GvIB Expert Letter – September 2006
ISSN 1872-4884, Volume 1 – No. 4

Setting up a security organisation. What factors are important?

Henk Bel

Bart Bokhorst

Ed Bronner

Ben Elsinga

Theo Engelsma

Jule Hintzbergen

Andre Jannink

Andre Koot

Ernst Oud

Lex Pels

Thom Schiltmans

Frank van Vonderen

Paul Wielaard

There is a growing need for more insight into the optimal way to organise the security function. Various publications, such as ISO 17799 and CobiT, describe very well what must be done with regard to information security. But it is still not clear who has to do what, and what is the best way to organise it. Which part of information security is a responsibility of the business unit and what should the IT department be responsible for? The most effective way to realise information security in practice and choosing the most suitable organisation form are not trivial matters. This expert group has examined which factors are important in setting up a security organisation and how it should be done.

http://www.gvib.nl/

✉ expertbrief@gvib.nl

2 INTRODUCTION AND DESCRIPTION OF THE SITUATION

In recent years, information security has been recognised by an increasing number of organisations as a relevant aspect of an organisation's management. In particular, the introduction of standards and new legislation and regulations with regard to compliance – such as the Sarbanes Oxley Act – has contributed greatly to this awareness. In addition to IT managers, business managers are becoming increasingly aware that good security is important for the reliability of business processes.

Information security is increasingly viewed as an integral part of business risk management and an important quality aspect. In the end, the risks to the operation of the business are the real justification for investments in information security.

Awareness on its own is not sufficient to achieve an integral approach to information security. For many, information security remains a difficult subject. Often, the "hot potato" is passed on to someone with responsibility within the department without providing the necessary mandate to go along with it. This "solves" the troublesome aspect. The result is that the problem is not dealt with by someone who is really responsible, which can hinder effective action and proper decision-making.

In practice, the information security function (IS function) is treated in different ways, which are often strongly influenced by historical developments and the company's culture.
Many organisations have appointed a "Corporate Information Security Officer" (CISO). However, the tasks and responsibilities of this position vary widely. A CISO who is the "security conscience" of a company will emphasise policy and risk analyses. A CISO in a predominantly technical environment will focus more on the provision of reliable technical solutions.

It is clear that the appointment of a responsible CISO does not mean that all the specific responsibilities and tasks of the IS function will be embedded in the organisation automatically. The further implementation of information security raises various questions: Are information security tasks specialised tasks or are they components of primary tasks that can be carried out by staff members as part of normal processes? Do they represent full-time positions or part-time roles, and can the activities be hired in or outsourced?

In view of the fact that information security is primarily a business responsibility, it would be logical for the IS function to report to the business unit. In practice, this is often not the case, which is understandable from a historical perspective. However, this often leads to problems in a number of areas.

This article discusses the organisation of information security. This includes everything that is related to information processing within an organisation. The security of persons and other safety aspects are beyond the scope of this article. This expert letter examines the setting up of a security organisation and the location and the roles of the security functions within an organisation. In this regard, the process of organising information security and the process of improvement based on, for example, the Demming circle are not included.

This expert letter will mainly describe the factors which influence this process. The exact ways in which these factors influence the setting up of an IS function will be described in a future expert letter.

Research Questions

An information security organisation can be set up in many different ways, varying from a single CISO supported by a number of IT staff with an information security role as an extra task, to a central team of specialists who have responsible tasks throughout the organisation. Information security organisations are sometimes strongly oriented towards technology and infrastructure, while others are expressly concerned with the management of business risks. The question is which organisation form, assignment of roles and position of the IS function in the organisation is the most suitable for setting up information security effectively and whether this approach is universal or is specific to, for example, a particular industry sector or company size.

Using the above starting point as a basis, the expert group considered the following questions:

- Which internal and external factors affect the setting up of the IS function?
- How do these factors influence the setting of the IS function?
- What are the problem areas and which trends can be recognised?

Related questions are:

- How do you organise information security really well? The formal description of the IS function on paper does not automatically create the proper basis and degree of support.
- Is it possible to develop a "recipe" that indicates the best possible organisation of the IS function on the basis of a number of parameters?

A workgroup has already examined the description of information security functions in connection with another expert letter. There is a risk of an overlap with the activities of this expert group, because the workgroup has realised that functions cannot be described without reference to an organisation model. In order to avoid reinventing the wheel, this article will build on part of the interim results of the workgroup.

In addition to internal and external factors that affect the organisation of the IS function, it is important to gain insight into the problem areas in the existing situation in many organisations. The most important problem areas are related to the current position of the IS function in the organisations. This will be discussed first.

