



**Functions in
information security**

Foreword	2
Management summary	4
1. Historical Development	5
2. Concepts and frameworks	6
3. Basic principles	9
3.1 Responsibilities	9
3.2 Separation of tasks	9
3.3 Outsourcing ICT	10
3.4 Function demarcation	10
4. General functions in relation to the Code of Practice	11
5. The IS functions	12
5.1 The six IS functions and their position	13
5.2 Applying the organization model	14
5.3 The six IS functions in more detail	15
5.4 Related functions	18
5.5 Specialist functions	21
5.6 Team formation	22
6. Function profiling	23
6.1 Result areas	23
6.2 Function model	25
6.3 Function profiles	26
6.4 Growth paths	32
7. Education	34
Appendix: Overview of skills as part of competencies	35
Literature	36

There is a great lack of clarity about functions in information security (referred to as IS functions in the following). The international literature, legislation and in practice in organizations, throw up an enormous assortment of function names and titles. You also often wonder to what extent the same kinds of functions are involved. When is it a technical function, and when is it a function that puts more emphasis on organizational and management aspects? And if the nature and levels of functions differ, how are they connected? How do they relate for instance to related functions in the field of security, risk or continuity management? What requirements should actually be made of functions, and what can a career path look like in information security?

All these questions formed the incentive for applying some order and profiling. Another motive is the fact that more and more kinds of courses are offered through regular education as well as by commercial institutions that aim at supplying or retraining professionals in the field of information security. A question must be posed there too: what kind of training is suitable for which function?

Organizations and educational institutions want clarity, and that applies equally to professionals operating in this discipline. A workgroup consisting of members of PvIB (the former Genootschap van Informatiebeveiligers (GvIB) and the Platform Informatiebeveiliging (PI)) has therefore given itself the task of developing this function profiling into a vision paper. An Expert letter devoted to this issue at the start of 2005 was followed by an evaluation of function descriptions from real life in a Security Café. This vision paper is the resulting follow-up product. The draft of this vision paper was submitted to the board and members of the GvIB and PI, as well as to representatives of related professional bodies, training institutes and other interested parties. Points for discussion were distilled from the many reactions and discussed in a workshop with workgroup members and colleagues. This final version was drawn up on the basis of that workshop. The result is a document supported by colleagues that can be of assistance to organizations and educational institutions. This vision paper targets not only colleagues and related functions, but also management and Human Resource Management (HRM) functions with responsibility for the setup, acquisition and selection of the IS functions.

The members of the workgroup that drew up this vision document are:

Bart Bokhorst RE RA, Belastingdienst [Tax department]
 Drs. Fred van Noord, Verdonck, Klooster & Associates
 Drs. Gerda van den Brink-Heikamp RE, 3A - Audit en Advies op Afstand
 Drs. Leo van Koppen MSIT, Academie voor ICT en Media Zoetermeer
 Ing. Renato Kuiper, LogicaCMG
 Ing. Sebastiaan de Looper, Ernst & Young
 Dr.ir. Paul Overbeek RE, KPMG
 Lex Pels, Capgemini
 Ir. Jeroen de Waal from Zuidema Personeelsmanagement supported the workgroup as a consultant on function profiling.

How to read this document

First of all we sketch out the historical development, touching on the growth phases of information security. Chapters 2 and 3 define general concepts and starting principles that are definitive for the context in which the IS functions operate and the way people regard these functions. In chapter 4 we discuss the people in management who are responsible for information security on the basis of the Code of Practice for Information Security Management. Chapter 5 then explains the IS functions identified, their positions in large and small organizations, and their relationships with associated functions. We also examine the meaning of team forming for the IS functions. In chapter 6, we derive the result areas from the Deming circle and elaborate the function profiles. Chapter 7 briefly looks at growth paths and makes the connection to the educational courses.

Finally, the IS functions apply of course equally to women as well as to men.



Online collaboration

This book has been published on the knowledge sharing platform for security professionals: IBpedia based on the Creative Commons Licence 3.0.

For the English version of this Wiki-book see:

http://www.ibpedia.nl/index.php?title=Wiki-book_Functions_in_information_security

For the Dutch version of this Wiki-book see:

http://www.ibpedia.nl/index.php?title=Wiki-boek_Functies_in_de_informatiebeveiliging

Register yourself within <http://www.ibpedia.nl> and have fun complementing and using the above Wiki-books for your own purpose !

The discipline of information security has really taken off over the past few decades. This is closely connected to the ever increasing importance of computerized data processing and the corresponding risks for the sound, confidential and untroubled provision of information. The risks have been given an extra dimension by the explosive, worldwide growth of electronic data exchange between people and organizations. For many organizations, ICT has assumed a significant proportion of the primary process. Managing information security risks has resulted among other things in a range of specialist fields within the discipline. Because the discipline is so broad and it interfaces with many other disciplines like IT audit, risk management, security and continuity management, a huge diversity of functions and function names has arisen. The ensuing confusion of concepts that has arisen and the overlap of function areas damage the professionalism that must be applied in working on information security. Applying this professionalism is not only meaningful for managing risks, but also provides opportunities for using new possibilities for electronic services, aided by the expertise of information security functions.

The function profiles worked out in this document are intended to support professionals in information security as well as management of the organizations they work for, in reaching a further phase in the road to maturity of the discipline.

A few criteria must be highlighted when we distinguish functions in information security:

- business versus ICT;
- strategic, tactical and operational;
- generalist versus specialist.

Six main functions have been designated on this basis. Together, they can provide a balanced division of tasks in an organization. Because organizations differ in size, complexity and the importance they attach to information security, this vision paper pays a lot of attention to the possibility of positioning functions in organizations and the relationship with other functions in adjoining disciplines.

A fundamental condition of the successful implementation of information security in an organization is the division of responsibilities and authorities for deciding, advising and controlling information security measures. That is why we have chosen a broad approach for mapping out the functions that play a part in this. That is the only way to obtain sufficient clarity about the demarcation of those functions, which are ultimately described in a profile in terms of result areas and competencies. This also makes it possible to make the translation to one's own organization and to the educational needs in all kinds of ways.

Finally, the paper points out the growth paths for the functions identified.

From supporting role to leading role

Over the past few decades, information security has developed from 'nice to have' to 'must have' for many organizations. In the sixties, the discipline first developed along the lines of the jerky development of ICT. Now that ICT is fully integrated into the business processes, information security is following the development in those business processes, focusing more precisely on the external meaning of those business processes. That development is outlined briefly below.

IT security

Early in the sixties and seventies, ICT had a purely supporting role for the primary processes. Almost all control measures were still located 'normally' in the business processes. Activities in the field of information security were outsourced to the 'head of the computing centre'. Physical security was important, procedures for input and output and instructions to the computing centre, but technical security was the focus of attention. It was mainly directed at logical access security and back-up.

Information security

The link between technology and the rest of the organization became increasingly clearer. The cooperation with the other supporting functions came to be seen as essential. These frameworks are known as (the Dutch acronym is PIOFAH): Personnel, Information Systems, Organization, Finances, Administration and Accommodation. The special attention to 'information security' is often drawn from IT with the Chief Information Officer (CIO) in the main role, but there are 'contacts' in each framework who have the responsibility of implementing information security within their framework. The connection to the primary processes was extremely loose. It was only properly evident in the area of management of authorizations. Information security was oriented towards measures, and did not do enough with the actual risks.

Risk management – service-oriented

The concept of service provider made its appearance. In line with the history, the first thing to receive attention was the risks, from the perspective of the service offered. The risks analyzed were those inherent to a service and to the provider of that service. The consumer of a service, the 'user', was not yet in the picture, nor was the fact that the risks in the use by the user were also relevant. As the object was an IT service, for the most part IT took the lead in this form of risk analysis. Process thinking became increasingly important at this stage.

Risk management – oriented towards organization or customer

Then the gap to the primary processes was closed. Risk management places the risks to the primary processes in central position. Risk management spreads out and covers the entire organization. We talk about enterprise risk management. Risk management's place in the organization shifts upwards. Usually the Chief Financial Officer (CFO) or Chief Executive Officer (CEO) holds the portfolio for risk management.

Compliance management

Organizations are less and less stable, isolated islands. Processes develop over many businesses in chains, interwoven to a greater or lesser extent. The necessity of having some insight into those dependencies, and the associated risks, is becoming increasingly clear. Increasing internationalism also makes it more and more important to maintain a view within organizations on what is being done in all corners of the business, or what is not actually being done. This is only possible if responsibilities are fulfilled at a low enough level and the reports get to a high enough level in the organization. Another motivation is the increasing influence of interested parties in the form of shareholders and other financiers, commissioners and supervisors. All these developments have resulted in agreements in the shape of external legislation, and also internal policies or rules that must be accounted for. Responsibility for meeting the agreements is primarily laid down in the business processes with the responsible managers. These managers then give account and declare they have met the agreements. External responsibility can also be achieved on the basis of consolidation and enrichment of these declarations. Compliance management not only indicates the extent to which you can be 'in control' with respect to the agreements and rules, but also whether this control is demonstrable.

Changes to functions

The area of attention we call information security has been enlarged over the past five decades with new functions. That provides interesting possibilities for career paths. The IT security officer of the past can now be a compliance officer. The old functions continue to exist, but will have to cooperate with different, new functions.

This vision paper does justice to the diversity of functions encountered in organizations and that is why our starting point was focused on IS functions being understood as part of a large whole and not isolated.

Before analyzing the functions we can distinguish in the discipline of information security and working them out according to different points of view, we will first have to make clear what we mean by information security. We need to determine which demarcation we use, partly because we have to be able to distinguish between related functions. We can define information security as follows:

Information security means defining, implementing, maintaining, preserving and evaluating a cohesive set of measures that guarantee the availability, integrity, confidentiality and controllability of the (manual and computerized) provision of information.

Processing data with the intention of providing information for the purpose of running organizations and being able to justify the administration performed is not restricted exclusively to ICT, but plays just as important a part for users of ICT where manual data processing occurs. Manual here means employees performing administrative procedures that cannot be separated in most cases from computerized processing.

We will briefly discuss a few related concepts below that are regularly associated with information security, but that strictly speaking do not come under the definition of information security and that are therefore not included here in the profiles of the IS functions.

