing changes in security requirements as well. To manage these changing requirements, information risk and security management is an integral part of all business processes. With the right security, the business objectives are supported and their achievement is assured, even when internal or external negative influences occur or if the IT fails.

The growing dependency on information and IT (and rapid development of the supporting technology), necessitate a proper management of current and future security controls that reflect the ever-changing risks and security requirements. This management activity is referred to as Information Security Management.

The objective of Information Security Management is to align information security, including IT security, with the business requirements for security and ensure that information security is effectively managed in all service and Service Management activities. IT security is a subject within information security. IT security is targeted more towards all IT technical components, including application, servers, networks, firewalls, etc) whereas information security addresses the wider scope of the information itself.

2.1 Perspectives on information security

An organization has implicit and explicit objectives. Business processes take place in an organization in order to achieve these objectives. In executing these processes, the organization is increasingly dependent on a well-functioning information management; organizations are increasingly dependent on IT services to meet their business needs. In this context, information security is not a goal in itself but a means of achieving the business objectives. Figure 2.1 shows the different perspectives on information security.

How information management is organized depends on the type of organization and the nature of the products or services it delivers in support of its business processes. The organization collects data in order to make products or supply a service. The data is stored, processed and made available when it is needed. Those people concerned have to be able to rely on its integrity; and it is equally important to ensure that only those who are authorized to do so can gain access to this information. Confidentiality, integrity, and availability should be expected as normal conditions of business operations and should not be open to discussion. An organization must

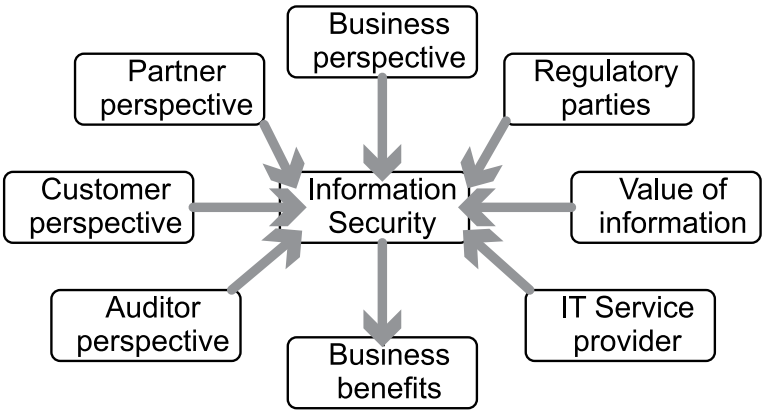

Figure 2.1: Different perspectives on information security

therefore organize the collection, storage, handling, processing and provision of information in such a way that these conditions are satisfied.

Information security exists to serve the interests of the business or organization; it is also relevant for other stakeholders with an interest in security – for example, individual data subjects or the authorities responsible for compliance obligations. Not all information and not all information services are equally important to the organization. The level of information security has to be appropriate to the importance of the information. This 'tailored security' is achieved by finding a balance between the security controls and their associated costs on the one hand and, on the other, the value of the information and the risks for the business in an information processing environment. Security in information systems can provide important added value. After all, having the right security for an information system means that more tasks can be performed in an accountable and responsible manner.

2.1.1 Value of information

Information security is intended to safeguard information. Security is the means of achieving an acceptable level of residual risks. Aspects that enable discussing the value of the information are:

- **confidentiality:** protecting sensitive information from unauthorized disclosure or intelligible interception
- **integrity:** safeguarding the accuracy, completeness and timeliness of information
- **availability:** ensuring that information and vital IT services are available when required.

Other aspects that are derived from the ones defined above include:

- **privacy:** the confidentiality and integrity of information traceable to a particular person
- **anonymity:** the confidentiality of a user's identity
- **authenticity:** the state in which there is no dispute about the identity of the participants involved
- **auditability:** the possibility of verifying that information is being used in line with the security policy and the ability of demonstrating that the security controls are working as intended.

The importance of having appropriate information management, and also adequate information security, is twofold for an organization.

Internal importance

An organization can only operate effectively if it has timely access to confidential, accurate and complete information. Information security has to be in line with this, ensuring that confidentiality, integrity and availability of information and information services is maintained.

External importance

An organization's processes supply products and/or services, which are made available in the market or the community, in order to achieve set objectives. Inadequate information security leads to imperfect products or services, thereby preventing the business objectives from being fully achieved and threatening the continued existence of the organization. Having adequate information security is an important precondition for adequate information management. Note that this applies to both the public and private sectors.

Besides the flow of results (products and services), countless information streams also flow from the external environment into the organization, internally through the organization, and from the organization out to the external environment. If these information streams suddenly dry up, the organization is no longer capable of operating effectively.

The requirements for adequate information security management reflect the degree to which the business processes depend on information. Information Security Management should form an integral part of an organization's overall quality management and quality assurance procedures as executed within the business processes. Therefore the requirements set for Information Security Management should largely come from the people who manage the business processes.

2.1.2 Types of security measures – controls

An important issue in Information Security Management is the degree to which an organization's management is able and willing to make a specific commitment to protecting the information, by making resources available: people, time and money. This commitment should be made on the basis of the available resources and the required level of information security, proportionate to the value of the information that has to be protected. Security measures can reduce the risks and vulnerability; they are also referred to as 'controls'.

Security measures make it possible to reduce or eliminate the risks associated with information and IT. The starting point, and by far the most important, is to have a good security organization, with clear responsibilities and tasks, guidelines, reporting procedures and measures that are appropriately matched to the needs of the business and the IT. Physical security measures, such as the physical separation of the data center, control physical access and provide a stable environment. Technical security measures provide security in an information system, operating system or network. This is, for example, the security offered by the operating system for the segregation of users. Process or procedural security measures describe how the staff is required to act in particular cases. For example, there must be procedures that describe who has access rights to the data center and when, or procedures that describe when a user's 'account' expires and what has to be done with the user's information after expiry of the account.

Security measures are effective only when used harmoniously with business processes. The security organization has to manage and maintain an appropriate balance.

Security measures can be used at a specific stage in the prevention and handling of security incidents, see figure 2.2. Security incidents are not predominantly caused by technical threats – statistics show that the large majority stem from human failure (intended or not) or procedural errors, and often have implications in other fields such as safety, legal aspects or health.

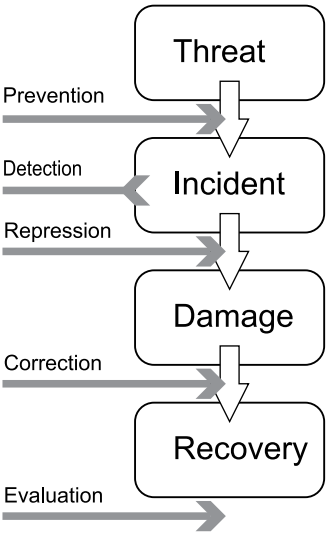

Figure 2.2: From threat to recovery; different types of countermeasures

The following stages can be identified. At the start there is a risk that a threat will materialize. A threat can be anything that would disrupt the business process or have a negative impact on business results. When a threat materializes, this is referred to as a security incident. This security incident may result in damage (to information or to other assets) that has to be repaired or otherwise corrected.