Historical Perspective and Problem Areas

In order to gain insight into the problem areas, it is important to know how they developed. For this reason, the development of the role of CISO as leader of the IS function will be described briefly.

Development of the role of the CISO

The role of the CISO has undergone major changes over time. The classic information security manager was mainly found in military environments and other high-risk environments such as banks and telecommunications companies. In a few organisations with security awareness, information was approached broadly at an early stage. In most organisations, however, the increasing number of external links to public networks led to a strong focus on the guarding of borders through firewalls and access services. In other words, the solution of technical issues to keep "the enemy" out – an almost purely IT problem. Even when the attention of the CISO shifted towards internal affairs, the role of the CISO continued to have a strong technical content.

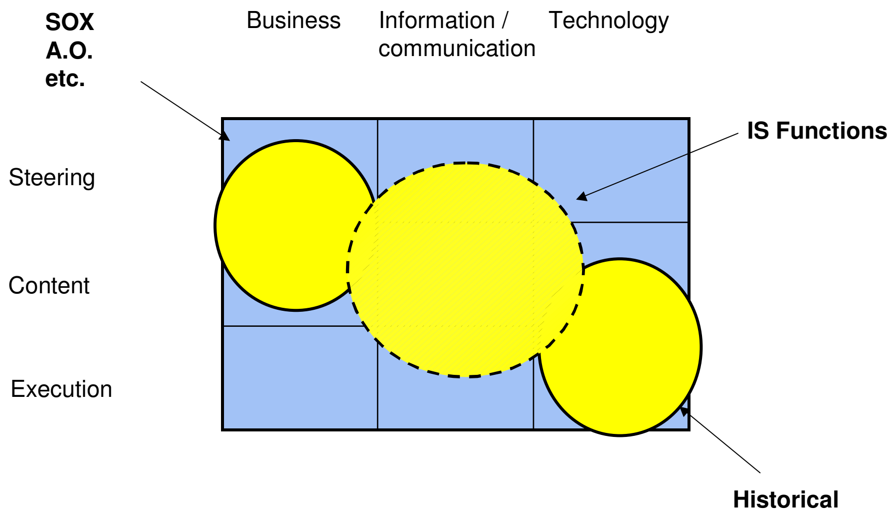
The CISO did not speak the language of the business unit and communication in terms of fears and uncertainties were not appreciated by business managers. Only during recent years have various incidents and the rise of standards such as ISO 17799 and legislated compliance requirements made the importance of information security clearer to business managers. Increasingly, CISOs began to use management terminology, such as "return on investment", "business continuity" and "reliability of information provision". Information security became a component of business risk management.

The broadening of the scope of security management led to greater specialisation and the identification of different information security tasks at different points in the organisation.

The current position of the CISO and problem areas

In many organisations, CISO's still report to the IT manager or CIO within the IT department. This is due to a strong technical focus in the past. Many organisations realise that the IS function is too distant from the management and struggle with the question of how information security can best be integrated and organised.

The figure below presents a model of how to look at the position of the IS function within an organisation. This is based on a model by Rik Maes.



On the vertical axis, the familiar strategic, tactical and operational levels may be identified. On the horizontal axis, an information column and a communication column have been added between the business and technology columns, showing that information and communications are connecting elements between business and technology.

This figure provides another visual representation of the fact that there is a need for bridging the divide between management and technology in the field of information security, and also that information security must become more of a part of strategic and tactical processes than it has been in the past.

Problems with the current situation

The fact that the CISO still often reports to the ICT manager or the CIO results in a number of problems that must be addressed in the definition of the IS function.

- Information security is not viewed to sufficient degree as an explicit responsibility in the management of the business or as an integral part of the definition of business processes. This means that information security is still seen as an ICT problem with a great risk of inadequate business alignment. This entails a risk of the CISO trying to promote secure working methods using “barking dog” methods because his or her mandate is not sufficient.
- Information security is also still too often seen as a bothersome and defensive extra burden and not as a quality aspect that can contribute to a positive company image. However, the increasing integration of business processes and IT systems between different organisations means that information security is an important building block in creating trust between organisations. In other words, it is a potential business enabler.
- The IT department must judge the quality of its own IT systems and infrastructure. If projects come under pressure due to a lack of personnel or resources (time), information security can be made subordinate to making functionality available without this being visible.
- An inadequate budget is made available for information security.
- Delegating information too easily is detrimental to the security awareness of business unit staff.

The optimal integration and definition of the IS function in the business helps to solve these problems. The question is: what then is the best possible definition?