The Beveiligingsvoorschrift Rijksdienst 2005 [Security regulations for the Public Service 2005] positions the concept of integral security for the Dutch national government; from these instructions an integral vision of the security of the public service must be made into a balanced whole of organizational, personnel, structural and electronic measures for the protection of the primary interests of the national government: people and information. Safety and Health are part of it, and encompass the in-house emergency service, firefighting, working conditions and the application of environmental measures. Public security as a concept is also pushed more and more at training institutes where the concept of integral security is connected to it straight away again. Because there are various separate functions anchored in associations and training courses for promoting aspects other than information security, for the time being there is no need to use this broader concept of security as a basis. Moreover, with integral security what is mainly concerned is a managerial concept whose purpose is to combine several disciplines and that can be expanded in any kind of organization or sector with one's own features. In this vision paper we consider the positioning of IS functions but not the decisive factors for the organization and the management of the information security. A separate expert group of GvIB and PI will tackle that subject.

Integrity can also relate to sound acting in general, as intended in official integrity in governments or the prevention of improper use through insider trading at the stock exchange and financial institutions. We classify the responsibility of taking measures in this field in the discipline of compliance.

You cannot deduce from the definition of information security where the measures should be taken that are decisive for guaranteeing the four aspects mentioned in the definition of information security. Obviously this will also contribute to the scope of the IS functions. From the 'best practices' such as the Code of Practice for Information Security Management, we can derive the object areas in which those measures are taken. See table 1.

Object areas of information security
Policy (for plans, standards, classification)
Personnel and organization
Communication (for raising awareness)
Buildings and rooms (for physical security)
Technical infrastructure
Applications (setup and processing)
ITIL processes (management and exploitation of ICT services)
System development
Information Security incidents
Business continuity management
Internal control and audit

Table 1 Object areas of information security

This clearly illustrates that promoting information security demands a broad orientation. This is expressed in another way through the (international) standards and legislation that increasingly will determine the discipline. Figure 1 shows them in a hierarchical arrangement.

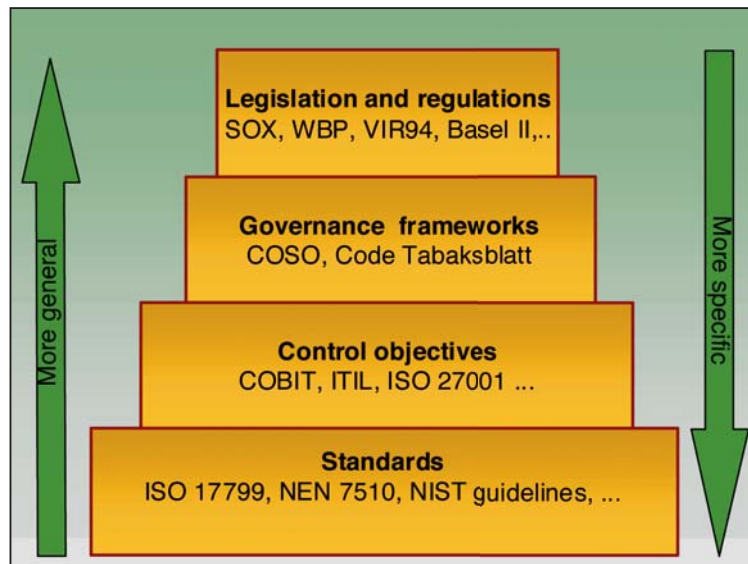


Figure 1 Frameworks determining the hierarchy for information security (adapted freely from Gartner)

The overview below summarizes the most important frameworks for information security.

Legislation and regulations:

- Government Departments Data Protection Regulations Decree 1994 (VIR) (currently under revision). Gives a limited number of general control principles for information security and positions the A&K Analysis.
- Personal Data Protection Act (WBP) 2001. Gives rules for the protection of the privacy of persons. This law is the basis for more detailed interpretation of the task area of the Data Protection Officer by means of a Guide in 2001.
- Government Departments Data Protection Regulations – special information (VIR) 2004. Gives security measures per classification level for state secrets and departmental confidential data.
- Government Departments Security Instructions 2005. Organizes the tasks of the security officer (BVA in Dutch) and security coordinator.
- Sarbanes-Oxley Act of 2002 (SOX). This law lays down rules for businesses listed on an American stock exchange (and its foreign branches, or a foreign business with a listed office) and has consequences for information security measures.
- Basel II. Contains legislation on a European level and among other things, obliges banks to limit operational risks such as fraud concerning systems, people and processes or failure of systems.
- Other laws. For instance, the Computer Crime Act, the Telecom Act, the Public Records Act, the Copyright Act and the Electronic Signatures Act.

Governance frameworks:

- COSO 'Internal Control - Integrated Framework'. A world standard for internal control that focuses on establishing an unambiguous concept definition for internal control and drawing up a standard for the evaluation of internal control systems.
- Tabaksblat Code (Dutch Corporate Governance Code). Contains both principles and concrete stipulations that the persons involved in a company (including board members and commissioners) and parties (including institutional investors) must adhere to with respect to each other. The principles can be understood as general ideas about good corporate governance. The principles are worked out in concrete 'best practice' provisions.

Control objectives:

- Control Objectives for Information and related Technology (CobIT), version 4 is a process-oriented management instrument for the control of the entire IT environment and covers all aspects of information and the supporting technology.
- ITIL is a process-oriented 'best practice' approach for IT management. Within the ITIL framework, the Security Management process provides the structural coordination of security in the administration organization of ICT. ITIL Security Management refers to the Code of Practice for Information Security Management for the norms and measures.
- ISO/IEC FDIS 27001:2005 Information technology - Security techniques - Information security management systems – Requirements. A management framework of which ISO/IEC 17799: 2005 (see below) is a more detailed elaboration and that is used for certification among other things.

Norms and measures:

- ISO/IEC 17799: 2005 Information technology - Security techniques - Code of practice for information security management. This is the de facto standard/best practice for the discipline.
- The National Institute of Standards and Technology (NIST) provides free of charge comprehensive and up-to-date implementation guidelines for the information security of

3.1 Responsibilities

Information security is primarily a responsibility of (line) management and the IS functions support management in this. The manager is the sole person who can decide responsibly about the possibly contradictory interests between information security, efficiency in the performance of processes and the user-friendliness of information systems. Information security can result in restrictions on the use of ICT tools and data, even though organizations also have an interest in open communication and user-friendly applications. Investing in ICT and meeting deadlines often requires making the difficult choice between information security, functionality and timely delivery. In addition, building in information security measures at a later phase usually requires much more effort. One of these days is none of these days.

Complying with information security measures often provokes resistance in users of information and information systems in connection with the limitations on access. Only management has the possibilities to introduce those restrictions into the daily work routine of the staff and to maintain them.

Finally, information security cannot be separated from the context in which the measures must function, so that no separate primary responsibilities (separate from that context) can be defined for it. This applies not only on management level, but also on the executive level.

A few examples to illustrate this point:

- reception receives visitors to direct them to their destination, so it is meaningful to make only reception responsible for issuing entry badges;
- it is only the system designer who can meaningfully translate the functional requirements for integrity controls into a functional design, while only the programmer can actually incorporate them in the software;
- users also have their own responsibility in complying with codes of conduct for keeping their passwords confidential.

Information security is an integral aspect of everyone's function, so that in the end everyone is proportionally responsible for the information security aspects assigned to their own function or area of responsibility. The IS functions are intended to make that assignment of responsibilities within an organization more explicit, to support it and to encourage the purposiveness and balanced coherence of the measures. The IS functions will continually evaluate the dynamics of organizations and their environment.

3.2 Separation of tasks

Management will delegate tasks and authorities (not the final responsible persons) to other functions. In doing this, management must ensure that the possibilities for creating opposite interests in the organization are used efficiently and effectively, following on from the existing work division. This will foster compliance (complying with legal, social and contractual obligations).

As far as assigning tasks and authorities in information security is concerned, this means the following:

- separate policy preparation (in this instance, planning and standardization or instructions) and execution (including the daily monitoring) of measures;
- by analogy, separate functions that determine formal rules and design functions within the architecture;
- separate decisions about measures from advice, supervision or control of those measures;
- separate primary advice and supervision from primary control;
- if the scale size is large enough, separate functional tasks from technical tasks.

Supervision versus control

Supervising is not the same as controlling. Someone who provides advice or makes standards without checking (supervising) whether they are understood and complied with by the persons concerned, eventually ends up in a vacuum with their work, because they do not get any feedback. Supervising the compliance with advice or standards can take place through one's own observations, through discussions with the persons involved or by studying documentation. It can also be done indirectly by using controls set by other people. Supervision does not aim primarily at giving an objective and independent judgment. In organizations, especially in the framework of compliance, the need for this is very evident. This kind of judgment requires expert knowledge with regard to control and an independent position. An employee whose primary job is advising and supporting others in the selection of measures is not in the ideal position for making an independent and objective assessment of whether the correct measures have been taken, because they can come up against their own recommendations. A controller who also wants to give advice, will have to limit their advice to the omissions they perceive from their controlling function, and will have to keep their advice open and global, allowing management to make the choice.

Giving a mandate

In the light of the above, it is important to consider the mandating of IS functions. Management can considerably improve the effectiveness of an IS function, for instance by having procedures include approval by the IS function of milestone documents of the process and system development and risky changes to the ICT exploitation process before these developments and changes go ahead. The organization must properly understand these approvals, because they may not contain any function of decision. If an IS function rejects a milestone document, this must be regarded as a negative advice to management, who will take the final decision about whether or not to give approval. For that matter, this final decision can be delegated to a steering group or Change Board, where all the interests are represented and the different aspects can be weighed up in their mutual connections, so that a balanced decision can be made.



3.3 Outsourcing ICT

The effect of the function profiles is transparent to outsourcing ICT. On the one hand, outsourcing means that the IS functions are simply outsourced along with the rest and do not change as such. On the other hand, some tasks of IS functions will have to be executed differently as a result of outsourcing. Communication patterns in particular will have to be different, and there will be significantly more emphasis on the contractual organization of mutual relations. At the same time, we can also state that it is possible to work on a mutual contract basis within large organizations as well, minimizing the difference with outsourcing. Furthermore, partial outsourcing of ICT services occurs frequently, especially in the ICT organization.

