

Paul Overbeek

Bart Bokhorst

Dirk Brouwer

Ben Elsinga

Leo van Koppen

Renato Kuiper

Fred van Noord

## Functions and roles within the information security

*This expert letter has been prompted by the dramatic increase of function titles within the information security and risk management. Also the relation between the functions among themselves and the relation to other functions within the organisation is not clear. There are other unanswered questions, like can career paths be developed, and which education and training is needed. The offering party would also profit from a clear picture of what are in fact the training needs in the market.*

Page

### THE RESEARCH QUESTIONS

2

- *Organisation perspective:* Which roles or functions can be defined within the area of information security and risk management, and which titles are used?
- *Individual perspective:* Which stages exist in the career development of an 'information security officer'?

3

### ORGANISATION PERSPECTIVE

- The distinction between regular and differentiated functions.
- Away from proliferation of certifications and towards a clear position on job titles and certification.

4

### INDIVIDUAL PERSPECTIVE

- The three growth stages of the information security officer as a base of development and certification.
- The information security manager as the key figure.

5

### THE CAREER

- Example career paths are an inspiration source for incoming talent.
- The information security officer as the gate to a CIO or CFO function.

6

### QUOTES ABOUT ORGANISATION AND INDIVIDUAL PERSPECTIVE

- The security architect will disappear.
- Current education does not (yet) fit the needs in the field.

 <http://www.gvib.nl/>  
 [expertbrief@gvib.nl](mailto:expertbrief@gvib.nl)



## TOWARDS CLEAR FUNCTIONS AND ROLES WITHIN THE INFORMATION SECURITY

### *Security must be clearly recognizable in BaMa-structure*

The cause of this expert letter is the dramatic increase of function titles within information security and risk management. Also the relation between the functions among themselves and the relation to functions within the organisation is not clear. Other unanswered questions are for example: can career paths be developed, and which education and training needs exist. The parties offering Bachelor's and Master's studies, the so-called BaMA-structure, as well as other educational institutions, would also profit from a clear picture of what are in fact the training needs in the market.

200 different function titles were identified within the member list of the GvIB (the Dutch Information Security Practitioners Association). Certifications are soaring too. Some better known are: MSIT, CISSP, CISM, ISSMP, CISA, CIA. In which way do these letter abbreviations relate to Drs., Mr., RE or RA (Dutch Titles, compare with Msc, Bsc, certified EDP auditor and CPA). Some institutes offer training that gives a nice abbreviation following the surname, for a discounted price of only \$500.00. How do these trainings fit within career paths and functions? Which qualities and skills fit with each function?

A team consisting of Dirk Brouwer (information security manager), Renato Kuiper (security architect), Bart Bokhorst (information security manager in the design process), Fred van Noord (consultant information security and interim service manager), Leo van Koppen (trainer), Ben Elsinga (facilitator in this process) and Paul Overbeek (ghost writer), asked themselves the questions mentioned above. The final goal is to get a clear picture about the function titles in information security and risk management and the competences, tasks and responsibilities that go with these functions. This makes it possible to stimulate the development of career paths and adopt a 'common body of knowledge' for development of competences with or without training.

### QUESTIONS RESEARCHED

The questions that this team wants to find answers to are the following:

- **Organisation perspective:** which roles/functions can be defined within the area of information security/risk management, and which titles will be used?  
The end result of this question will be an overview of function titles, function requirements, overviews with tasks-responsibilities-qualifications (TVBs or TRQs) personal competences, knowledge and skills. Perhaps a link can be made between these profiles and trainings and certifications.
- **Individual perspective:** which stages of development can an 'information security officer' or 'risk manager' pass?  
The answer to this question gives more clarity about the development paths that a professional can take and the competences that can contribute to it.

These questions are not meant to be answered today or in the isolated environment of the 'expert group'. It is important to come to a position and to formulate points of discussion which can be elaborated upon during discussions with colleagues in the field, or other concerned parties, and then reach a widely accepted picture in a relatively short period of time.