The most important internal and external factors that affect this definition are examined below.

External Factors

Organisations operate in an external environment with many interested parties and increasing threats. The interests of society or of certain interest groups are mostly set out in standards or legislation.

Often, organisations are not independent but are part of different cooperative associations to which their business and IT processes are linked. For example, business process outsourcing and IT outsourcing call for clearly defined interfaces and agreements between organisations.

The most important external factors identified are:

- Increasing threats
- Obligations
- Chain integration

Increasing threats

Hacking activities through the Internet are increasingly carried out by criminal organisations. Organisations which have something worth stealing are the targets. The more an organisation is susceptible to these kinds of threats, the more its IS function will have to be oriented to the areas of prevention, detection, monitoring and incident response.

Obligations

Compliance with laws and regulations is a prerequisite for an operation to operate in an external environment. These laws and regulations are often formulated in the language of the stakeholders and must be translated within the organisation into the consequences for information security, both on tactical and operational levels. Examples of these are SOX, Basel II, ROB, HIPAA and WBP.

Depending on the market within which an organisation operates, certain compliance requirements apply. In an organisation, this translates into the implementation of specific measures and the need for monitoring and reporting in specific areas. The influence of compliance on the definition of the IS function is partially described below, but must certainly be investigated and elaborated in greater detail.

Chain integration

The trend towards further chain integration between market players leads to the need for good agreements and measures, both at a business and a technical level. The reliability of information exchange and the confidentiality of communications are determined by the agreements and measures taken as a whole. Depending on the situation, the risks and mutual trust, the accent may be placed on procedural and contractual measures or on technical measures. In order to deal with risks in a cost effective and efficient way, a combination of procedural and technical measures are taken. This is why it is desirable for the IS function to have a broad orientation. On the one hand, the IS function must be able to support the business unit with advice about achieving a good balance between the different measures. On the other hand, the IS function will have to cooperate with external parties to determine the possibilities there are available and which solutions best suit the parties involved. Sometimes there is freedom to make bilateral agreements, but there is often a need for industry-wide guidelines that are more or less obligatory.

The influence of compliance on the IS organisation

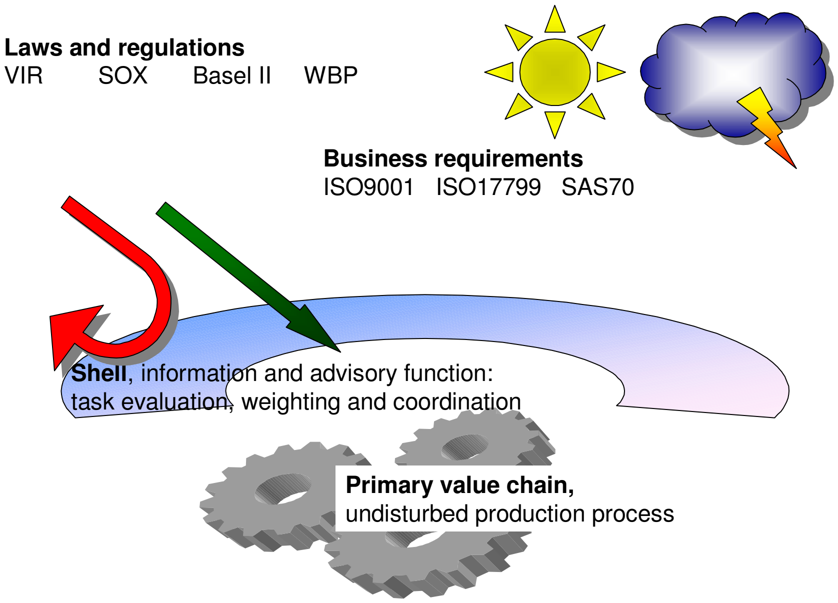
Usually, an organisation has to fulfil compliance requirements coming from different angles. Each set of compliance requirements has its own specific reporting requirements, but they actually overlap in many areas.

Parts of the organisation can get into a situation where they have to provide different reports about comparable aspects. A need thus arises for a common reporting system, which can be used to produce different reports for the different compliance standards. This can avoid the situation in which operational organisations are more occupied with reporting than with the production process itself. It is important that the production process in an organisation's primary value chain is able to proceed with as little disturbance as possible.

Creation of a common reporting system requires coordination by a "change organisation" that evaluates, filters and translates all external influences to produces a common set of requirements which uses clear and unambiguous terminology.