Suitable measures can be selected for each of these stages. The choice of measures will depend on the value of the information – that is, its importance to the business.
Preventive security measures are used to prevent a security incident from occurring. The best-known example of a preventive measure is the allocation of access rights to a limited group of authorized people. Further requirements associated with this measure include the management of access rights (granting, maintenance and withdrawal of rights), authorization (identifying who is allowed to access to which information and using which tools), identification and authentication (confirming who is seeking access), access control (ensuring that only authorized personnel can gain access).

If a security incident occurs, it is important to discover it as soon as possible: detection. A familiar example is monitoring, linked to an Event Management procedure. Another example is virus-checking software.

Repressive measures are then used to counteract any continuation or repetition of the security incident. For example, an account or network address is temporarily blocked after several failed

attempts to log on or a bankcard is retained when multiple identification attempts are made with a wrong PIN number.

The damage is repaired as far as possible, using corrective measures. For example, corrective measures include restoring the backup, or returning to a previous stable situation (roll back, back out). Fallback can also been seen as a corrective measure.

In the case of serious security incidents, an evaluation is necessary in due course, to determine what went wrong, what caused the incident and how it can be prevented in the future. However, this process should not be limited to serious security incidents. All (near) breaches of security 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 and weaknesses is required to be able to evaluate the effectiveness and efficiency of the present security measures based on an insight into all security incidents and vulnerabilities. This is facilitated by the maintenance of log files and audit files, and of course, the records of the Service Desk function, which are discussed later in more detail.

2.1.3 The business perspective: how to manage information security

The starting point is effective organization of information security, in which responsibilities, authorities and duties are clearly specified in increasing levels of detail:

- policy and/or codes of conduct (**which control objectives** aligned with business requirements are we aiming for)
- processes (**what** has to happen to achieve those objectives)
- procedures (**who** does what and **when**)
- work instructions (**how** do we specifically do that, when and where and how does reporting take place).

Maintaining information security is a continuous process. All the factors that influence its results, and therefore have to be acted upon, are seen as inputs. There are internal and external influences that have their effect on information security. The internal influences stem from decisions within the organization. External influences come from the environment in which the business processes take place. This diversity makes Information Security Management a challenge.

Examples of changes in input which require adaptation of the process are:

- changes in business demands
- organizational changes, mergers, acquisitions
- changes in tasks or the importance of tasks
- physical alterations, e.g. after relocating business premises
- environmental alterations
- changes in assessment of the IT used
- changes in legislation
- changes in hardware and/or software
- changes in threats
- the introduction of new technology
- ageing or obsolete technology.

The result should be that, seen from a business perspective, the Information Security Management process provides a large degree of confidence that a certain level of confidentiality, integrity and availability has been achieved, that is sufficient for the business's purposes, and sufficient for the organization's (business) partners.

The developments in information security began in the early 1970s and took place independently of developments in IT management. Today, it is generally recognized that IT management and security are inseparable. The model below shows the management model for information security, from a business's perspective (figure 2.3).

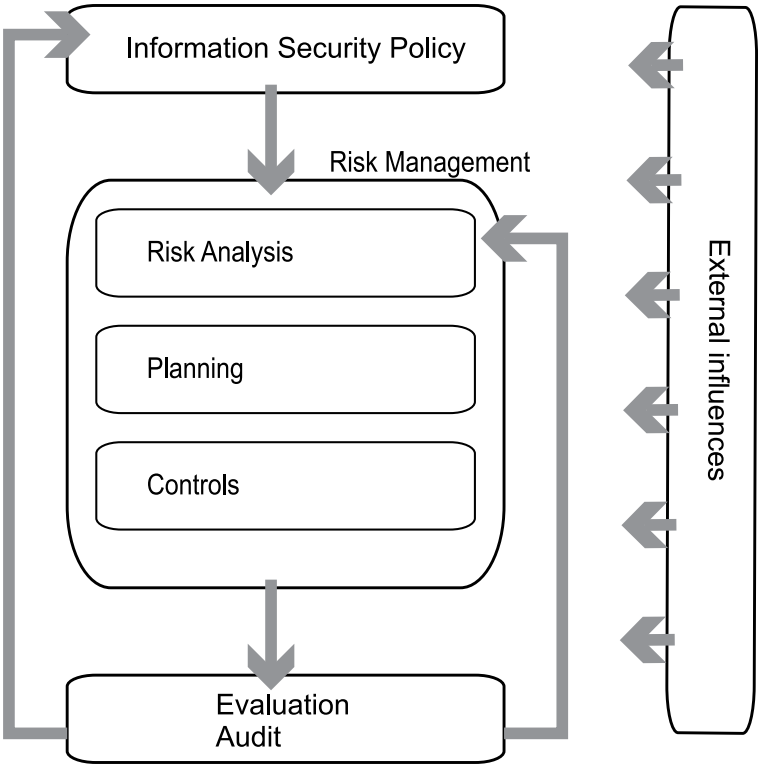

Figure 2.3: The Information Security Management System

The management system in figure 2.3 represents the complete information security process during all the phases of its cycle, from policy to maintenance. It is comparable to the management systems found in standards such as ISO 9000 and ISO/IEC 27001.

New business processes, at the earliest phase of formation, need to take information risks into account when considering business risks. This is also valid for existing business processes for which information security has never been an issue.

To determine what information security requirements are applicable and what countermeasures/ controls are required, a risk analysis is performed. The Information Security Management system consists of the closed loop created by evaluation and feedback to risk management of the process.

The risk analysis produces the details of the business case that supports investments in security. In this analysis, the requirements for security and details about risks become available; this information is used to detail information security in the security section of the Service Level Agreement (SLA), usually in the form of control objectives or a list of controls or countermeasures.

Information Security Management does not cover the details of performing such a risk analysis. For more details on the context of risk analyses within risk management, see ISO/IEC 27005.

In most organizations, information security and its management is governed by an Information Security Policy, whether as a separate document or as part of a larger (e.g. security or information) policy. With such a policy, consistency and coherence of processes and controls in the organization is dictated.

ISO/IEC 27005 is primarily concerned with risk analysis, the stage leading into the selection of security controls. ISO/IEC 27001 and ISO/IEC 27002 and ISO/IEC 27003 are more explicit on the planning, implementation and operation of security controls. The corporate information security policy provides direction to Information Security Management. It contains the mandatory management guidelines on, among other things, the organization, establishing the management control framework, responsibilities, scope and depth. This corporate policy is known under many names. It is sometimes part of (or related to) the Enterprise Risk Management policy, and policies for governance, risk, compliance or assurance.

Risk analyses should be performed to define the security objectives from a business perspective as well as from a technical perspective. These analyses make clear the current status and quality of information security (the current situation) as well as the security measures that are to be implemented (the desired situation). The required situation is described in a security plan or security handbook.

Planning is required to move from the current to the desired situation. After implementation, operation of the measures forms part of normal day-to-day operations. Management uses the management control framework to review the effectiveness and efficiency of the implementation of the security measures. These reviews also provide the necessary feedback to either improve the implementation or improve the plan. This input is used in the periodic (annual) security improvement plans, also known as risk treatment plan. The results of the audits also provide input to adapt the policy, or to improve the 'toolkit' for Information Security Management, including, for example, the risk analysis tools.