A short list of the areas of interest connected to this will suffice at this point:

- include requirements in the area of information security in requests for offers;
- make agreements about information security, including governance aspects in contracts;
- consult about service level reports and accountability about compliance to information security norms;
- evaluate and adjust the contractual provisions.

3.4 Function demarcation

In practice, organizations have all kinds of employees whose functions include security or equivalents in the designation.

Examples:

- Security Administrator: the officer who manages the logical access security of a platform.
- Security officer: the officer in uniform, who provides reception and surveillance services.
- Registered Security Expert (RSE): the specialist in protecting persons and objects (or having them protected).

The question is what determines whether this is an information security function as referred to in this vision paper. Although it is difficult to stick to sharply delineated criteria for this purpose, the most important consideration is that it must be a function that fits in the definition of information security at any rate (see 2.2 Concepts and frameworks).

The concept of 'function' is central to this paper. That raises the question of whether we can talk about a role. And in that case, when can we talk about an occupation?

Occupation, function, role

The Nederlands Genootschap van Informatici (NGI) [Dutch Society of Informatics] has a workgroup for Functions in Administrative Information Science (WFBI) that is in charge of the NGI publication 'Tasks, functions, roles and competencies in informatics'. This workgroup puts it the following way. An occupation is the generally distinguished designation for the whole of activities considered to belong to the activities to be performed by the practitioner of that occupation. Distinct from the concept of occupation is the concept of function, seen as a designation specific to an organization or sector for the whole of someone's professional activities. That means you also have a function role, function results and function profile. A role represents the position that its holder assumes with respect to certain activities, such as execution, leadership, research or advice. A role can demand particular (role-) specific competencies and partially determine the distinction between professional levels. We add that a role is often linked to the execution of certain related activities in a process. This fits in with the control of logical access security, where the concept of role is also used.

For the time being, the concept of function fits best with the objective and selected approach of this vision paper. All the same, in situations on a smaller scale than that on which this document is based, the functions distinguished here can often be performed as a subtask by another function. That is why people talk about fulfilling a role in many organizations. If a part of the tasks belonging to the functions is performed, this vision paper will call it task area in order to preserve the distinction with role.

The primary executive responsibilities for information security are part of functions that can generally be indicated in organizations. To that end, table 2 itemizes the object areas for information security as they emerge in chapters and sections in the Code of Practice for Information Security Management (ISO/IEC 17799: 2005).

The tasks that belong to these primary responsibilities are, in brief:

- giving the order to take information security measures;
- ensuring that these measures endure or are adapted to changed circumstances;
- setting up internal monitoring of the compliance with the measures, insofar as they are part of human action.

Chapters in the Code	Sections	General functions	
5 Security policy		Member of group's board of directors	
6 Organization of information security		Member of group's board of directors	
7 Asset management		Designated owner of those assets	
8 Human resources security		HRM head	
9 Physical and environmental security	9.1.1 Physical security perimeter	Head of Facilities Services	
	9.1.2 Physical entry controls		
	9.1.3. Securing offices, rooms and facilities		
	9.1.4 Protection against external and environmental threats		
	9.1.6 Public access, delivery and loading areas		
	9.2.1 Equipment siting and protection		
	9.2.2 Supporting utilities		
	9.2.3 Cabling security		
	9.2.4 Equipment maintenance		
	9.2.1 Placement and protection of equipment		Member of ICT management team
9.2.2 Support equipment 9.2.4 Maintenance of equipment	Operational managers supported by HRM		
9.2.6 Secure disposal or re-use of equipment			
9.2.7 Removal of property			
9.2.5 Security of equipment off-premises	Member of ICT management team		
9.1.5 Working in secured areas			
10 Communications and operations management	10.1 Operational procedures and responsibilities	Operational managers supported by HRM	
	10.2 Third party service management		
	10.3 System planning and acceptance		
	10.4 Protection against malicious and 'mobile code'		
	10.5 Backup 10.6 Network security management		
	10.7 Media handling		
	10.10 Monitoring		
	10.7 Handling media		No unambiguous assignment
	10.8 Exchange of information		Operational managers supported by HRM
10.9 Electronic commerce services			
11 Access control	11.1 Business requirements for access control	Member of group's board of directors or member of the Business Unit management team	
	11.3 User responsibilities	Operational managers supported by HRM	
	11.2 User access management	Member of ICT management team (in coordination with member of group's board of directors or member of Business Unit management team)	
	11.4 Network access control		
	11.5 Operating system access control		
	11.6 Application and information access control		
12 Information systems acquisition, development and maintenance	12.1 Security requirements of information systems	Business Unit/Information management or process owner	
	12.2 Correct processing in applications	Lid management team ICT Member of ICT management team	
	12.3 Cryptographic controls		
	12.4 Security of system files		
	12.5 Security in development and support processes		
	12.6 Technical vulnerabilities management		
13 Information security incident management	Member of the group's board of directors or member of the management team		
14 Business continuity management	Member of the corporate group's board of directors or member of the Business Unit management team		
15 Compliance	Member of corporate group's board of directors (in coordination with member of ICT management team)		

Table 2 Indication of the primary task division for information security.

5.1 The six IS functions and their position

The IS functions and their positioning are worked out on the basis of large and complex information-processing organizations. Consider banks and insurance companies, large industrial multi-nationals and huge government implementing bodies, where applying ICT occupies a central position in the primary business processes. The issue of demarcation (who does what), of coherence (how do functions fit each other) and coordination (which functions give direction to the others) arises pre-eminently in large organizations. We decided not to use a growth or maturity model to show how the variety of IS functions arose, because in practice as well as theoretically, many development paths are followed. In addition, there will be smaller, mature organizations that can manage quite well with just one or two IS functions. The largest common denominators of the functions that can be found in large, complex organizations can be positioned in a simple schematic picture of an organization (see figure 2).

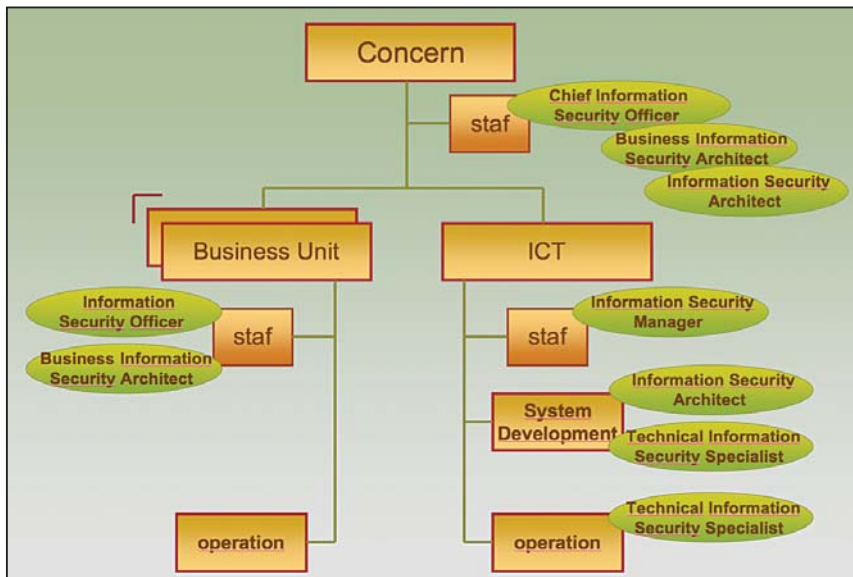


Figure 2 Positioning IS functions

This schematic picture of an organization identifies the following functions with their abbreviations and Dutch names; the functions are further explained in 5.2:

IB-functies	Afk.	Nederlandse namen
Chief Information Security Officer	CISO	Concernmanager Informatiebeveiliging
Information Security Officer	ISO	Functionaris Informatiebeveiliging
Business Information Security Architect	BISA	Procesarchitect Informatiebeveiliging
Information Security Manager	ISM	Manager Informatiebeveiliging
Information Security Architect	ISA	Informatiebeveiligingsarchitect
Technical Information Security Specialist	TISS	Technisch Informatiebeveiligingsspecialist

Table 3 The IS functions

The Dutch names adhere as closely as possible to the international terminology. With respect to ITIL Security Management, we have added the term 'Information' to the function names used there (Security Manager and Security Officer); this fits in with our approach in making a distinction with the (physical) security functions.

We can identify two main features in distinguishing between the functions:

- the level of the organizational section (strategic, tactical or operational) and
- the sphere of action: business or ICT (or both).

The distinction into levels derives from the importance of central control of the aspect area. The distinction between the spheres of business and ICT has to do with the difference in the field of knowledge and the nature of the information security measures to be taken. Within the ICT organization, the Technical Information Security Specialist is considered to be an operational function that can perform as a designer or technical administrator. In large organizations, both on the side of business and ICT, there can be a need to set up functions on the operational level with corresponding tasks, like the Information Security Officer and the Information Security Manager. In those cases, you can make a distinction in the function name by calling them Local Information Security Officer (LISO) and Local Information Security Manager (LISM). Of course, as a result, on the tactical level the functions are more coordinating tasks. In our approach to distinguish between IS functions, we chose only to name functions within organizations. That will apparently not do justice to the consultancy functions that offer services in the area of information security to other organizations. We can note here that consultancy functions are usually called in to set off insufficient qualitative or quantitative staffing of the internal IS functions, or to perform one-off tasks as customized jobs that are not suitable for function profiling. The function framework we have developed can, however, be used as a reference in consultancy practice for delineating requested tasks. Moreover, it enables you to make a list to see whether any other IS functions are fulfilling tasks as a limiting condition. This makes it possible to prevent differences in the patterns of expectation between demand and supply.


5.2 Applying the organization model

On the basis of the relative maximum distinction between IS functions that was taken as a basic principle for this vision paper, it is an interesting question to see how these functions should be used in smaller organizations or in cases where information security is considered to be less important. In this vision paper we chose not to develop normative models with an optimum division of IS functions. That is because there are simply too many factors to identify that can influence the structure of an organization and therefore also the interpretation of the IS functions. We refer in this matter to the recently published Expert letter 'Setting up a security organization', for which many follow-up activities are planned. Instead, alongside the schematic diagram of the organizational positioning of the IS functions (figure 2) we have developed a relations table (see figure 3) that can be used for positioning IS functions in smaller organizations. The relations table is based on the general functions supported by the IS functions. Specialized functions will only arise if the scale of the organization is large enough, or the importance of the specialism requires it. The relations table only includes those general functions for which the IS functions primarily supply their support. That means the relations table has fewer general functions than table 2. Take note that not only managers are supported by IS functions, but also general executive functions.