This will lead to an increased need for the integration of information security with other processes, such as enterprise risk management (ERM), operational risk management (ORM) and business continuity management (BCM). It is safe to say that compliance requirements mean that the information security organisation must cooperate more intensively or become more integrated with other parts of the organisation that are involved with risk management. A following expert letter will answer the question of how this can be organised in the best way possible.

The figure below illustrates the need for a filtering and coordinating shell around the operational processes.


Laws and regulations
VIR SOX Basel II WBP
Business requirements
ISO9001 ISO17799 SAS70
Shell, information and advisory function:
task evaluation, weighting and coordination
Primary value chain,
undisturbed production process

Internal Factors

An important finding of the expert group is that many more internal factors were identified than external ones. Without an immediate and clear understanding of how these internal factors affect the organisation of the security organisation, the expert group believes that the following factors affect the optimal organisation:

- Drivers and support within the organisation
- Maturity of the organisation
- Vision
- Culture
- Scope and definition of the IS functions

- Size of the organisation
- Geographic distribution

Drivers and support within the organisation

In order to integrate information security successfully into an organisation's processes, it is important to connect to existing and accepted processes in the organisation. Examples are risk management or quality management. If these processes are regarded as important, information security is given a positive profile almost automatically and it is easier to obtain commitments.

Which processes are recognised as being important often depends on the interests of one or more stakeholders. By using the terminology of the stakeholders in communications, the stakeholders will more quickly recognise the importance of information security and support it. In turn, resources and budgets will be made available more readily, because this will be seen as serving the stakeholders' own interests. There may be a number of stakeholders and their interests may change over time. The use of the right degree of momentum can be important to get the organisation onto a higher plane. At the moment, the necessity of complying with the Sarbanes Oxely Act can be used to provide important leverage for improvement.

The need to adapt flexibly to the interests of stakeholders also sets demands on the flexibility of the people involved. They should have a broad orientation in the field of information security and must be able to express the same message in different ways. It should also be possible to change priorities or even the organisation form in a flexible way. However, it cannot be taken for granted that staff members actually have this flexibility, because changes may represent a threat to their positions.

Maturity of the organisation

Experience is still the best tutor. Organisations must be find out what does and does not work and will have to learn and make adjustments based on an analysis of causes. This requires time and patience. It is a good thing to aspire to a certain level, but it is important to determine what the conditions are for achieving that ambition. A step towards a certain level of maturity can only be taken if the previous level has been reached. For example, if there is no basic level of security in place, IS officers will mainly be occupied with incidents and "putting out fires". It is important to establish structure and routine, but if the whole building burns down in the meantime, the structure is pointless. Or, if the organisation's risk management is not adequate, it is difficult to build on it in implementing information security.

"Quality assurance tasks" should be an integral part of business processes. As management, primary and supporting staff become more responsible for continuity and reliability of the information supply, specialised information security will become superfluous. This implies that every manager or employee knows that he or she is responsible for carrying out the task. This idea also assumes that they have sufficient knowledge of information security and that they have adequate time and resources to be able to execute this task optimally. In view of the fact that this is often not the case, a need remains for IS officers who can provide advice and support at the right places and with the right knowledge, and who can enforce correct action where necessary.

The maturity of an organisation is a determining factor in the degree to which information security can be integrated and organised separately.

Vision

The importance of information security is dependent on the organisation's primary business process. In most organisations, IT facilitates the processing of information related to the primary processes. However, there are also organisations that offer IT as a product or a service. In this case, good security may be essential in order to supply the services at all. However, all organisations have facilitative IT and in this sense their needs are comparable; so organisations offering IT as a product do not differ significantly from other organisations. Basic information security is a necessity and is often viewed as a defensive measure. Information security can also be deployed as an offensive measure to create a security image or to use security as a business enabler. For example, e-business would not be possible without information security.

The importance of information security for an organisation's business process is a determining factor of the required IS capacity and the place within an organisation given to the IS role.

Culture

In addition to the factors described above, the culture of the organisation influences the implementation of information security. An autocratic or formal management style will quickly lead to a top-down managed security organisation, while an informal organisation allows many responsibilities to be assigned to lower levels in the organisation's hierarchy. Where does the centre of power lie in an organisation? Is it on the business unit side, or on the IT side? This is often strongly determined by historical factors. The management's risk perception is also important. Does the management avoid risks or seek opportunities?

Information security involves technical measures, but it still essentially concerns people. To a large extent, an organisation will have to implement information security with the staff it already has. What is their attitude and which responsibilities can they take on?

The style with which an organisation conducts its business with other organisations is also a determining factor. Does an organisation do business on the basis of trust, or must business transactions be verified through technical checks or guaranteed by lengthy contracts? The more checking, the less trust, and vice versa. The greater the need for verification, the larger the role of IS will be.