This book does not prescribe any risk analysis technique, such as ISO/IEC 27005 (Risk Management), IRAM (Information Risk Assessment Method from ISF) or the CCTA Risk Analysis and Management Methodology (CRAMM). Although risk analysis is required in identifying risks and the selection of measures, it should only be applied using a methodology that fits the organization and used where and when needed. Risk management and the selection of an approach that fits the objectives and maturity of the business are described later.

Management in general is concerned about money, as in cost and revenue. In information security measures, these aspects are to be treated seriously in order to avoid the perception of cost-only activity, so the outcome of a risk analysis should take the form of a balance, in which both risks and measures are (at least qualitatively) balanced between their 'costs' and their 'revenues'.

When a risk assessment is carried out professionally, management will obtain a positive view on information security and should be able to make decisions at the management level without the need to understand technical details.

2.1.4 A manager should be in control

Information security is about assurance. A manager should be 'in control'. Effective information security assures the continuity of the business, and the achievement of business goals.

To secure the IT infrastructure costs money (in terms of the cost of resources, maintenance and control). Not to secure the IT infrastructure also costs money (in terms of loss of revenues, costs of lost production, replacement costs of stolen or damaged data/equipment, compensation payments for unfulfilled contractual obligations). Estimating the costs requires business knowledge in order to produce meaningful financial values. It is even more important to estimate losses because of reputational damage, adverse publicity and loss of customer confidence. Reputational damage is not easy to quantify in financial loss. The financial aspects of Information Security Management are covered in section 4.1.4.

Effective Information Security Management depends on accurate risk analysis so that knowledge of the impact of risks and the costs of avoidance is understood. Without it, the tendency is either to ignore risks in the hope that they never happen, or spend disproportionate amounts of time and money on avoiding risks of minor potential impact. Risks are an inevitable feature of business life, and must be managed. Known risks, as well as unknown risks have to be managed: be prepared for the unexpected. Information Security Management is concerned with those activities that are required to maintain risks at manageable proportions, such as evaluation of effectiveness of measures, registration and trend analysis of security incidents.

2.1.5 Customer perspective

IT service providers have evolved into highly professional organizations. Customers of these service providers depend on their services to a large extend. In such a relationship, the professionalism of customer and service provider should be comparable, to enable a balanced relationship.

Figure 2.4: Trend in assurance and compliance

In the past, customers simply had to trust a service provider. Nowadays, under the pressure of legislation and regulations, customers require assurance about the security performance of their service providers that is based on evidence.

The movement from 'trust me' to 'prove to me' is a recent development (see figure 2.4). In Eastern cultures the focus has always been on trust, while in the Western world evidence has been more important.

In the process of specifying the Service Level Agreement (SLA), the service provider needs to ensure that it captures the customer's specified security requirements. If these requirements are matched with the security services from the service provider's Service Catalog, this is a benefit. The service provider can standardize its operation, which is easier to enforce and with less potential for error. It should also be more cost effective, since the same way of working is applied for more customers.

If the standard Service Catalog does not provide the required standard security services, then security services are tailored to the customer's need. This may be done via the Service Design phase of the service lifecycle.

Service providers can anticipate the need for confirmed assurance. The options below give some suggestions on how to provide sufficient assurance for groups of customers:

- **management assertion:** declaration of a service provider's management that a defined Information Security Management process is established and/or a certain internal or external standard is met
- **certification:** confirmation of a management assertion by a certification body, that an external standard such as ISO/IEC 27001 is met. The Code of Practice for Information Security Management (ISO/IEC 27002), provides best practices that help the organization to meet the requirements. Certification aims to address the requirements of a wide range of customers
- **third party conformation** by an independent auditor to report on the status of control objectives and controls of service organizations for use by user organizations and their auditors.

In addition to the required security services that are laid down in the SLA, a process (or at least a communication mechanism) should be established between the customer and the service provider to address security issues, including:

- common processes: incident management, authorization management, business continuity planning
- points of contact/responsibilities for the above processes
- reporting
- escalation mechanisms.

The security paragraph of the SLA is not limited to a description of control objectives. It should also define requirements for common processes, not only for maintaining objectives, but also for management of incidents, authorization and continuity. The SLA can, for example, address requirements for a common risk management process.

This alignment should be organized as part of the normal customer-service provider relationship model. Experience shows, however, that over time specific contacts for security issues emerge.

2.1.6 Partner perspective

More and more, parties are part of a value chain or network in which each link or node adds value to a service or product. An example is the distribution and supply chain, taking care of

physical goods. For each and every link in the chain, it is important that the quality of the information in the chain is known, and that it is timely. In value chains, two concepts for information management are commonly used:

- **centralized:** parties share information in a common place, that is managed by one of the participants or a service provider
- **decentralized:** parties distribute the information themselves across the relevant links in the chain.

Centralized information management

When parties share information in a common place, the requirements of all the participants should be analyzed and shared with the service provider. The situation is not very different from a 'customer'-'service provider' relationship as described above. Assurance can be organized in the same way.

Decentralized information management

Requirements should be communicated between the links. Because the links depend on each other, it is not sufficient to only address the needs of adjacent links; assurance must be organized over the whole chain.

Since in both models more parties are involved, standardization becomes even more important. For assurance, a common governance model, or a way to demonstrate compliance, has to be agreed upon. Accredited certification is valuable as a means for the organization to prove the existence of a standards-compliant information security management system without the need for each party in the chain or network to check security for themselves. There is a cost saving plus the adoption of generally accepted good security practices.

2.1.7 Oversight and auditing perspective

In today's governmental and business environment, 'assurance' is an ever-growing issue. An informal definition of assurance is: a level of certainty that something (a product, service or more generic organization behavior) meets defined criteria. These defined metrics usually imply compliance to agreed specifications, a norm or standard. 'Compliance' in broad terms, takes into consideration factors such as:

- the set of control objectives or controls that is to be implemented
- supervision, internal management oversight (e.g. using exception reports to identify situations that may deserve closer scrutiny; and internal auditing)
- review mechanisms (internal and external independent reviews, certification)
- awareness, training and educational activities to drive up compliance through understanding and appreciation of the requirements, pragmatic guidance and motivation
- sanctions, and the threat of sanctions
- the scope and quality of the standard or requirement against which compliance is sought (e.g. the Payment Card Industry Data Security Standard (PCI DSS)).

Compliance is often focused on external requirements, e.g. from legislation, the oversight body or customers. In that case compliance does not say much about the organization's own requirements for security.

When failure of one organization may have a high impact on all similar organizations in the same business segment, or on a group of consumers, assurance can be organized for this whole business segment by means of 'oversight'. In the banking and insurance environment, for example, oversight is there to stimulate and assure that all parties meet the assurance objectives set by the oversight body.

Oversight bodies have to balance their demands carefully. One the one hand, a dynamic commercial environment, aiming at innovation, competition and taking acceptable commercial risks, is to be stimulated and the cost of compliance should fit the purpose. On the other hand, the interests of all parties require that each of these parties acts responsibly, maintains a clear view on risks and limits these risks in such a way that continuity and stability can be expected. Two approaches, the rule-based and the objective-based, are used. In the rule-based approach oversight bodies present a detailed checklist with controls that are to be implemented. In the objective based approach oversight bodies set the objectives and the overseen entities have to explain their control selection that meets these objectives. In both cases, organizations have to demonstrate that controls have indeed been effectively implemented.