The goal is to create a reasonably widely accepted picture in a wide discussion through the website of the GvIB and through forum discussion. This article is just a stage in the process and will hopefully serve as a "beacon on the path to further maturity within our industry".

## ORGANISATION PERSPECTIVE

The starting point of good information security is a risk management process. Examples are the information security management system (ISMS), which is described in the Code of Practice for Information Security or the risk management process of the COSO and COBIT-models. Organisations make distinction between the operational, tactical and strategic levels. A similar distinction is also made in a senior secondary vocational education, higher vocational education, or university work and thinking level, but not necessarily on a one on one relationship.

From the organisation perspective a distinction is made between regular functions and differentiated functions. As far as regular functions are concerned, there is a distinction between regular staff members and managers. Each having defined competences (knowledge, skills and attitude) that all staff members and managers should have regardless of their position within the organisation.

As far as differentiated functions are concerned, the proliferation of titles is thought to be an impediment. The work group suggests using a limited number of functions. Consensus is growing over the function 'information security manager'. All other indications are not considered specific functions but more as roles or specialisations. Examples are the 'security architect', the 'risk analyst', the 'authorisation manager' and the 'encrypter'. It is striking that the large number of titles does not lead to recognition within the market. The tens of kinds of certifications don't help either. The work group calls to be reticent.

Also surprising is the confusion about functions and roles. One can, in a particular function such as 'senior policy maker', fill in different roles with regard to security, i.e., risk analyst or continuity coordinator.

Another issue are the temporary roles. The work group notes that an indication for a phenomenon that temporarily needs more attention is easily confused with a function. A clear example of this is the 'anti-Spam-manager'. Within a short time this 'function' is a regular part of the anti-virus/software management. But from a 'security architect' point of view, one can also wonder if this is a real function, or that the need for this role arose because of absence of knowledge within the natural positioning of the right role; the wish being that the natural functions at some moment will have enough 'basic knowledge' to consider the security aspect as a regular part of their duties.

## INDIVIDUAL PERSPECTIVE

The development of an employee to a professional information security manager is defined as follows (according to: [www.ics2.org](http://www.ics2.org)):

- Level 1: upcoming talent with little relevant experience;
- Level 2: an ethical all-round professional with relevant knowledge and experience;
- Level 3: specialised in security management or security architecture or other field specific specialisations.

Instead of levels they are also called (growth) stages.

From the individual perspective, a distinction is made between the three levels of knowledge, experience and personal skills.

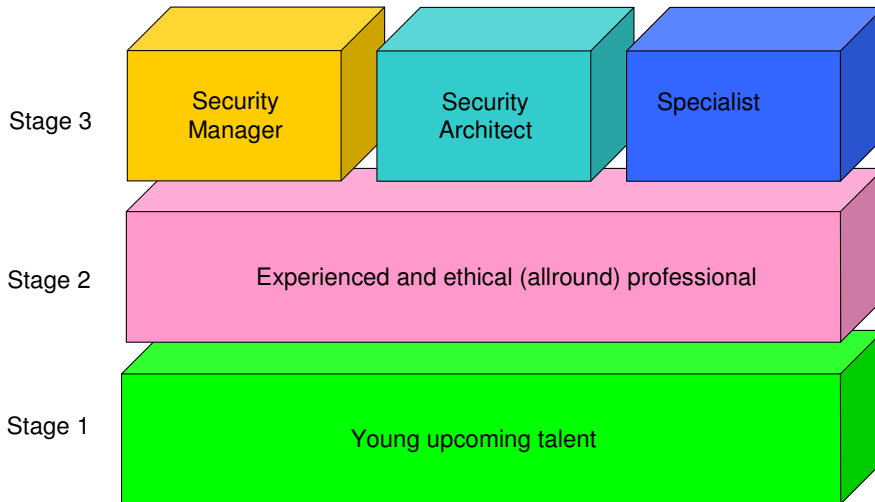
The basic level (level 1) offers enough knowledge and experience and the matching personal skills to place and address the security issues within a non-specialised function. The basic level is the package that you would like to offer all your employees and which you hope that all your managers already possess. The wannabes fall into this category as well, as they are eager to learn and often have at least some affinity with information security. These are people who have the talent for information security.