Scope and definition of IS functions

Implementation of information security requires a thorough inventory of all the security tasks that must be carried out, varying from formulating policy to the careful administration of users. Security tasks are carried out by various levels and affect many parts of an organisation. It is wise to make an integral inventory of tasks and, where possible, to assign them to roles in the normal organisation.

One risk is that if an integrated frame of reference does not exist for the organisation as a whole, task descriptions will be defined too much on the basis of local interests. The implementation can then easily become dependent on the interests of the local manager, on the factors upon which his performance is evaluated, as well as his scope and limited resources. Room for filling in the tasks according to the local situation is important however. The more employees can act independently the better. The outline of what has to be done can be defined integrally, but how to implement this can best be decided locally.

The degree to which integration of IS within the organisation can eventually lead to less specialised security functions is partly dependent on factors such as the size of the organisation, knowledge levels, efficiency and the vision of whether information security should be a specialised function or whether security roles should be part of generic functions.

Size of the organisation

It is obvious that the size of an organisation is a determining factor in the defining the IS function. An important assumption is that execution and monitoring are clearly separated. This is easier to achieve in a large organisation than in a small organisation in which several tasks have to be carried out by a single person.

As an organisation grows and the amount of IS work increases, there will often be more specialised work that will be carried out within an IT department. In all cases, the business management has final responsibility. The business management determines the requirements and the strength of the controls, while the IT department determines to a large extent how the controls are implemented.

In a large organisation, part of the control function will quickly lie within the IT department, especially where specialised work is required. In small organisations, a single person is often responsible for the specialised IS task; this person should report to the management but in practice he or she often still reports to the CIO or IT manager. The final responsibility for weighing risks and accepting residual risks always remains with the business management however.

Geographic distribution

In organisations with a large degree of geographic separation and similar processes at different locations, there will be greater need for standardisation so that each does not have to “reinvent the wheel”. In comparable situations, comparable measures must be used. Standardisation can be implemented on various levels, both by imposing measures hierarchically as well as by establishing consensus between the different parts of the organisation. This choice will be strongly determined by the company’s culture and power issues.
A strong geographic separation will lead more quickly to a decentralised IS organisation, in order to deal adequately with local aspects such as language, culture, time zone problems, etc. Good central coordination of the IS function is essential for this.

Other aspects to take into account

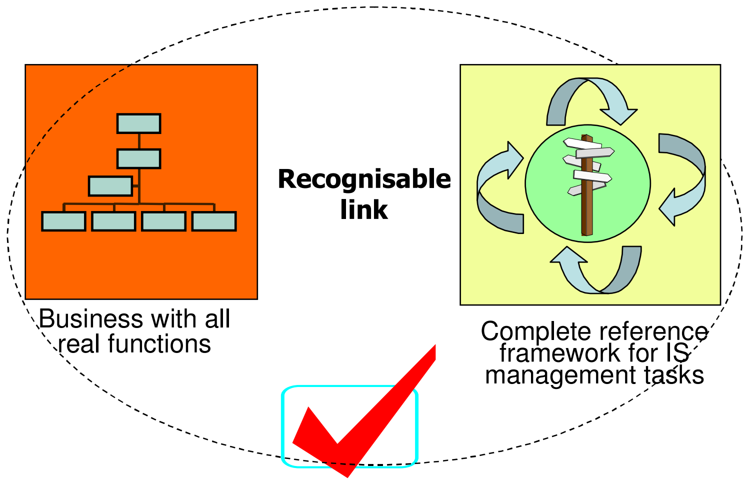
- Designing an organisation is often something beyond the expertise of the information security officer. This entails the associated risk that someone will be doing work that is beyond his or her expertise. It is more difficult to set up a really effective organisation that it looks. The failure to recognise areas of tension and personal interests can stand in the way of setting up the best possible IS organisation.
- If attempts to set up of a formal organisation are (temporarily) unsuccessful, an informal organisation is a good alternative. Bear in mind that an informal organisation

has a more limited mandate or no mandate at all, so results must be achieved on the basis of personal influence.

- A virtual organisation of experts to provide support is useful if the knowledge is not present “in-house”.
- Network and chain organisations call for a cooperative model of information security because hierarchical management of different organisations is usually more difficult to achieve.
- A security organisation may not be rigid. It must be flexible enough to react to new threats, technological developments or new legislation.
- It is important for the organisation model that tasks, responsibilities and authorities are clear and well adjusted.
- An IS organisation must preferably be multidisciplinary and adequately embedded in the business management so that both technical and non-technical aspects are given adequate attention.