In short, IT auditors review risks relating to IT systems and processes including:
- inadequate information security
- inefficient controls, use of corporate resources or poor governance
- ineffective IT strategies, policies, controls and practices.

As part of their role, IT auditors check for compliance or conformance to agreed internal or external standards. Their requirement is that either their customer has a defined internal control framework, a set of control objectives/controls, or that an external standard can be adopted. Where processes are in place that provide for compliance, the auditor merely verifies that these processes are indeed adequate and perhaps validates a suitable sample. If these processes are defective or not present at all, the IT auditor has to gather evidence much deeper in the organization and the systems. This usually has a greater burden on the organization. For efficient auditing, the standards with which to comply should be defined beforehand, and the compliance processes, possibly supported by tools, should be implemented as well.

2.1.8 Perspective of the IT service provider

The IT service provider acts on identified customer requirements and has a security baseline (see 4.1.3 for an explanation of the concept) for its own security. Expectations of its customers about the quality of security services and evidence of their quality tend to grow rapidly. For an IT service provider communication about what is, and is not, part of the standard offering is important – not only for the purpose of managing the expectations of the customer, but also for legal reasons. If the limitations of the service offerings are not defined, the customer may reasonably expect their service to meet a level that is common in the market.

The definition of the security services can be part of the Service Catalog. Elements are: the Information Security Management process, a baseline for security control objectives, and reporting and sign-off. In addition the service provider offers security services in this Service Catalog, on top of the standard elements, on a commercial basis.

2.2 Security architectures

One of the definitions of 'architecture' used in ITIL (Service Design) is: 'the structure of a system or IT service, including the relationships of components to each other and to the environment they are in. Architecture also includes the standards and guidelines which guide the design and evolution of the system.'

This definition of 'architecture' comprises the design principles for:
- the objects themselves
- their relationships
- their interaction with their environment.

For example:
- an information system including hardware, software and applications
- a management system, including multiple processes that are planned and managed together, such as a Quality Management System
- a database management system or operating system that includes many software modules that are designed to perform a set of related functions.

Security architecture is defined along the same lines: a related set of entities that work together to achieve an overall security objective. 'Achievement' in security has two facets:
- the utility or functional aspect that a certain security functionality is offered, which makes the entity **fit for purpose** in establishing a secure environment
- the warranty or non-functional aspect of an entity that security is otherwise not compromised and cannot be bypassed, which makes it **fit for use** in a secure environment.

2.2.1 Security architecture relationships

Figure 2.5 shows the positioning of security architecture in the security framework.

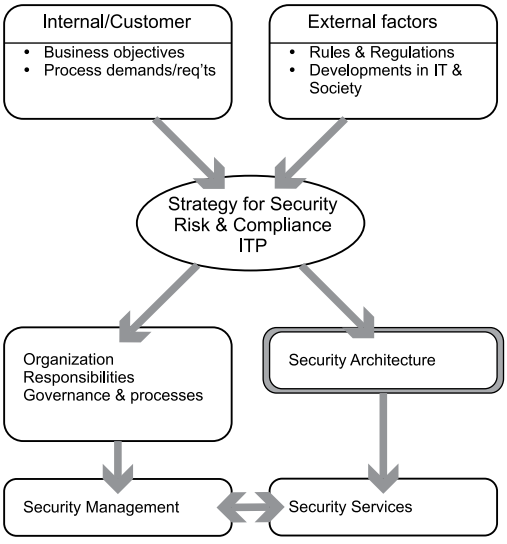

Figure 2.5: Security architecture relationship

The strategy for security, risk and compliance - see section 4.1 'Service Strategy' - is positioned in the center.

Architecture follows strategy. The strategy gives the boundaries of what can be done centrally and what is a local responsibility. The information security policy translates the business objectives, with support of risk assessment, into control objectives. These control objectives are realized through a set of controls that can be embedded in processes, be part of the culture of IT professionals, or are implemented in the domain of information and IT. The architecture needed for the latter part is a consequence of the choices reflected in the policy.

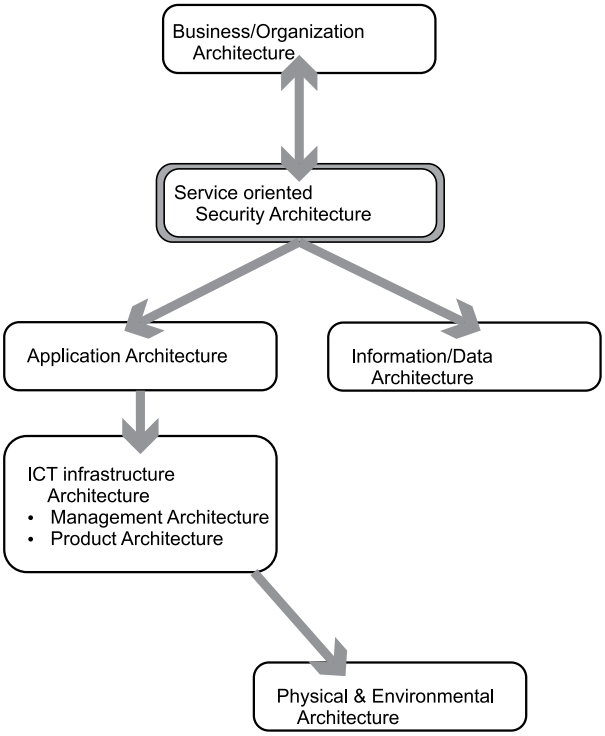

Figure 2.6: ITIL hierarchy of architectures

2.2.2 Elements of security architecture

The security architecture defines which *security services* are offered to whom. It also describes generic security guiding principles and security patterns to be used in designing new solutions not yet defined as services. The security architecture also provides *design guidelines* for new or renewed services. These two basic elements of security architectures are described below. In ITIL, a hierarchy of architectures is used. Figure 2.6 shows this hierarchy. The services of the security architecture are translated into protection:

- at the information/data level
- in the application

- in the supporting general infrastructure (platforms, networks, operating systems, generic applications, middleware, etc)
- in the wider environment, including cultural and physical aspects.

Note that a security service includes both the utility, the functional part, e.g. access control, as well as the warranty, the non-functional compliance part so that the functional part cannot be bypassed. The latter part, referred to as hardening, is not to be forgotten. Where the functional part may be offered somewhere in the hierarchy of functions, the compliance is required everywhere: a leakage of information at any place or level may jeopardize all good intentions in other places. However, the assumptions about what protection is expected where, as a precondition for effective behavior of a security service, must be made explicit. These 'conditions for effective usage' should be a standard part of each security product.

Other elements of the definition of a security service include:
- assurance, trustworthiness and proof of the reliability, suitability and quality of the service
- associated management activities and controls e.g. metrics, roles and responsibilities and accountabilities.

The security architecture defines the security services and the generic rules for implementation. Services can be centralized or decentralized, can be offered in the sub-architectures addressing information/data, application, infrastructure and environment, and can be implemented through a wide range of technical solutions. 'Identification and authentication', for example, can be a centralized or decentralized service. The challenge is to provide flexibility over time.