At level 2 we find people who concern themselves professionally with all aspects of the field. They have a Bachelors degree or commensurate academic training and have a minimum of five years experience in different parts of information security. Ideally, these people, in collaboration with people in other disciplines, see to it that the information security is built into the solutions instead of attaching security later. The security officer at level 2 is also capable of working out a risk analysis and presenting this at management level.

Level 3 is the level of the information security manager. He is often a member of the staff with a limited number of “direct reports”, as well as limited executive responsibilities. His role is one of coordinating and/or lending support to the rest of the organisation. He must be capable of overseeing the entire area of information security with all aspects (physical, HRM, legal, line, audit, technical) and set priorities. He must also have enough authority and support to make things happen at places within the organisation where others bear no responsibility. This level requires a lot of personal skills, management capacities and a good working knowledge of the industry.

Another example of level 3 is the specialist. This individual has a high level of knowledge and experience in a specific area. A specialist is primarily approached for his knowledge rather than for his personal skills. Examples of specialists are the cryptologist, the risk analyst and the security architect. Just like the risk analyst, the security architect (as far as differentiated in a specific role) is part of a team that takes care of several disciplines. Only in this way the information security is a truly integral part of management and thus supporting ICT to be a company means.

The information stages of an information security officer  
From young talent till experienced greybeard



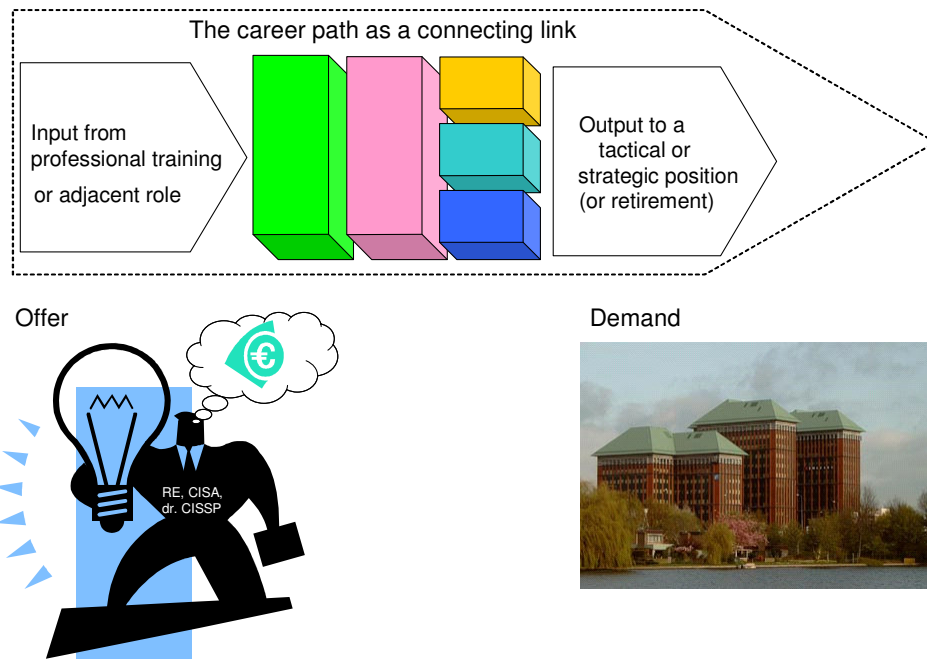
## CAREER

A career is the grow path of the individual within an organisation. A career can include security roles and other functions. The work group's opinion is that example career paths can be helpful when attracting new talent. Some complain that once you are in the field of security, the only career path left is within security, and that it is a very short one.

One could ask if that isn't the case within all fields? After all, isn't it true that in every field there is a structure of pupil, mate, and master?