The importance of a recognisable link between IS tasks and normal functions within an organisation is illustrated by the figure below.

Embedding IS in the organisation


Recognisable link
Business with all real functions
Complete reference framework for IS management tasks

Management information

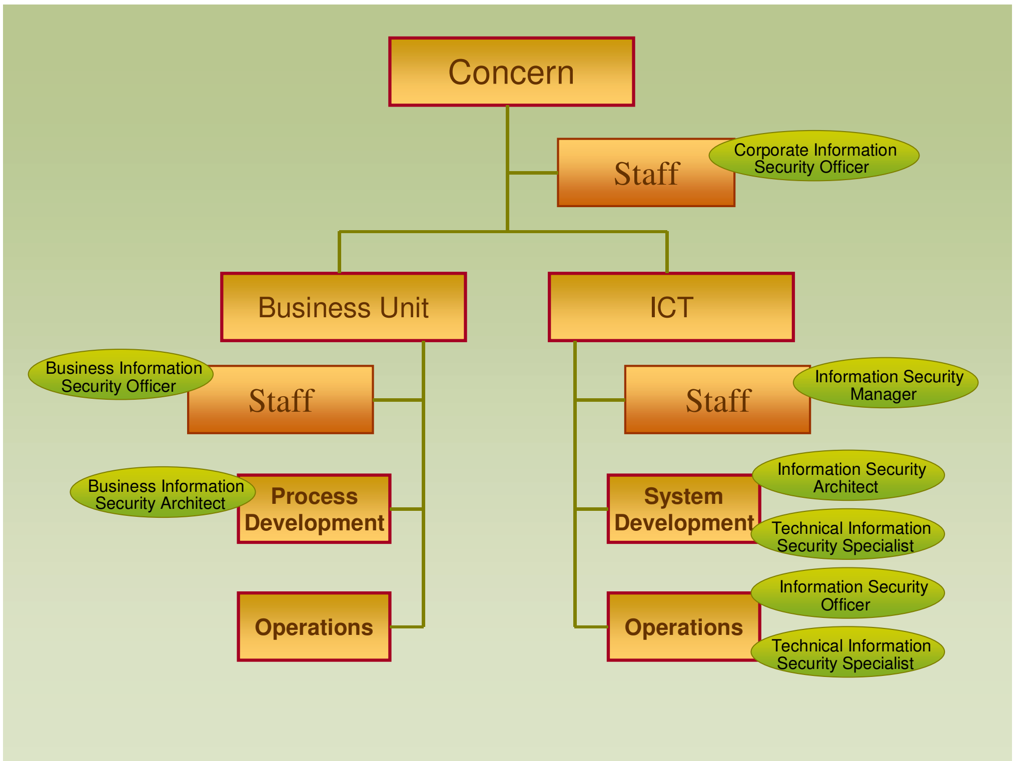
Organisational Aspects

The factors that affect the definition of the IS function are described above. The question is which aspects of the definition they influence and in what way. The aspects that may be influenced include:

- Embedding and structure of IS within the organisation
- Size of the specialised IS function
- Delimitation of roles with tasks, responsibilities and authorities
- Reporting hierarchies
- Position in the organisation
- Authorities of IS organisation and of (local) officials

- Scope of the IS function in relation to bordering areas, such as personal safety, internal control, BCM and risk management.

As a reference, this article refers to the draft model for setting up an IS organisation drawn up by the GVIB/PI workgroup that deals with functions in the field of information security.


Concern
Staff
Corporate Information Security Officer
Business Unit
ICT
Business Information Security Officer
Staff
Staff
Information Security Manager
Business Information Security Architect
Process Development
System Development
Information Security Architect
Technical Information Security Specialist
Operations
Operations
Information Security Officer
Technical Information Security Specialist

The functions in this model apply to large and complex organisations. For smaller organisations, the workgroup has explained how these functions can be combined. The relationships between functions that are related to each other or overlap have also been described. For further details, please refer to the article on this matter that will be published soon.

Although the precise influences of the factors identified have not yet been determined by the expert group, a number of factors can be identified that lead to a more formal or more informal organisation.