Examples of recognized practices for security architectures include:
- Enterprise Information Security Architecture
- Common Data Security Architecture/Open Group
- ISO OSI Security Architecture (enriched ISO 7498-2)
- Jericho Architecture and COA Framework (Jericho Forum/Togaf)
- RFC 4301: Security Architecture for the Internet Protocol
- ISO/IEC 10201: Security in the health environment
- NIST SP 800 series
- ISO/IEC 18028 -2: Network Security Architecture
- Octave
- SABSA

2.2.3 Common design principles for security services

The architecture gives the common design principles for security services. Given the speed of change, a first recommendation is to allow for evolution in the service and recognize the need for growth paths in the service offering itself. A challenge is to facilitate the ever-changing boundaries of protection, known as pre-, de- and re-perimeterization (see [JER]). It is normal that a security architecture evolves and that different concepts for protection co-exist for a longer period of time, which can be problematic.

The security architecture should provide design principles for security services. Key characteristics of the definition of a security service include:

- **functionality:** the service definition
- **trust models:** assumptions about the (unbroken and continuous) trustworthiness of the service itself and its environment
- **condition for effective use:** prerequisites, dependencies and possible interaction:
  - **boundaries:** is the service limited to a certain domain?
  - **trusted sources:** are these required and, if so, how are these identified and authenticated?
  - **environmental awareness:** is the service able to gain any required information about its environment?
  - **interaction:** if the service requires input or communication with other services, how is this interaction established?
  - **trust assumptions:** what protection is assumed from underlying layers, from other services, etc.? Is there a trustworthy part of the infrastructure? What is to be regarded as hostile or friendly?
  - **secure sessions:** is it possible to set up secure communication and, if so, which protocols are supported and how is identification, authentication, authorization and access control established?
- **management of the security service:**
  - central, decentralized, reporting, logging, monitoring, alerting
  - roles and responsibilities
  - ownership, responsibility, delegation
  - management of trust
- **resilience:**
  - hardening
  - vulnerability management
  - self-repair, fail safe defaults
  - survivability
  - 'graceful' degradation and revival
- **performance and capacity management**
  - recovery and contingency planning.

One of the challenges today is that some parts of the information, services and infrastructure are under the business's control and management, some may be outsourced under reliable security agreements, some may depend on partners in a chain of trust and some parts may be completely unknown.

2.2.4 Design principles for secure environments

Design principles for secure environments have evolved since 1975 [Sal]. They provide design principles that every architect, designer and developer in security should take into account.

- **isolation:** isolate critical components, monitor their behavior and keep them as simple as possible to enable controllability and auditability. Examples: firewall, centralized authoritative sources, cryptographic functions, etc.
- **fail-safe defaults:** deny everything that is not explicitly authorized. Reasons: create a fail-safe mode by preventing vulnerabilities caused by omissions or neglect. Examples: No access unless authorized, 'stripping' the web server operating system
- **complete mediation:** every access must be mediated. Reason: completeness. Examples: all external access must pass a firewall, all logins must pass the access control system, no back doors in the network, binding of functions so that these cannot be easily by-passed

- **open design:** security must not depend on secret design. Reasons: open design will be tested extensively and a secret design cannot be kept secret anyway. Examples: use well-known cryptographic algorithms, use proven technology, avoid home-made or end-user software
- **privileges: specify and separate.** Be clear about responsibilities and accountability. Be clear on reporting. Divide sensitive functions between different employees and/or services. Reason: create opposing interests, enabling the detection of fraud or error, and provide social barriers for fraud or abuse. Examples: separate granting of access from operational responsibilities, separate development from production, be specific on responsibilities for application management versus IT management, create a position for assigning user identities
- **limited functionality or least privilege:** components and users can only do what is necessary, so a functional need should exist ('need to use', 'need to access'). A more informal version is the 'need to withhold'. Reason: limit risk by cutting off potential vulnerabilities. Examples: menus based on authorizations, use protocols with defined limited functions, access only granted to identified and authorized components, limited access to operating system functionality, operational management through scripts only, run privileged functions under non-interactive limited accounts
- **compartments (levels, zones):** create separation so that activities from one compartment to another can be controlled and problems from one area cannot emerge/cross over to another. Reason: limit potential problems to a known specified area ('untrusted zone', e.g. the outside world) or concentrate security services on a known critical application area ('trusted area'). Examples: sub networks or zoning, Demilitarized Zone (DMZ)
- **ergonomics:** the interface must minimize the possibility of error and allow for error detection/correction. Examples: Rm –rf .*/*, 'to cancel, abort; press 'no' to continue'. Reason: prevent accidental error
- **redundancy:** never rely on a single barrier. Reason: be safe. Examples: access control both on application and operating system level, redundancy in web hosting, different paths to same destination, Raid-grade storage (Raid: 'redundant arrays of independent disk', today used to indicate the reliability of storage)
- **diversity:** never rely on multiple identical barriers. Reason: if one barrier is broken, everything is broken. Examples: two factor authentication, firewalls from different manufacturers, proxy and router
- **adaptability:** provide flexibility such that security mechanisms can be replaced over time. Reason: even the best security today may be insufficient or may be broken tomorrow. Examples: start with password security today, enable to add chip card tomorrow, and perhaps biometric techniques in the future; start with a cryptographic algorithm today but make sure it can be upgraded when required
- **resilience and survivability:** design services such that poor functioning is detected and recovered from. Enable the detection of vulnerabilities and controlled upgrades, fixing/automated patching. Define recovery points and safe states in case of failure. Reason: things will go wrong. Examples: 'hot fixing' newly detected vulnerabilities in operating systems, recovery points for databases
- **manageability:** make sure the service can be maintained and controlled
- **report:** a service must provide information on its own functioning and of defined events. Reason: enables manageability and detection of unwanted events. Examples: function reports, audit files, incident and event reporting, alarm messages.

Be aware that the boundaries are ever moving. In the last few decades many of the controls were bound to a specific geographical location with controls focusing on isolation of this environment with its local area networks and operating systems/platforms residing on hosts physically placed on that same location. Later on, an additional boundary of protection was added in the application layer. And now we see that since both data and applications become moving objects (sometimes with unknown or virtual locations), the controls are tied to the object of protection itself ('self defence'). An example of the latter is 'Jericho', the security architecture proposed by the Jericho Forum, part of the Open Group [JER]. All these developments will have to co-exist somehow. This is why it is important that services have an awareness of their operating environment so that events or incidents are more easy to recognise and can be anticipated upon, e.g. through limitation of their normal functioning.

The design of an architecture should not be an isolated exercise. From the start of the architectural design, it must be clear which common management processes (see figure 2.5 and 2.6) are required. This should ensure that the architecture and the management framework go together.