Examples include:

- an information security architect supports an ICT architect and not the ICT management. The information security architect can be regarded as a specialization of the ICT architect;
- a security administrator is a specialization of a system or application administrator.

Smaller organizations might not use the distinction into three levels, but perhaps only use two levels, so the tactical IS functions are either not applicable or are shifted to the operational level. Creating a relationship with related functions that are also included in the relations table is important, because it makes it possible to merge different task areas into one function in smaller organizations. In large organizations for that matter you can think along the horizontal line in the relations table about team forming, with different specialisms reinforcing each other. We will examine this in more detail later in this vision paper. In practice you also come across functions, for instance based on instructions, in which a sub area of information security is practised as a specialism. Refer to the column Task areas of information security in the relations table. It can be part of the security process (see section 6.1), as a policy staff member can perform it, or part of the object areas, such as the Data Protection Officer. Technical Information Security Specialists in particular will be deployed in operational sub areas of information security. We will examine that in more detail later too.

Larger organisations **Functions specialism** 

Layers in organisations	General functions with Information Security task	Information Security functions	Task areas and subareas of Information Security
	STRATEGIC LEVEL		
	- Group's board member	- Risk Manager - Business Continuity Manager - Compliance Officer - Quality Assurance Manager - Internal or IT-auditor (do not combine with IS functions!)	Chief Information Security Officer - Information Security Policy Officer - Data Protection Officer (according to Privacy Act)
	- Enterprise Information Architect		Business Information Security Architect
	- IT-architect		Information Security Architect
TACTICAL LEVEL BUSINESS UNIT			
	- Managementteam member	- Internal Control Officer - AO (/IC) Officer	Information Security Officer
	- Information Architect		Business Information Security Architect
TACTICAL LEVEL / DEVELOPMENT ICT			
	- Managementteam member	- Internal Control Officer - AO (/IC) Officer - Quality Officer Information	Information Security Manager
	- IT-architect		Information Security Architect
OPERATIONAL LEVEL ICT			
	- System Specialist - Application administrator - Technical administrator		Technical Information Security Specialist - Cryptography Specialist - Security Administrator - CERT-Officer - Ethical hacker, etc.

Table 4 Relations table of functions in information security

5.3 The six IS functions in more detail

Chief Information Security Officer (CISO)

The Chief Information Security Officer acts on the highest management level and must therefore understand and speak the language of management in the first place. He communicates both with the corporate management as well as the management of business units and with the ICT management. The extent to which he himself must act as a direct superior depends on whether there is any central team formation of security officers, whereby employees from different backgrounds and with different specialisms must be managed. The Chief Information Security Officer provides functional direction to the work of the IS functions at the lower levels. He is clearly a generalist in the field of information security, who must be able to make the connections between the different business and security interests in general outline. He covers all object areas: see Table 1 Object areas of information security. He must be capable of uniting contrary interests, weighing up the recommendations from different experts and the interests of management on their own merit. All this is necessary to be a good advisor for the corporate management.

Information Security Officer (ISO)

The Information Security Officer works from the viewpoint of frameworks that are specified on corporate level. Of course he will be involved in the maintenance of those frameworks, but he concentrates mainly on compliance with them in the operational processes. The Information Security Officer derives his added value from his knowledge of the business unit and the transition required from general IS norms to the specific business situation. Those general IS norms relate above all to staffing and organization, communication (for consciousness-raising), buildings and rooms (for physical security), information security incidents and the interpretation of business continuity management in the business unit. Business

Information Security Architect (BISA)

The Business Information Security Architect, as a security specialist, works in the sphere of the business and processes. If he is performing on corporate level, the generic corporate applications of course take up a major place, such as Enterprise Resource Planning packages, functional aspects of Internet, mail, portals, electronic messaging services and suchlike. The Business Information Security Architect is mainly active in the first phases of process and system development. In the maintenance and evaluation phases of processes and information systems, he will supervise the preservation of the basic principles of information security.

The Business Information Security Architect can choose to perform his task from different points of perspective; see figure 7. He can supply and maintain an information security (partial) architecture and further advise and supervise its implementation in other architectures and in processes or ICT designs. Within this approach, the global design of generic security functionalities is a further fleshing out. Conversely, if the Business Information Security Architect positions himself in the first instance as an advisor and supervisor, that means that the function contributes to the embedding of information security as one of the quality aspects in all other architectures. This aspect must be made visible separately in the architectures and designs, for instance in a security section.

The basic principles formulated earlier are the basis for working out this function. In drawing up design frameworks at the highest level and supervising compliance with them, it is preferable to separate the design of sub architectures and functional designs in the area of information security. This incompatibility becomes most apparent when IS functionalities are being designed.

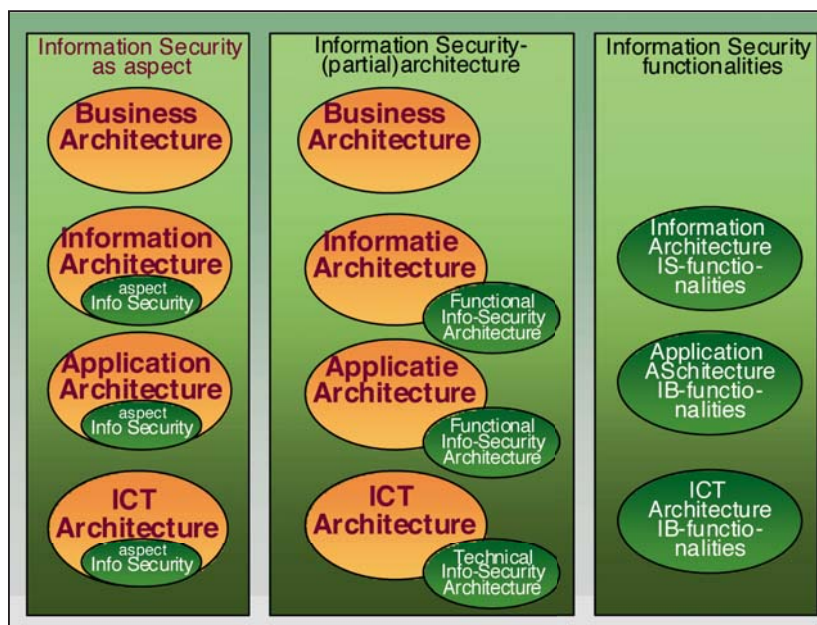


Figure 3 Perspectives on information security in relation to the architectures

Information Security Manager (ISM)

In the ICT sphere, the tasks of the Information Security Manager are similar to those of the Information Security Officer. However, he must not only guarantee the general corporate guidelines in the area of information security as they apply to Business Units, but also those that are specific to the ICT organization. Important areas of interest related to this are the internal administration and exploitation processes of ICT and the technical infrastructure. More than with Business Units, he can come up against outsourcing situations and the need to demonstrate for third parties that the

security norms are actually being complied with. What will also come up for discussion earlier is that he will have to give functional guidance to other IS functions. It's for these kinds of reasons that his function profile is based on more serious, competence requirements.

Information Security Architect (ISA)

The information given above for the Business Information Security Architect applies to a great extent to the Information Security Architect as well. As far as ICT is concerned, the difference with the Business Information Security Architect involves the technical orientation of the Information Security Architect and the greater emphasis on the technical infrastructure. Figure 4 shows this in a different way.

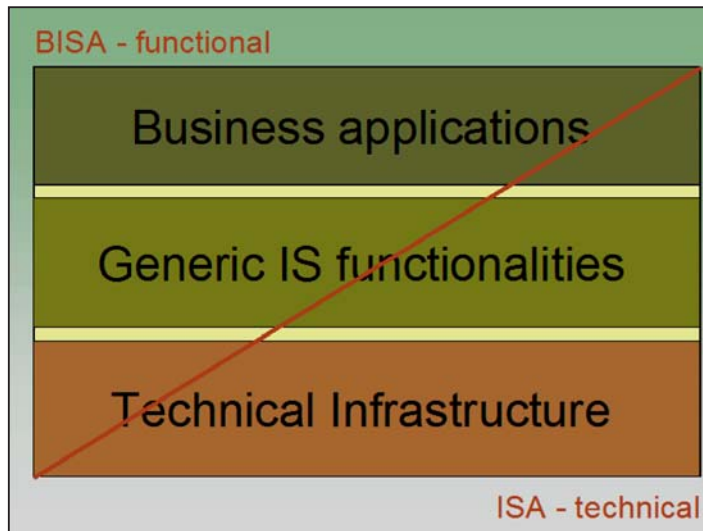


Figure 4 Connections and differences in IS architect functions

Technical Information Security Specialist (TISS)

In principle, the Technical Information Security Specialist performs tasks on the operational level within the ICT organization. In this vision paper, this function is an umbrella concept for a series of functions that are explained in more detail in section 5.5 Separate task areas.

5.4 Related functions

In practice, you can encounter a wide variety of related and/or overlapping functions according to scope, maturity or sector of an organization. To arrive at effective and efficient task performance (for the related functions as well), we need to delineate the connections and differences clearly. If you organize their mutual positions properly, functions can strengthen each other. However, they can also weaken each other if they perform each other's functions (partially and from different points of view), whether or not this happens deliberately. That is why we give a brief characterization of those related and/or overlapping functions, so that you distinguish them satisfactorily from the functions in information security. Figures 5 and 7 use core words to provide a highly simplified way of recognizing the connections and differences between the related disciplines and the IS functions.

The Risk Manager

The Risk Manager works in a wider sphere of action than information security, as risks are not only connected to data processing, but also inherent to day-to-day management. There are numerous business risks such as project, environmental, finance, product, political and social risks. The Risk Manager supports the various management layers in the organization in controlling these risks by facilitating risk analyses, getting the planning cycle up and running and keeping it going, and by supervising reports on the cycle. The application of ICT will form a major point for attention, in accordance with the business typology.