Formal organisation	Informal organisation
Bureaucracy	Dynamic organisation
Autocratic management	Decentralised management
Large organisation distributed geographically	Small organisation
Management avoids risks	Management seeks opportunities
Accent on obligations and monitoring	Accent on relationships and trust
Mature organisation (repeatable process)	Immature organisation (heroes)

Completeness

When setting up an organisation it is important to be as complete as possible and to take all important factors into account. In order to achieve this, it is necessary to:

- Clearly define what is meant by information security, which management objectives this involves and what its scope is.
- Explain how information security relates to other concepts, such as quality, risk management or compliance.
- Use the language of the business unit.
- Take external stakeholders into account.
- Find a good balance between supply and demand (what is needed, what is possible).
- Keep communication between demand and supply focused on the level of What (not How).
- Avoid shortcomings in determining the What level by making use of best practices and standards.
- Make sure that a responsible party is designated for every aspect of IS.
- Assign IS responsibilities to the owner of the most stable element in an organisation (process, organisation, department, functions) so that changes within the organisation will have as little impact on the IS function as possible.
- Determine a practical aggregation level for demands at the What level.

Conclusions and Follow Up

The expert group has, to a large extent, succeeded in finding answers to the questions it posed. The most important influencing factors have been identified and partly explained. Some aspects of the information security function that are affected by the various factors have been described. An important trend has also been identified: more and more frequently, organisations in the "network world" become part of a whole chain or partially outsource their activities. In so doing, they lose a certain amount of autonomy and there is a need for coordination and cooperation with other parties in the chain. This requires flexibility on the part of the IS function.

The expert group has decided to devote a second session to the following, as yet unanswered, questions: In what direction and to what degree do the influencing factors affect how the information security function is organised? It would be ideal to develop a model (recipe) based on a generically valid reference framework and defined parameters that could automatically present the optimal organisation form.

It is important to have as much experience-based information available as possible in order to uncover relevant links. To help us prepare for the next session, the expert group thus invites you to comment on this article and to provide as much input as possible with regard to the links described in it. Send your reactions to expertbrief@gvib.nl. Your views on this expert letter are also very welcome.

14

LITERATURE

The expert group made use of the following literature in the writing of this expert letter:

Fred van Noord, *Top-down en bottom-up gaan hand in hand - BS7799 werkend krijgen in organisaties*

Gartner, *The evolving role of the Chief Information Security Officer*

Jentjes and van Dijk, *Groeien naar een integrale beveiliging bij RWS RIKZ*

Ton Thoma, *Waarborgen beveiliging bij uitbesteding*

Fred van Tol, *Project Informatiebeveiliging Defensie Interservice Commando*

Bart Bokhorst, *Functie in de informatiebeveiliging, deel 1*

Andre Koot, *Enhanced Security Management - Informatiebeveiliging verankerd in een dynamische Business Alignment theorie*

Rik Maes, *Reconsidering Information Management Through a Generic Framework*

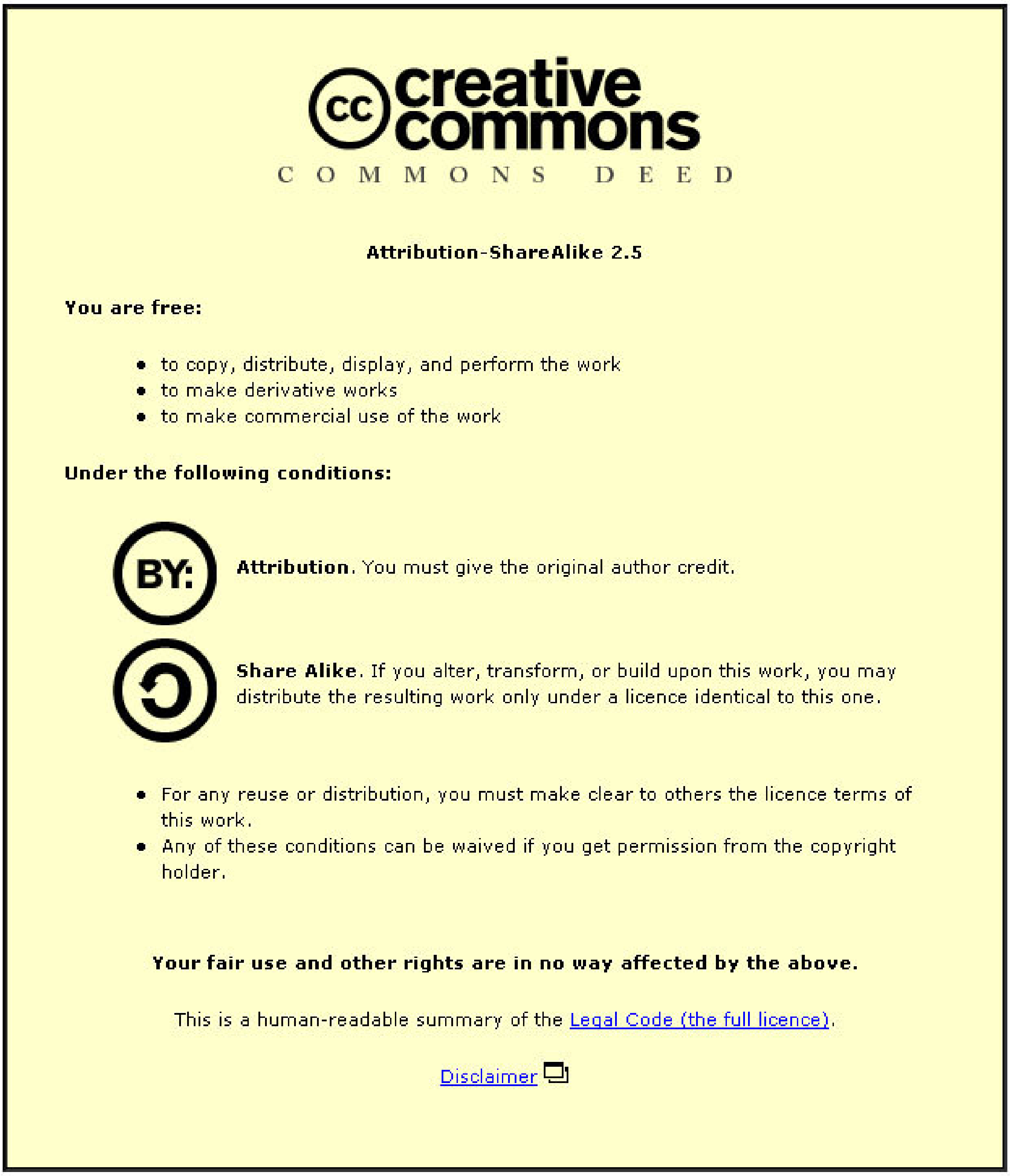
A Hofman, *Adaptive Security: flexibele beveiliging in de netwerkeconomie*