2.2.5 Common security services

The main common security services are:

- **identification:** recognizing an object (digital representation of a human being; application; network; machine; intelligent components, etc.)
- **authentication:** validation and accepting/rejecting of an assumed or declared identity. Often different levels of trust are supported for different purposes
- **authorization:** allowing/enforcing rights for access or execution of activities. Authorizations are often linked to objects. Many authorization mechanisms and methods exist. Examples are single use authorization; distributed, central or federated authorizations, etc. Authorization models may also address domains, roles, time-dependency, assurance and required evidence. Little standardization is available at present
- **access control:** enabling and enforcing access to information and/or activities limited to authorized objects only
- **boundary protection services:** geographical or logical boundaries are created, e.g. in networks to separate the trusted inside from the hostile outside world
- **secure communication services:** span the transfer between one safe domain, crossing untrusted domains, possibly to another safe domain
- **alarm, alerting, logging, monitoring:** signalling of defined events. Examples include monitoring of events, incidents, vulnerabilities and their follow-up, policy enforcement, etc
- **continuity services:** react to events that indicate that availability (such as response time) can be an issue or data loss is signalled to exceed a certain threshold. Example reactions include: enable the use of additional resources; gradual degradation of a service; disallow new connections
- **integrity services:** protect continued correctness, completeness and 'currentness' of data, applications, etc; detect anomalies, prevent, detect and respond to errors. Examples: full input checking; syntax checking; semantic validation; output validation; virus detection and control
- **confidentiality services:** enforce, protect and support use of confidential information. Examples: enforce classification and labelling and supporting policies
- **cryptographic services:** cryptography to protect confidentiality, validate and demonstrate authenticity and integrity, hide presence of communication

- **hardening services:** monitor and enforce security settings according to policies; detect and report divergence; respond and react to (new) vulnerabilities; patch management.

The security services themselves must be securely managed as well, so the following are needed:

- management and control of security services:
  - monitor correct behavior of security services
  - define points of administration
  - define Change Management with clear acceptance after testing
  - enforce security policy
- ownership and responsibility for managed objects
  - the definition of split or shared responsibilities between service providers and their customers is relevant here. Also, management of trust across a service delivery chain is an issue
- authoritative sources of security information:
  - which are recognized authoritative sources?
  - how are these maintained?
  - example: which model for authorizations is used and enforced?
- detecting and monitoring incidents, events (especially near misses, which provide valuable lessons), vulnerabilities and follow up
  - signalling of intrusions, weaknesses, vulnerabilities and incidents. This may be based on input from trusted internal or external parties, such as a CERT (Computer Emergency Response Team)
- reporting, assurance and compliancy services: evidence of correct behavior as well as evidence that certain levels of performance are or are not met are useful since these reduce the cost to prove compliance. New rules and regulations have put a heavy burden on organizations to not only exceed expectations, but also to provide sufficient assurance that this is indeed the case. The more these processes can be automated, the easier it is. (Note: a simple example of developing maturity is that in the first couple of years, the emphasis will be on demonstrated assurance in the general infrastructure, then on 'proven' assurance provided by applications and finally the emphasis will be on risk management in business-relevant terms.)

These are the common security services; many more exist. For a detailed description see *The Common Criteria for IT Security Evaluation* ISO/IEC 15408.

A service oriented security architecture defines:

- which security services are provided centralized/decentralized
- where services are provided in (which combination of) the supporting architectures:
  - in the data/information architecture
  - in the application architecture
  - in the IT infrastructure architecture
  - in the physical/environmental architecture
- which security mechanisms are mandatory, optional, supported,… and again, the placement of these mechanisms.

For further information about security architectures see the ISO 7498-2 standard.

3 Fundamentals of management of information security

Information Security Management is essentially a series of activities that manages a specified level of security of information and IT. It deals with establishing and maintaining all that is needed to keep the required level of information security. Whether threats from the outside world or changes of business processes, the required level of security has to be maintained to keep business risk at an agreed and acceptable level.

The basis for that required level is the agreed specification of information security. These specifications are laid down in contracts or agreements such as a Service Level Agreement (SLA). ISO/IEC 27002, as a best practice, provides a list of controls to be considered as a starting point, including:

- availability of a corporate information security policy
- description of controls to ensure asset protection
- user and administrator training
- provisions for transfer of personnel
- specifications of the process of change management
- access control policy
- points of contact
- compliance
- details about auditing security
- reporting.

How to reach the required level of information security – that is, how to determine what measures/controls are to be taken – is one part of Information Security Management. It contains subjects such as risk analysis, the definition of appropriate measures, creating a standard minimum level of information security, the implementation of controls and operational monitoring such as intrusion detection.

The other part of Information Security Management deals with maintaining information security at the required level. Subjects include incident registration and handling, trend analysis and reporting, escalation support, maintaining standards, vulnerability management, awareness communication, etc.

When information security is in place, operational and functioning, it is a continuous process. The Information Security Management process coordinates and directs the security activities, using a standard process management cycle.

3.1 Information Security Management – the continuous effort

The management of information security is a continuous effort. This continuous effort concerns the effectiveness of security in everyday operation and comparing that level of effectiveness with the actual control objectives/security requirements. There must be regular evaluation of the goals and targets of information security in order to maintain the required confidence from the business.

But the continuous effort of the management of information security is not only in the operation. It should also be in the transition towards operation, in the design of services and in the strategy for security. A proper feedback loop is needed as well, to enable maintenance or continuous improvement of security.

3.2 Information Security Management as a PDCA cycle

A process approach is adopted to describe the activities that in combination result in Information Security Management. A process is defined as a set of related activities that transforms input to output, uses resources and is managed. This allows use of the well-known PDCA cycle (Plan-Do-Check-Act) to detail functions such as establishing, implementing, operating, monitoring, reviewing and improving of the management of the process. The PDCA cycle is also the basis of ISO/IEC 27001.

3.2.1 Overview

The PDCA cycle, also known as the Deming Cycle [DEM], provides a framework for improvement of a process, although it lacks a controlling function to maintain the momentum. To emphasize the importance of maintaining momentum, a central control function has been added to the model without altering the role and functions of Plan, Do, Check and Act (see figure 3.1).

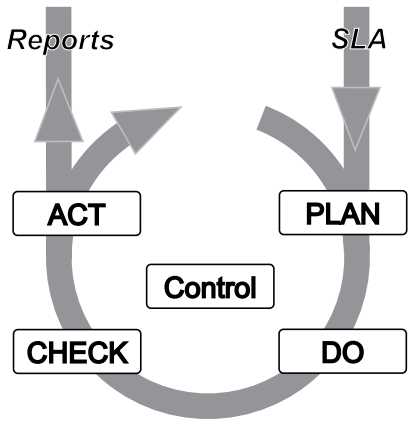

Figure 3.1: The Information Security Management PDCA cycle

The input of Information Security Management consists of the information security requirements stated by all business, partners involved and the service provider itself; the output is the established information security that meets those requirements. Reporting is used to provide evidence of meeting the requirements. The same reporting provides overview information, which is useful in awareness and communication programs for the organization.

Care should be taken when organizations are part of a chain or network. There could be a situation where security in the leading and trailing processes falls outside the scope of this Information Security Management domain; however, consistency over all processes in the chain is necessary to ensure that security is not breached in another part of the chain.

Special consideration is required where multiple SLAs exist. Often the required security levels differ; and different service providers may offer variations in security levels. Information Security Management must be investigated to determine to what extent those variations will create additional security implications. Effective communication on this subject between the parties may well be one of the more challenging activities to organize.