The Business Continuity Manager (BCM)

One of the things the Business Continuity Manager looks after is a sub aspect of information security. The aim of Business Continuity Management is striving for continuity of business processes in the event of calamities. The Business Continuity Manager will have business impact analyses and risk analyses performed and supervise them to underpin the continuity measures. That means that he will have to gear those activities properly with the Risk Manager.

The Business Continuity Manager concentrates especially on the repressive measures (limiting damage) in the area of availability, for all objects that must also be considered for information security, among other things. Other objects are related to means of production in the primary production process, for instance. Measures aimed at the safety of staff (such as evacuation) are also often included in the event of emergencies. The Business Continuity Manager will develop and maintain the tactical and operational guidelines with respect to the preservation of continuity. The Business Continuity Manager takes a major task area out of the hands of not only the Risk Manager, but also of the IS functions. This task area can be considered a separate specialist field, partly also given the company's own international standards and institutions. He will have to collaborate closely with the IS functions, because they serve the preventive availability measures (possibly can be better), due to their involvement with architectures and designs among other things.

The Compliance Officer

This is a relatively new and broader function than an IS function. It arose from the far-reaching regulations that organizations must or want to comply with. Compliance, the demonstrable adhering to regulations, can mean different things in different organizations. It can be about legal regulations, for instance concerning cartel formation, misuse of the market and in that respect, the Private Investment Transactions Regulations (Compliance Regulation of the AFM [Netherlands Authority for the Financial Markets]), sector-related rules (Basel II for the banks), contractor codes for Corporate Governance, rules applied independently (for example, ISO 900x series for quality in a general sense), internal policy and the fulfilment of contracts. On the basis of legal regulations (for example for financial institutions), the Compliance Officer can be assigned special powers for performing his task, especially for maintaining personal integrity of employees in sensitive functions. From the compliance approach, the control process for complying with rules by definition shows some relationship with the process of information security, where norms have to be complied with. Furthermore, certain regulations also imply rules for information security. Depending on the work area of the Compliance Officer, it will be necessary to do some fine-tuning with the IS functions.

The Quality Assurance Manager

Quality is about the properties inherent to processes and products, whereby information security can be seen as forming a subset of the whole of the aspects/properties that can be distinguished. If an organization is to satisfy a large number of normalized quality aspects, for instance because of legal, sector or market-oriented requirements, it can mean that the organization will have to set up a quality system with corresponding employees for advice and testing. In these kinds of situations it can be advantageous for information security to 'hitch a ride' in this action and integrate information security (partially) in it.

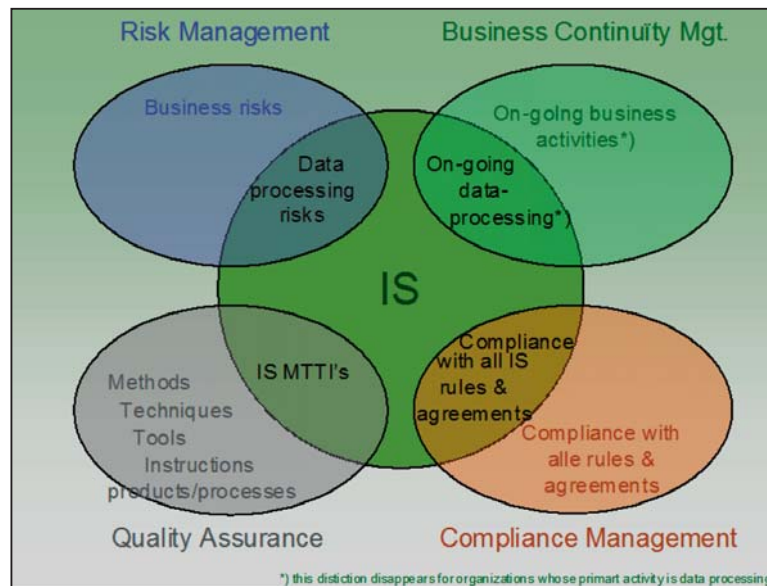


Figure 5 Connections and differences with related functions - 1

The Security Manager

The demarcation of the concept of information security in section 2 already made a link with the various other concepts of security that involve physical, public, personal, business or integral security. As an extension of that, just as many functions have come into being under the denominator of 'security', sometimes with different adjectives in the name. At any rate, there is an overlap with the object area of physical security. Depending on how you interpret the concept of security in an organization or sector, you may find more overlapping object areas.

What is needed, then, is mutual coordination. Collective reliance or control can be to each party's advantage, because more power can be applied to the scale this way.

The IT Auditor

The function of the (internal) IT auditor is primarily a verifying one. This is in contrast to the IS functions (except for the Technical Information Security Specialist) whose role is primarily consultative. The IT auditor covers at least the same object areas as those of the IS functions. If compliance with norms for information security is checked by (internal) general auditors in Business Units instead of by IT auditors, we make no distinction between them in this vision paper, for reasons of simplicity.

As a result of his findings, the IT auditor gives advice such that the persons with primary responsibility for information security can make the decisions about implementation themselves.

The IT auditor can basically perform his function in two ways, namely in a distanced manner whereby he must always be requested to perform an order, or in a proactive way, whereby on behalf of top management he keeps an eye on whether the information security norms are being complied with continually and provides advice about it. Conversely, if information security is certified, particularly for the benefit of third parties which is often the case with information security, a more distant task performance is more suitable. In that case, he will limit his advisory work as much as possible.



Figure 6 Different tasks for the same object area

The proactive interpretation of tasks by the IT auditor can mean that he (instead of the IS function) plays an approving role with respect to IS aspects in designs of ICT facilities or by performing audits on vital ICT projects for which he has a permanent order. From a management point of view he is expected to monitor important developments and arrange audits whenever he feels that is necessary from the perspective of business interests. For that matter, this requires an express mandate from top management and high availability of the function. For example, the IT auditor can also use the architectures as a framework for assessment.

The proactive approach is connected to the need of management to obtain certainty as objectively as possible that the correct IS measures are being taken on time. Let it be clear that the degree to which a proactive role of the IT auditor is demanded also depends on the business typology and the way the IS functions have been deployed and are positioned in the development path. The two functions can complement each other well, but their activities also overlap for a part. Good agreements will therefore have to be made about the mutual positioning.

Administrative Organization and Internal Control Officer

One employee who can be meaningful to information security in an entirely different way is the Administrative Organization and Internal Control Officer, hereafter referred to as AO/IC officer. This officer has a consulting role in the setup of business processes, while he also mainly performs registration tasks by systematically recording processes and sometimes work instructions as well. If process architects make the designs for the process organization, he will be more active on the operational level in an organization (section) and can perform an assessing role to ascertain whether the process description is complete and logical, matches other processes within an organizational section and for instance whether the requirements for separation of functions have been met. As a specialist in the field of operational processes and manual procedures he can take care of embedding the manual IS measures in the daily work processes. Finally, he can perform a supervisory role with respect to the timely and full documentation of process descriptions for organizational changes and the introduction of new or changed information systems. In short, an essential function for the management of a sub area of information security.

The IT Quality Assurance Officer

Many ICT organizations put the function of quality assurance officer inside the process of design and maintenance of processes and ICT facilities. The quality assurance officer concentrates on both the process of design and maintenance and the products issuing from it, such as phase documents. He is responsible for the Methods, Techniques, Tools and Instructions and provides advice on their application in the development and maintenance projects. Although he does not have to be a specialist for all aspects in the field of product quality, he is responsible for ensuring that it is included sufficiently in the designs. He also has a supervisory task in ensuring compliance with the instructions. In the event the quality assurance officer uses ISO 9126 as a basis for product quality in ICT, there will be an overlap and possible friction with product-oriented norms from information security because the definitions of sub aspects do not always correspond. The Quality assurance officer can at any rate perform the important task for information security of ensuring that the process-oriented IS norms are complied with. The two kinds of functions clearly have to coordinate their work together.

The Internal Control Officer (IC officer)

The officer responsible for Internal Control activities concentrates mainly on the routine checks on the effects of processes, that is the compliance of processes and procedures as documented by the AO/IC officer. Under certain conditions, the IT auditor can make good use of this function. As a result of his findings, the IC officer can also give advice. One way of dividing the work with the general IS functions could have the assessment or provision of advice upon processes being set up assigned to the task of the IS function because this function wants to monitor the whole of the IS measures as well as their mutual connections. This applies particularly to processes where ICT and information security are important. In that case, the IC officer can provide advice on compliance issues (the effects of the processes). The control findings of the IC officer form the input for the evaluation of the IS function.

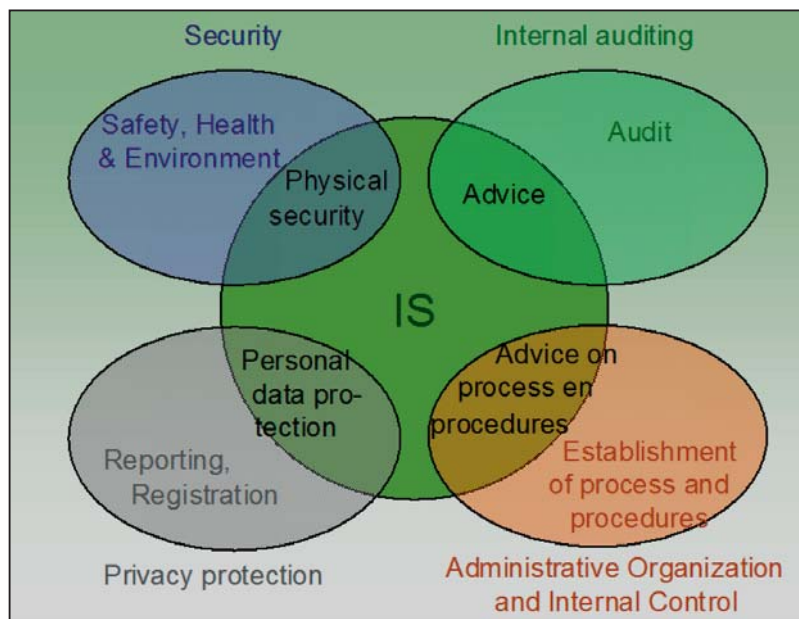


Figure 7 Connections and differences with related functions - 2

5.5 Specialist functions

The relations table (table 4) shows a number of functions that can be designated as specialisms within the IS functions. This can mean that parts of the tasks are perhaps performed in combination with other specific tasks, or that the tasks concentrate on specific objects or sub areas. Combinations of them are also possible. A few well known functions are explained in brief below.