A Jannink, *Kan AOR en Besfuta u helpen?*

GvIB*, Raamwerk AOR23 March 2006 issue of GvIB*

APPENDIX: LICENSE FOR THIS PUBLICATION

This expert letter has been published according to the following license: http://creativecommons.org/licenses/by-sa/2.5/



creative commons

COMMONS DEED

Attribution-ShareAlike 2.5

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works
- to make commercial use of the work

Under the following conditions:

Attribution. You must give the original author credit.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a licence identical to this one.

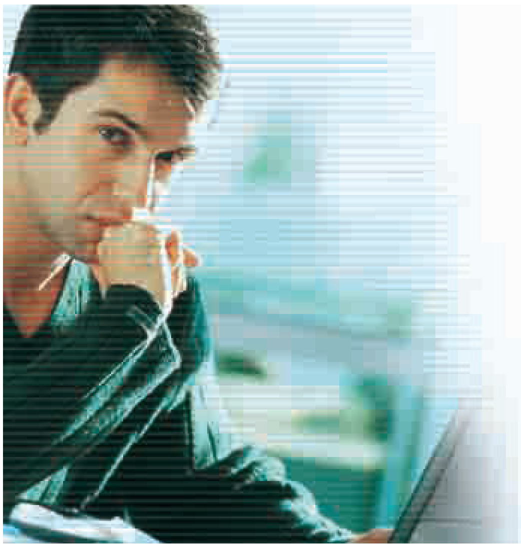
- For any reuse or distribution, you must make clear to others the licence terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full licence).

Disclaimer

JOIN THE GVIB, FOR SAFETY AND SECURITY ...



Information security has been an essential and exciting subject for many years. Almost all occupations are having to place more emphasis on the confidentiality, availability and integrity of their information. Whether you are a CISO, manager, consultant or programmer, the Information Security Practitioners Association (GvIB) can help you with information security issues.

What is the Information Security Practitioners Association?

The GvIB is an open, broad-based association for professionals to build a more professional approach to information security, through the exchange of ideas, information, knowledge, insights and above all, practical experience.

What are our aims?

We aim to promote the physical, systems and organisational security of data and data processing equipment against in-coming and outgoing breaches. We also promote the exchange of knowledge and experience and the networking of practitioners in the sector - through this Expert Letter, for example.

Our target group

The target group for the GvIB includes everyone involved in information security, either as a student or professionally, or who are especially interested in the field. Our rapidly growing membership covers many different disciplines: students, information architects, technicians, managers, organisational consultants, legal specialists, security officials and ICT auditors. Our members come from all kinds of educational backgrounds, companies, public authorities, organisations and suppliers.