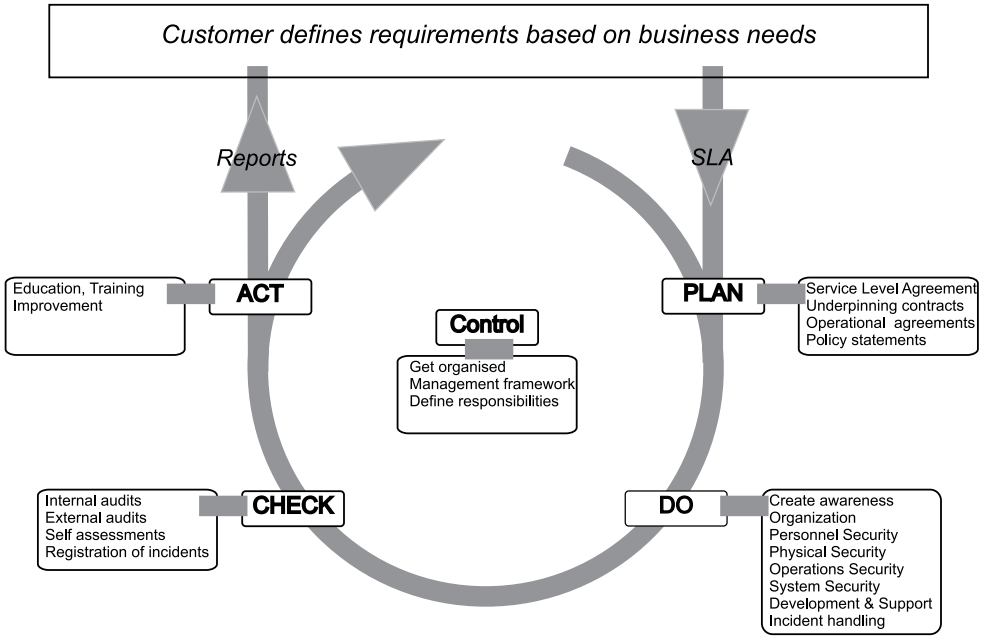

Figure 3.2: The PDCA circle in more detail

3.2.2 CONTROL: Control of Information Security Management

Control of Information Security Management looks like the conundrum 'who manages the manager'. For implementation and functioning of Information Security Management, control is indispensable.

The objective is to organize Information Security Management. It provides the ability to implement and execute Information Security Management in a consistent manner. Without control the results are less predictable and management will not be able to perform as required. Certification of an Information Security Management process will be impossible without control in place.

Summary of activities

The control activity is aligned with the other control processes within IT management. The Information Security Manager (ISM) is the manager of the control activities; this can be a role or a function. The ISM is a peer to his/her fellow process managers.

Control of Information Security Management directs and organizes the Information Security Management process, which includes the organization of the management framework for Information Security Management. Implementation of an Information Security Management process requires planning and procedures. In addition, control enables reporting of status, results and progress.

The control activity defines the (sub)processes, the functions, roles and the responsibilities within those subprocesses. It also identifies the organization and reporting structure.

Management forum

It is important to establish a steering body, providing input from internal and/or external customers. For internal service providers, control of Information Security Management is greatly supported by a management forum for information security. This forum can be composed of the jointly responsible line managers, plus employees with specialist security roles (who can also do the work required to prepare for forum meetings). The forum meets several times a year (for example as part of an extended normal management team meeting) to give direction to information security. The typical tasks of such a forum would be to:

- provide steering
- review the policy, review control objectives
- modify the control framework and security measures
- approve security plans
- maintain responsibilities
- monitor changing threats and incidents.

Input for this forum can come from corporate assurance functions such as a Governance, Risk and Compliance Board or Enterprise Risk Management.
External service providers can also use this approach by organizing customer security interest groups.

Coordination

Another vital part of the control of Information Security Management is the coordination of information security within the organization of the service provider. This refers to:

- implementing plans and measures
- agreements about co-operation and co-ordination between the various roles and responsibilities relating to information security

- agreements about the methods and techniques to be used (for example, the method used for risk analysis and the use of a single classification system throughout the organization)
- setting up organization-wide initiatives (for example a security awareness program).

The coordinating role does not only address operational issues, but also the coordination of other issues including strategy, design, transfer and review.

Security in new IT: testing, acceptance
A major subject of information security is authorization of information processing processes, which includes the authorization process for information services and IT facilities. Before these become operational, they must be tested to ensure that security requirements are met. This requires a process for testing and acceptance. Testing usually implies positive testing (whether a specified input results in a specified output). Security testing also implies negative testing: the absence of unwanted functionality, vulnerability testing, negative impact from/on layered or adjacent infrastructure such as other operating systems or applications, performance under pressure, robustness for input or processing errors and resilience. These aspects should be built into the testing process.
Acceptance of a new service, IT facility or part of the infrastructure is a formal step. It may involve acceptance by the representative of the service user organization.

Specialized advice
Part of Information Security Management is about making decisions in highly technical security matters such as encryption, risks or audits. Specialist advice may be necessary.

Sharing
There is a great deal of co-operation between organizations in the specialist security sector. There are organizations such as the Information Security Forum (ISF – www.securityforum.org), the SANS institute (www.sans.org) or the International Information Integrity Institute (I4 – www.i4online.com) that share experiences and provide best practice information. Not only methods and techniques are discussed; threats, risks and surveys of security controls are also frequently discussed topics.

Independent review
This is another mechanism that supports Information Security Management. It ensures that the implementation of information security is regularly reviewed by an independent party – for example, those of the internal or external IT auditor.

3.2.3 PLAN: Planning within Information Security Management
The starting point of planning is proper organization of information security, which means that responsibilities and authorities are defined and specified at all required levels.

Objective
The objectives of the PLAN sub process are twofold: define/maintain 'to be'-plans and define/maintain the annual cycle for Information Security Management.

Summary of activities

The main activities are defining and maintaining 'to be' plans, together with the annual cycle of information security management activities.

Maintain/define 'to be'-plans

The SLA requirements and control objectives of the customers (as well as those of the service provider) are translated into controls/measures laid down in plans; they are maintained in such a way that the controls/measures remain actual in view of changing risks. These plans typically address the baseline controls and additional controls that reflect the specific risks of an information system; they may also describe typical control activities that are implemented in a process.

Examples are:

- description of risk registers and risk treatment/security improvement plans
- control frameworks or lists of baseline security measures
- templates for reporting
- periodic reviews, assessments, audits and evaluation
- collection of event and incident information, evidence, log files
- description of the crypto key hierarchy and management
- process descriptions for incident, user/authorization and continuity management.

Typical outputs of this sub process are the Information Security Policy and the security baseline. Security service levels can be defined here as well. Customers will be likely to have diverse requirements, but note that a translation of these requirements to the standard baseline or to a small number of security service levels is often possible, which limits the requirement to maintain error-prone specials.

One of the main products of this sub process is the security improvement plan or risk treatment plan in which the improvement activities are laid down and residual risks are accepted.

Annual cycle for Information Security Management

Many Information Security Management activities are planned ahead and executed accordingly. In resource planning, a good practice is to make reservations for ad hoc activities that cannot be planned upfront. Examples of periodic activities are organizing self-assessments, awareness activities, monitoring security in innovation processes, reviews/audits, risk analysis and improvement planning.