Information security policy officer

In large organizations and government institutions in particular, special departments concentrate on developing and maintaining policy, while the execution of that policy is left up to operating companies or implementing bodies. In these circumstances, the Chief Information Security Officer will restrict himself mainly to the result area of Policy (see chapter 6).

Data Protection Officer (DPO)

Businesses, sector organizations, governments and institutions can appoint an internal supervisor for the processing of personal data themselves: the Data Protection Officer. Within the organization this officer supervises the application of and compliance with the Personal Data Protection Act (WBP) and has legal tasks and powers, thus giving him an independent position in the organization.

The Genootschap van Functionarissen van de Gegevensbescherming [Association of Data Protection Officers] provides a guide that describes the tasks, which we will summarize here:

Obligatory tasks:

- Supervision: the officer supervises the compliance with the legal rules about the processing of personal data in his organization. - Reports: the DPO has the legal task of drawing up a report annually of his activities and findings.
- Reports register: if an organization has appointed a DPO, the processing of personal data can be reported to the DPO, instead of to the Dutch Data Protection Authority (CBP).

Optional tasks:

- Inventory: the DPO can play a supporting role in listing all processing done in the organization and indicating what constitutes 'processing' in the sense of the WBP.
- Provision of information: within his organization, the DPO can provide information about handling personal data and give advice on issues related to processing personal data.
- Technology and security: the DPO can advise the organization on the realization of the suitable level of information security.
- Complaints handling and mediation: the handling of complaints about the use of personal data can be part of the range of tasks of the DPO.
- Development of norms: within an organization or sector a need can arise for norms/codes of conduct that are tailored to the specific processings within the organization or sector. The DPO can design those norms and codes of conduct.

Personal data is part of the data for which an organization takes information security measures. If the IS functions are fully implemented in an organization, a clear overlap of task areas can be observed. In principle, the task areas of the DPO can be covered fully by those of a Chief Information Security Officer or Information Security Officer. It's also possible, for instance, to place the DPO's tasks related to reporting, reports register and complaints handling with a member of the Legal Department, of course in close cooperation or collaboration with the IS functions mentioned above.

Manifestations of the Technical Information Security Specialist

The Technical Information Security Specialist can appear in many different object areas and in diverse processes. The need for his specialism will depend on the state of the technology, the scale of the work and the importance attached to information security. We suffice with an indicative summary. Known object areas include:

- cryptography;
- network security, including firewalls, intrusion detection and prevention, malware, information security in protocols;
- information security in applications;
- logging and monitoring;
- incident investigation and handling, for example by a Computer Emergency Response Team;
- logical access protection (Identification, Authentication and Authorization applications).

These object areas can come up for discussion in system development and maintenance, but also in implementation, administration and exploitation. That means that the Technical Information Security Specialist can appear as a designer, technical administrator, but also as a Security Administrator for logical access protection or certificate administrator for Public Key Infrastructures. One specific function implementation is that of Ethical Hacker. This function tests the protection of infrastructures and internet applications from an independent position in live situations, and provides advice to solve gaps that have been discovered. Another implementation is that of the Computer Investigator who needs sound knowledge of many of the object areas mentioned above and who can, for instance, also find his work area within private organizations.

It is less appropriate in this vision paper to attempt a full and up-to-date summary of these operational, specialized functions.

5.6 Team formation

In practice, teams of specialists from several disciplines are often formed to achieve synergy on various fronts. This can ensure that activities are better matched to each other, that mutual stimuli arise and that the same approach is followed in approaching the target groups, which are often the same. Unambiguous management of these kinds of specialists can also help an organization realize a major advantage. Usually a team will have a stronger position in an organization than an individual. A team can place itself more independently and profile itself better towards management on the various levels within an organization. And last but not least: a team can better absorb the disadvantages of extreme function differentiation. On the executive level, often you can no longer see the wood for the trees when you want some advice or a problem needs solving. Which of the many different kinds of specialists should you approach for advice?

Combining functions can relate both to the combination with related functions, and to the merging of IS functions themselves. The latter can be under discussion if an ICT organization or Business Unit is too large for a single Information Security Manager or Information Security Officer. If a team of IS specialists is formed, you create possibilities of specialization into the various object areas or into branches, departments or result areas. Good possibilities also arise within teams for following and supervising career paths, or preparing for IS functions elsewhere within the organization. It is important to pay attention to incompatible functions in team forming (see chapter 3 Basic principles). Team forming will have consequences for the organic place. It is preferably neutral with respect to the most important interested parties to avoid preferential treatment or unbalanced influence by one organizational section. At the same time, the organizational distance can form a certain risk in the acceptance of guidelines, recommendations or outcomes of evaluations.

6.1 Result areas

Tasks are grouped according to result areas for the description of functions. To identify the result areas of information security, we follow the process steps of the Deming circle: Plan – Do – Check – Act; see figure 8. The accents for each phase are not equal on the three levels of the organization. On a strategic level, 'Plan' is the most important, while on the tactical level it is 'Do' and on the operational level, 'Check'. Of course, the content of the phases in the cycle is different at each level, but they do have to fit together. This cyclic approach to the result areas in a function is only less applicable to the Technical Information Security Specialist, given the variety of deployment possibilities applicable to that function. There is also the remark that the Do phase for most IS functions means that they perform their advisory and supervisory tasks there, because the implementation of information security measures is in itself an executive task.

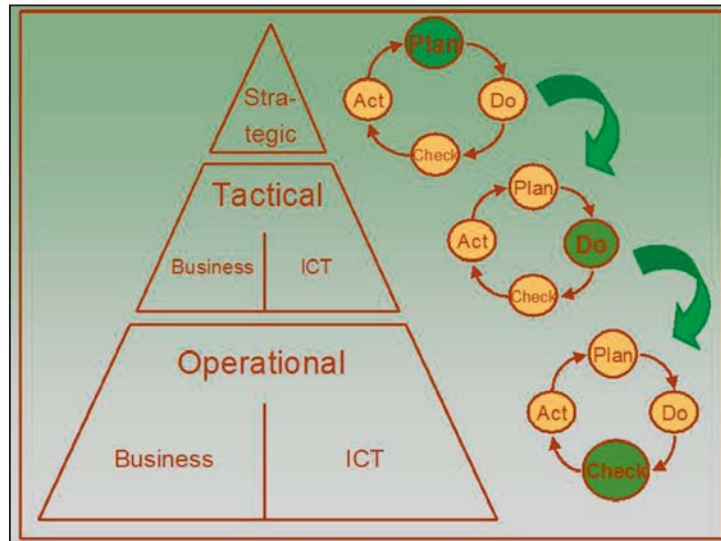


Figure 8 Result areas in the information security process.

The tasks of each result area are represented in keywords in table 5 below, with the names slightly adapted into more common terms for function profiles. The four process steps of the Deming circle are indicated with: Plan – Do – Act – Check. 'Manage' has been added as an extra result area.

Result area	Core concepts in setting tasks
Plan	<ul style="list-style-type: none"> - Draw up IS strategy and architecture - Develop IS norm frameworks and execution instructions - Make information security plan
Manage	<ul style="list-style-type: none"> - Functional management - Act as project leader of IS projects
Do	<ul style="list-style-type: none"> - Implementation of IS measures (only TISS) - Advise and supervise implementation of IS measures - Encourage IS awareness - Perform risk analysis
Check	<ul style="list-style-type: none"> - Take care that internal control and audits take place and findings are solved - Perform own investigation - Handle information security incidents
Act	<ul style="list-style-type: none"> - Adapt Policy - Adapt (recommendations) implementation of IS measures

Table 5 Task list of main outlines per result area

The function profiles of the IS functions identified in this vision paper are further elaborated in the following chapter.

6.2 Function model

Besides the result areas discussed above, the goal of the function is defined in one line as the core of the function profile preceding it. The function to which the function reports in theory is given, and the function context. By context we mean positioning the function in its environment and briefly mentioning the most important function elements and any special circumstances. The result areas are concisely worked out on the basis of table 5 and supplemented by a summary of the internal and external contacts that are maintained by the function. Finally the competences are worked out in terms of educational level, required knowledge areas and skills. The skills, relevant to all of the IS functions, are explained in more detail in the appendix.

6.3 Function profiles

Function name: Chief Information Security Officer (CISO) Department: Corporate staff Reports to: Member of the corporate group's board of directors			
Aim of the function:	Developing strategy and policy concentrating on information security, promoting and coordinating the development of execution guidelines and supervising the realization of the policy.		
Function context	Functions as independently operating internal policy advisor, accountable to the member of the corporate management team responsible for information security. Provides functional guidance to information security employees in the entire organization through control of internal reporting on the execution of the information security policy, compliance with execution guidelines. Must conquer resistance to have the policy and guidelines complied with, which are often experienced as an impediment to the execution of the work.		
Result areas	<p><u>Plan</u></p> <ul style="list-style-type: none"> - Forms his own view of the meaning of information security for the corporate group through continual creation of the picture concerning risks and solution directions for measures suitable for the corporate policy. - Sets aims for information security. - Develops a strategy to achieve those aims. - Develops a policy for the execution of the strategy and draws up a corporate policy and yearly plan, partly on the basis of the sub plans for information security. <p><u>Manage</u></p> <ul style="list-style-type: none"> - Gives functional guidance to Information Security Officers and Information Security Manager. - Acts as project leader or customer for corporate-wide projects in the field of information security. - Organizes and facilitates corporate consultation for control and coordination in the field of information security. <p><u>Do</u></p> <ul style="list-style-type: none"> - Promotes the development of execution guidelines and gives them direction. - Initiates information and IS awareness programs and gives them direction. - Initiates and facilitates risk analyses on corporate level. - Evaluates execution guidelines against the policy and if necessary, advises on improvement. - Prepares corporate decisions in the area of information security. - Advises corporate management, Business Units and ICT in policy (decisions) with consequences for information security. <p><u>Check</u></p> <ul style="list-style-type: none"> - Assesses reports from Information Security Officers and Information Security Manager about the compliance with the execution guidelines. - Assesses reports from internal and external audit bodies for relevance to information security. - Gives orders for execution of internal investigations and audit. - Maintains a central registration of information security incidents and their handling. - Assesses developments in society, the sector and the discipline. <p><u>Act</u></p> <ul style="list-style-type: none"> - Adjusts the IS vision, strategy and policy and encourages adjustment of execution guidelines on the basis of evaluations. <p><u>Contacts</u></p> <ul style="list-style-type: none"> - Internal: corporate management, corporate staff, management of Business Units and ICT, tactical IS functions. - External: auditors, sector and professional colleagues 		
Competencies	<u>Level of working and intellectual ability</u> - Masters <u>Knowledge areas</u> - ICT and information security (broad) - Organization of provision of information - Business processes (broad)	Skills	- Integrity - Leadership - Awareness of environment - Sensitivity to organization - Power of persuasion - Resistance to stress - Vision



Function name: Information Security Officer (ISO) Department: Business Unit Reports to: Member of management team or head of Business Unit			
Aim of the function:	Developing policy aimed at compliance with corporate frameworks for information security, supporting management in this and supervising the realization of the policy.		
Function context	Functions on behalf of the management of the Business Unit as independent advisor in the field of information security. Supervises compliance with the execution guidelines. Must conquer resistance to have the policy and guidelines complied with, which are often experienced as an impediment to the execution of the work.		
Result areas	<p><u>Plan</u></p> <ul style="list-style-type: none"> - Every year, draws up the information security plan for the Business Unit organization. - Contributes to the corporate policy plans for information security from the perspective of the ICT organization. <p><u>Manage</u></p> <ul style="list-style-type: none"> - If necessary, gives functional or direct guidance to Local Information Security Officers. <p><u>Do</u></p> <ul style="list-style-type: none"> - Actively disseminates execution guidelines in the field of information security in the Business Unit organization. - Advises on execution guidelines in the field of information security. - Initiates information and IS awareness programs and gives them direction. - Executes risk analyses within his field of competence. - Advises management of the Business Unit organization upon decision-making of the consequences for information security. <p><u>Check</u></p> <ul style="list-style-type: none"> - Assesses internal reports. - Assesses reports from internal and external control and audit bodies. - Advises management on performing of internal investigations and audits. - Maintains a registration of information security incidents and assesses their handling. <p><u>Act</u></p> <ul style="list-style-type: none"> - Adjusts the IS year plan on the basis of his evaluations. <p><u>Contacts</u></p> <ul style="list-style-type: none"> - Internal: Business Unit management on all sections, own Business Information Security Architect, Chief Information Security Officer and other Information Security Officers. - External: auditors. 		
Competencies	<u>Level of working and intellectual ability</u> <ul style="list-style-type: none"> - Bachelor <u>Knowledge areas</u> <ul style="list-style-type: none"> - information security - Business processes - Internal regulations 	Skills	<ul style="list-style-type: none"> - Perseverance - Integrity - Sensitivity to the organization - Power of persuasion - Progress monitoring

Function name: Business Information Security Architect (BISA) Department: Business Unit (possibly Corporate)			
Reports to: Member of the management team of Business Unit or head of Business Process Management			
Aim of the function:	Developing and keeping up to date of a vision or sub architecture for the aspect of information security in the Enterprise or Process Architecture as the realization of a part of the strategic IS policy and the positioning of generic security functionalities within it.		
Function context	Process architect specialized in information security. Translates policy frameworks for information security into Enterprise or Process Architecture and plays the role of both architect and advisor. Acts especially as process architect for generic security functionalities, for example in the area of logical access security, encryption, logging and auditing. Supervises the compliance with architecture principles for information security. Continually monitors market developments in the area of information security products.		
Result areas	<p><u>Plan</u></p> <ul style="list-style-type: none"> - Forms his own vision of the meaning of information security in the scope of the Enterprise or Process Architecture and takes into consideration the corporate strategy for information security. - Contributes to the corporate strategy for information security from the perspective of process development. - Contributes to policy-making and yearly planning for the execution of this strategy within his field of competence. <p><u>Manage</u></p> <ul style="list-style-type: none"> - Acts as project leader for projects in the field of information security. <p><u>Do</u></p> <ul style="list-style-type: none"> - Independently designs sub architecture of the Enterprise or Process Architecture for the domain of information security or contributes to making the aspect of information security more explicit as an integral part of this architecture. - Executes risk analyses within his field of competence. - Tests process designs against architectural principles for information security and if necessary, advises on improvement of those designs. - Tests designs for generic security functionalities against architectural principles for information security and if necessary, advises on improvement of those designs. <p><u>Check</u></p> <ul style="list-style-type: none"> - Assesses process-oriented developments in day-to-day management with possible consequences for IS aspects. - Assesses IT audit reports, reports about information security incidents and user evaluations of generic security functionalities. <p><u>Act</u></p> <ul style="list-style-type: none"> - Takes care of adjustment of the aspect of information security in the Enterprise or Process Architecture or its implementations on the basis of his evaluations. <p><u>Contacts</u></p> <ul style="list-style-type: none"> - Internal: Enterprise/Process architects, process designers, information managers, project leaders for process-oriented innovations, other IS functions, IT auditors. - External: Sector and professional colleagues. 		
Competencies	<u>Level of working and intellectual ability</u> <ul style="list-style-type: none"> - Masters <u>Knowledge areas</u> <ul style="list-style-type: none"> - ICT and information security - Organization of provision of information - Principles of architecture - Business processes (broad and deep) 	Skills	<ul style="list-style-type: none"> - Analytical ability - Creativity - Initiative - Awareness of environment - Sensitivity to the organization - Cooperation - Vision



Functienaam: Information Security Manager (ISM) Department: ICT Reports to: Member of management team or head of ICT			
Aim of the function	Developing policy aimed at information security within the ICT organization, supporting management, taking care of developing execution guidelines and supervising the realization of the policy.		
Function context	Functions on behalf of the ICT management as an independent advisor with a broad operating scope and as supervisor in the field of information security. Provides functional guidance to information security employees in the ICT organization through control of internal reporting on the execution of the information security policy, compliance with execution guidelines. Must conquer resistance to have the policy and guidelines complied with, which are often experienced as an impediment to the execution of the work.		
Result areas	<p><u>Plan</u></p> <ul style="list-style-type: none"> - Annually draws up the information security plan for the ICT organization. - Contributes to the corporate strategy and policy plans for information security from the perspective of the ICT organization. <p><u>Manage</u></p> <ul style="list-style-type: none"> - If necessary, gives functional or direct guidance to other IS functions within the ICT organization. - Organizes and facilitates consultation to coordinate measures and evaluations within the ICT organization in the field of information security. <p><u>Do</u></p> <ul style="list-style-type: none"> - Takes care of current execution guidelines in the field of information security. - Initiates information and IS awareness programs and gives them direction. - Performs risk analyses within his field of competence and on corporate level as a representative of the ICT organization. - Advises management of the ICT organization upon decision-making of the consequences for information security. - Supervises the compliance with recommendations/control findings in certification processes. <p><u>Check</u></p> <ul style="list-style-type: none"> - Assesses department and process reports within the ICT organization. - Assesses reports from internal and external control and audit bodies. - Gives orders for execution of internal investigations and audits. - Assesses or participates in the handling of information security incidents. <p><u>Act</u></p> <ul style="list-style-type: none"> - Adjusts the IS year plan and IS execution guidelines on the basis of his evaluations. <p><u>Contacts</u></p> <ul style="list-style-type: none"> - Internal: corporate management, corporate staff, management of Business Units and ICT, other IS functions. - External: auditors, sector and professional colleagues. 		
Competencies	<u>Level of working and intellectual ability</u> <ul style="list-style-type: none"> - Masters <u>Knowledge areas</u> <ul style="list-style-type: none"> - ICT and information security - Organization of provision of information - ITIL 	Skills	<ul style="list-style-type: none"> - Perseverance - Integrity - Leadership - Power of persuasion - Sensitivity to organization - Awareness of environment



Function name: Information Security Architect (ISA) Department: ITC Reports to: Head of System development/Architecture			
Aim of the function:	Developing and keeping up to date the aspect of information security within the ICT architecture that is aimed at satisfying the IS policy and the IS instructions as well as the generic security functionalities within the technical infrastructure. Also pertinent is making this architecture (system draft) applicable to the main features of the design and the maintenance of the generic security functionalities.		
Function context	ICT architect specializing in information security in relation to ICT. Translates policy frameworks for information security into ICT architectures and plays the role of both architect and advisor in doing so. Acts especially as ICT architect for generic security functionalities, for example in the area of logical access security, encryption, logging and auditing. Supervises the compliance with architecture principles for information security. Continually monitors market developments in the area of information security products.		
Result areas	<p><u>Plan</u></p> <ul style="list-style-type: none"> - Forms his own vision of the meaning of information security for ICT from the viewpoint of the corporate group through continual creation of the picture concerning risks and solution directions for measures suitable for the corporate policy. - Contributes to the corporate strategy for ICT in relation to information security. - Contributes to policy-making and yearly planning for the execution of this strategy within his field of competence. <p><u>Manage</u></p> <ul style="list-style-type: none"> - Acts as project leader for projects in the field of information security. <p><u>Do</u></p> <ul style="list-style-type: none"> - Independently designs sub architecture of the ICT complex for the domain of information security or contributes to making the aspect of information security more explicit as an integral part of the ICT architecture. - Acts as ICT architect for generic security functionalities. - Tests ICT designs against architectural principles for information security and if necessary, advises on improvement of those designs. <p><u>Check</u></p> <ul style="list-style-type: none"> - Assesses developments in the ICT market with respect to new IS risks and generic solutions from suppliers. - Assesses internal developments within the ICT with possible consequences for IS aspects in the ICT. - Assesses IT audit reports, reports about information security incidents and user evaluations of generic security functionalities. <p><u>Act</u></p> <ul style="list-style-type: none"> - Is responsible for adjusting the aspect of information security in ICT architectures on the basis of his evaluations. <p><u>Contacts</u></p> <ul style="list-style-type: none"> - Internal: ICT architects, ICT designers, ICT project leaders, other IS functions, IT auditors. - External: ICT suppliers and professional colleagues 		
Competencies	<p><u>Level of working and intellectual ability</u></p> <ul style="list-style-type: none"> - Masters <p><u>Knowledge areas</u></p> <ul style="list-style-type: none"> - ICT and information security - Principles of architecture - Standards concerning information security 	Skills	<ul style="list-style-type: none"> - Analytical ability - Creativity - Initiative - Awareness of environment - Cooperation - Vision