3.2.4 DO: Operation of Information Security Management

The operation of Information Security Management means performing the activities required to maintain the level or quality of the organization's information security in the context of the organization's and customers' overall business risks.

Objective

The objective is to executed ad hoc and planned activities in an efficient and effective way that reflects the requirements of the customers as well as the service provider.

Summary of activities

Some activities are continuous processes; some take place several times a year as defined in the annual cycle; and some are projects defined in the Security Improvement Plan that take place as continuous processes.

Examples of continuous processes are:

- security incident handling. Incident handling encompasses a wide range of activities that deal with incidents, from the procedure to report incidents, via registration to coordination of handling the incidents, escalation if required and cooperation with Problem Management and other Support Management
- support of Change Management. Changing requirements or occurrence of security incidents require follow-up by modifying systems, organizations or procedures. For this, the Change Management process is instrumental. Expertise from the information security organization is required to prevent decrease of the security level
- user, identity and authorization management/access management: given the increasing requirements in this area, a common policy and process is needed that guarantees or provides coherence of access rights throughout the organization and for customers
- CERT (computer emergency response team), vulnerability management, patch management
- maintaining awareness. Communication is an activity that does not automatically fit within Information Security Management. However, to maintain momentum, to keep the organization alert as far as information security is concerned, communication is crucial. Only through communication is it possible to prevent the failure of well designed controls because of human failure, neglect or lack of users' willingness to cooperate
- supporting the organization with risk assessments
- supervising reviews and audits. After planning (in the PLAN phase) reviews and audits have to take place. Supervising and supporting the reviews is one of the regular tasks within Information Security Management. Registration of the reviews and filing and reporting on the results are additional tasks.

Implementation of information security controls and the coordination of that implementation can be seen as one of the activities of the operation phase of Information Security Management.

3.2.5 CHECK: Review of Information Security Management

Information security without reviews will not work, because there has to be some means of assessing its effectiveness in operation. There will always be human error or reluctance to follow security procedures. Since security controls and countermeasures require effort or performance, people tend to take the easy way out, forgetting about rules and procedures that are not designed to make work easier.

Different types of reviews can be used. These can range from formal audits, through independent reviews, supervision and self assessments to ' Quick Scans', designed to take a snapshot of the controls in place.

Whether executed by external parties or by the internal auditing department, reviews help to identify if every player is still performing. It is the best instrument to determine where and what to change to maintain the required security level.

Objective: to assess (check) compliance with the information security policy and standards of the service provider and compliance with the agreed objectives, controls and standards of the customers, usually laid down in the SLA. This requires a regular audit of the (technical) security of the information systems. The service provider supplies information for this to an independent auditor or the customer's auditor.

Summary of activities

- undesirable use of information, services or IT facilities: focus on preventing undesirable use or even misuse of the resources placed at the discretion of employees. Only permit use for authorized business objectives, covered by the job description of the employee. The same limitation applies to the use of resources by and of third parties. This includes, for example, not only those activities that may be covered by legislation on computer crime, but also the improper use of IT facilities, such as playing computer games or keeping private accounts. Include in the SLA details of what is expected of the service provider in this area
- compliance with security policy and standards: regularly check compliance with the security policy, the security standards and any other security requirements taking into account the effectiveness and efficiency of the policy and the framework of security measures
- legal compliance, including prevention of illegal copying of software
- security reviews of IT systems: regularly check compliance with the technical security standards for IT facilities
- IT audits: carefully plan and execute the audits in the information processing environment so that the organization and responsibilities are clear; the audit activities are laid down and interference with production is kept to the minimum. The knowledge and level of experience of the IT auditors must be monitored
- audit tools should only be available to authorized employees.

3.2.6 ACT: Maintaining Information Security Management

Security has to be maintained. The reasons to enhance security can come from incidents reports, vulnerability assessments, audits, trends in risks and developments within the market and the customers' business environments.

Risk assessments should be updated as part of risk management on a regular basis. The risks in the outside world as well as within organizations are constantly changing, and controls in place may gradually become obsolete due to developments in IT.

It is advisable to repeat the risk assessments regularly. This is even more important after major changes in infrastructure, in organizational structure, in processes or in operational goals.

Part of the maintenance effort has to be devoted to the descriptions of the 'to be' situation in plans and security handbooks. These descriptions have to be updated.

In this step it is a good practice to register the reasons for maintenance and all actions taken.

Objective
- to improve the 'to be' situation (PLAN). The 'to be' situation includes the agreements on security as specified in SLAs, the internal standards such as the Information Security Policy, the baseline, handbooks and Operational Level Agreements (OLAs), as well as the agreements with the underpinning contracts
- to improve implementation of specified security measures (PLAN, DO)
- to report to the customers on security performance.

Summary of activities
- analysis of the evaluation reports
- providing input for the PLAN sub process, the security plan(s) and the annual improvement activities
- providing input for the SLA maintenance activities (for the Service Level Manager) as well as for the maintenance activities on operational level agreements and underpinning contracts.

Management review as part of Information Security Management
A management review takes place to check the effectiveness and efficiency of the current implementation of controls/measures. The input to the management review should include information on:
- analyses from the collected incidents and vulnerabilities
- feedback from interested parties
- results of independent reviews/audits
- status of preventive and corrective actions
- results of previous management reviews
- process performance and compliance with information security policy
- changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment
- trends related to threats and vulnerabilities
- assessments of third parties/partners/suppliers; information security incidents and status of security
- recommendations provided by relevant authorities.

The output from the management review should include any decisions and actions related to:
- improvement of the organization's approach to managing information security and its processes
- improvement of control objectives and controls
- improvement in the allocation of resources and/or responsibilities.

A record of the management review, clearly stating management involvement and approval, should be maintained.

3.2.7 Reporting
Reporting is an inevitable part of Information Security Management; it is necessary to provide assurance, to give insight on the current status and to account for the current achievements.

Objective

The objective is to provide the customers or the organization with relevant information on information security.

Summary of activities

In general, the Information Security Management process provides reporting data to the Service Level Management process. Service Level Management takes care of the communication with the customer.

Possible regular reports and reportable events are:

- reports on the PLAN sub process:
  - reports on conformance to the SLAs and internal standards including the agreed key performance indicators (KPIs) for security
  - reports on the status of the controls: as long as there is evidence that controls are working, the desired level of security should be met.
  - reports on underpinning contracts and defined non-conformity in their fulfilment
  - reports on OLAs and policy statements
- progress of the security improvement plan and other annual plans
  - regular reports on the DO sub process:
  - status of information security such as implemented measures, education and reviews including self assessments and risk analyses
  - overview of security incidents and the reaction to these incidents, compared to a previous time frame
  - status of awareness programs
  - trends on incidents by system, by process, by department, etc.
- reports on and of the CHECK sub process:
  - results of audits, reviews and internal assessments
  - warnings, vulnerabilities, trends, new threats, et cetera

Specific reportable events:

- for certain security incidents, the Incident Control or Service Desk and the Security Manager should have a direct channel to the customer's representative. This is part of the alerting/ escalation procedure, which goes beyond the normal reporting procedures.