Function name: Technical Information Security Specialist (TISS) Department: ICT Reports to: depends on the work location			
Aim of the function	Performing development, administration or advisory work in an ICT organization that requires in-depth technical knowledge of ICT and information security.		
Funciecontext	This function can come in many forms and can only be indicated in general terms here. The meaning of the function is closely connected to the way it is deployed in the ICT organization and what the state of affairs of the technology and business or ICT typology demands. The core of the function involves the expertise to operate on the cutting edge of ICT technology and information security, as designer, advisor or implementer of (generic) security functionalities as well as in the daily administration of complex environments that require the maintenance of a high level of information security. Security functionalities can relate to logical access security, encryption, logging and auditing, protection of networks against intruders or malware, incident handling, live testing of the robustness of security and suchlike.		
Result areas	<p><u>Plan</u></p> <ul style="list-style-type: none"> - Not applicable. <p><u>Manage</u></p> <ul style="list-style-type: none"> - Not applicable. <p><u>Do</u></p> <ul style="list-style-type: none"> - Independently designs or administrates information security aspects of the technical infrastructure or (generic) information security functionalities in it. - Advises on the implementation of information security aspects of the technical infrastructure or (generic) information security functionalities. <p><u>Check</u></p> <ul style="list-style-type: none"> - Independently performs live tests to determine whether there are gaps with respect to the information security in the technical infrastructure or in combination with application software insofar as he is not involved in the design, implementation or administration of the environment to be tested. - Is involved in the analysis and handling of information security incidents. <p><u>Act</u></p> <ul style="list-style-type: none"> - Is responsible for solving weaknesses discovered from information security incidents and testing. <p><u>Contacts</u></p> <ul style="list-style-type: none"> - Internal: ICT architects, project leaders, designers and administrators, other IS functions. - External: ICT suppliers. 		
Competencies	<p><u>Level of working and intellectual ability</u></p> <ul style="list-style-type: none"> - Bachelor <p><u>Knowledge areas</u></p> <ul style="list-style-type: none"> - ICT and information security - ICT platforms - Technical standards for information security 	Skills	<ul style="list-style-type: none"> - Analytical ability - Creativity - Perseverance - Emphasis on quality - Capacity to learn - Result-oriented

6.4 Growth paths

We can distinguish three levels for the IS functions: strategic, tactical and operational, while the focus can be on the business or on ICT. This makes it possible to identify growth paths within the functions. It is also important to check which other functions are suitable for progressing through to the IS functions and vice versa. Because information security is a broad discipline that requires contacts to be made everywhere in the organization, it can be attractive to perform an IS function as part of a career path.

Of course, this does not have to mean promotion to a higher function; horizontal flow can be just as relevant, with information security providing a widening of the horizon.

Figure 9 shows a number of obvious growth paths. It must also be noted that it can be interesting for an IS function to aim at other object areas within the same kind of function, thus broadening his own functioning. Performing another kind of IS function can be an intermediate step in growing towards an entirely different function. For instance, an Information Security Architect who is interested in the management side can first perform a function as Information Security Manager before growing towards a general management function within ICT.

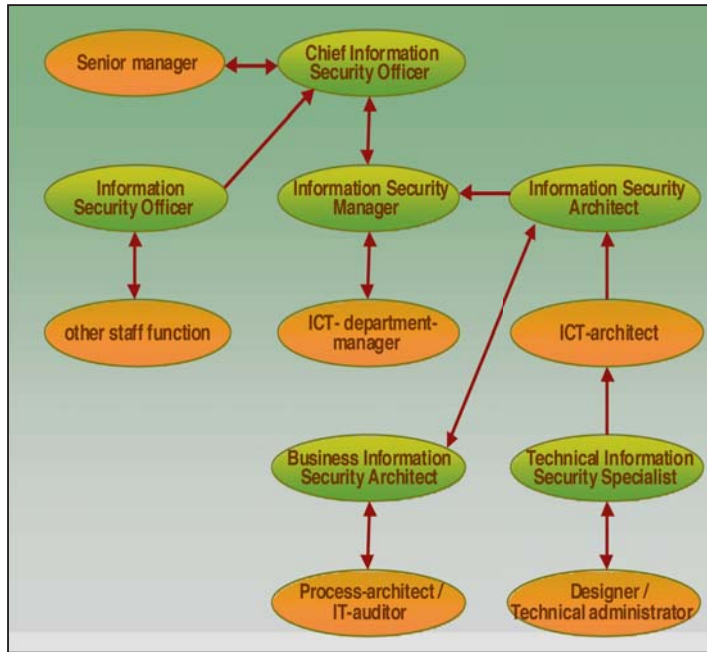


Figure 9 Growth paths of IS functions.

Depending on his background, the new intake or horizontal shift for IS functions will have to develop extra qualifications. Table 6 provides a list of those qualifications.

IS function	background	direction of development
Chief Information Security Officer	Senior manager	orient towards information security
	Information Security Manager	orient towards the business and/or corporate group
Information Security Officer	other staff function	orient towards information security
Business Information Security Architect	process architect	orient towards information security
	IT-auditor	orient towards architecture
Information Security Manager	ICT department manager	orient towards information security
	Information Security Architect	orient towards ICT processes (ITIL) and ICT organization
	Business Information Security Architect	orient towards ICT processes (ITIL) and ICT organization
Information Security Architect	ICT-architect	orient towards information security
	Technical Information Security Specialist	as designer: orientation towards architecture and possible widening of knowledge of information security
Technical Information Security Specialist	designer/technical administrator	orient towards information security

Table 6 Growth paths and direction of development.

We can identify two lines of orientation for the IS functions for the purpose of educational objectives. On the one side you have the orientation aimed at organization and management, the management direction, while on the other side you have the more specialized ICT orientation. Additionally, the functions should be performed at different levels. Table 7 splits the IS functions into these orientations and levels.

type of education	management orientation	technical orientation
Master	Chief Information Security Officer	Information Security Architect
	Information Security Manager	
	Business Information Security Architect	
Bachelor	Information Security Officer	Technical Information Security Specialist

Table 7 Educational orientation.

The function profiling as elaborated in this vision paper is new. That means there has not yet been any coordination of these profiles with what is available in education.

Given the dynamics of the educational world, we have not included any overview in the vision paper of the educational institutions with their range of information security courses. We regard that as a follow-up step, in which it will be more practical to place the results on the association's website, making it simpler to keep the list up to date. That will also make it possible to ensure the coordination mentioned between profiles and educational course availability.

Analytical ability	Capable of investigating problems systematically. Distinguishes between main issue and minor issues. Capable of making connections, tracing causes and processing information into useful units.
Decisiveness	Makes decisions on the basis of information and experience. Weighs up the pros and cons of a decision. Commits himself by giving opinions.
Creativity	Comes up with original ideas for problems that are connected to the function. Concentrates with investigative and curious mind on future renewal of strategy, products, services, markets.
Perseverance	Capable of concentrating intensively for long periods on a task, even with setbacks. Perseveres with a plan until the intended aim is reached.
Leadership	Stimulating, motivating, influencing and guiding others in reaching aims; setting aims, giving direction.
Initiative	Is alert and anticipates opportunities, new situations or problems, and acts accordingly at an early stage. Undertakes action himself.
Integrity	Observes generally accepted social and ethical norms in activities related to the function.
Emphasis on quality	Focuses on supplying good products and services and where possible, improving the quality of products and services.
Capacity to learn	Can absorb, analyze and process new information and ideas quickly and apply them effectively in the work situation.
Awareness of environment	Demonstrates he is well informed about organizational, social and political developments or other environmental factors (inside and outside the organization).
Sensitivity to the organization	Observes and has insight into the influence and consequences of decisions and behaviour of people in an organization.
Power of persuasion	Behaviour intended to convince others of a particular point of view and gain acceptance of certain plans, ideas or matters.
Result-oriented	Despite problems, setbacks, opposition or distractions, capable of concentrating on achieving the objective.
Cooperation	Contributes to a communal result by optimum coordination between own qualities and interests and those of the group or the other person.
Vision	Develops and carries out the main lines of a guiding future picture for the organization/department/products/services.
Progress monitoring	Draws up, follows and executes procedures to safeguard the proper progress of processes, tasks or activities of employees and himself.

'Beveiliging moet los van IT', Tijdschrift CIO IT-strategie voor managers, IDG Communications Nederland, volume 2, number 4, April 2003

Bokhorst Bart, *Functies in de informatiebeveiliging, een visie op ordening, deel 1 en 2*, Informatiebeveiliging 7 (2004) and Informatiebeveiliging 1 (2005)

Cazemier Jacques A, Overbeek Paul, et al (1999), *Security Management, CCTA*

Coul J. C. op de (2001), *Taken, functies, rollen en competenties in de informatica*, The Hague

Dunn Lex, Kuiper Renato (2003), *Security-architectuur, modekreet of bruikbaar?*, Informatiebeveiliging 8

ECABO (2004), *Beroepscompetentieprofiel Digitaal Rechercheur*, www.ecabo.nl

GvIB, Expertbrief 'Functies en rollen in de informatiebeveiliging', March 2005

GvIB, Expertbrief 'Het inrichten van een beveiligingsorganisatie', July 2006

Hoek Cobie van der, Koppen Leo van, Spruit Marcel (2004), *Competenties van de Informatiebeveiligiger*, Tinfon 4

Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, 'Informatieblad – Taken van de FG', December 2005, www.ngfg.nl

NEN, *Nederlandse norm NEN-ISO/IEC 17799 (nl) Code voor informatiebeveiliging (ISO/IEC17799:2005)*

Oud Ernst J., *Praktijkgids Code voor Informatiebeveiliging*, November 2002, pp.107/108

Overbeek Paul, Roos Lindgreen Edo, Spruit Marcel (2000), *Informatiebeveiliging onder controle*, Pearson Education

Stichting SURF (December 2005), *Leidraad functieprofiel Informatiebeveiligiger in het hoger onderwijs*

Functions in information security is a publication of:



www.pvib.nl

ISBN/EAN: 978-90-78786-02-3