A career in information security shouldn't be a dead-end street, nor should it be a final step in that career. In the opinion of the work group this is a sign of weakness and serves as a deterrent for upcoming talent. Career development within an organisation has to anticipate this. A management function within information security offers one the opportunity to explore each remote corner of the company, develop his personal skills and prepare for a function such as CIO or CFO of the company.

A number of cross connections with other functions within the organisation can be distinguished. For example, the relationship between the audit function and corporate risk management. The work group's opinion is that there is room for improvement in this area. Examples of role models with successful careers reaching to the top of the organisation are needed.



## QUOTES ABOUT ORGANISATION AND INDIVIDUAL PERSPECTIVE

### *Organisation perspective*

What is an *information security manager*? There are many different images that come to mind. It is a member of the staff who understands the business. He takes care of coordination, priority setting and movement and getting the job done by subordinates. He also sees to the execution of the management cycle: plan – do – check – act. The work group prefers a function title that includes the word 'manager' rather than the American word 'officer'. In the Dutch language security officer is used for roles in the security administration area.

What about the function of *security architect*? Is that a separate function, or is it a role that should be executed within the regular function of system design? That is, if the knowledge is there within that regular function, the ICT architect needs to have security knowledge! And that is considered the crux of the problem; as long as the knowledge level within the regular functions is too low, these functions will be flanked with comparable functions with the prefix 'information security'. As soon as this knowledge deficiency is solved, these specialised security functions will disappear again. So the security architect disappears as soon there is enough security knowledge within the function of system design.

There is in fact only one special function, namely the one of the information security manager.

In addition, there are specialist (or regular) roles, where a 'role' is defined as part of the job responsibilities. From this perspective, 'auditor' can also be a role according to the work group. But, the role implies that a certain distance till the audit object is needed. That is why, as soon as the size of the company permits it, the auditor will be a differentiated role and, when the company grows, differentiated function.

In 2004 the professional competence profile, *Digital Detective* was developed. The digital detective detects and investigates cyber crime. He does this by initiating new investigations, securing digital evidence and searching for evidence. Training should take place within regular education. The detective function as well as the digital detective is usually placed at an senior secondary vocational education level. The description of the competence level for the digital variety seems higher however, more like higher vocational education. Is this a characteristic of a normal development within a profession, or are the requirements too ambitious?

Isn't a digital detective one with knowledge of automation? The relationship with information security would then be limited; in that case this function is not a specific security or risk management function.

The COSO framework states it nicely: security should be built IN, rather than built ON. Differentiated functions lead to problem isolation and island behaviour. There shouldn't be a separate security architecture. Instead, security attributes should be weaved into the pre-existing architecture.

The security official can be compared with the quality official. When quality arose as an issue, the quality official came about. Then they saw to it that an integrated quality process was put into place, and we now see that the separate quality officials aren't needed in abundance anymore. They are only there where they have an added value. In, say, 20 years the 'information security official' won't exist either. The 'role' will become part of the function of compliance manager. A sort of life cycle has come into existence for functions: they are created at times of problems, usually because of a temporary deficiency of knowledge, and after a while they can be removed again.

The security function is a normal function, but with additional knowledge and an attitude commensurate with the function. Of course, the security in the development cycle of information systems must be warranted. But who takes care of that? You have to be at the front line of the process and it appears that the differentiated functions are there too late. We have to identify the functions that are at the front line of the process and those we must enrich with the necessary (extra) security knowledge. The information security manager will have to ensure that the knowledge level within those functions remains sufficient. Those 'normal' functions must be able to recognize the problems and, if necessary, hire a specialist. That specialist brings additional knowledge that was gained in the field or as a result of specific training, which may or may not have a special title. So it all comes back to integrating information security knowledge into the regular processes. The information security manager is, just like the normal manager or ITIL manager, a regular process manager. The only extraordinary element is that many of the activities of security management take place within other processes, which requires more coordinating qualities.

The information security function seems to contain two basic competences: analysing and consulting. This applies for information's security managers as well as security architects. They never work alone and are often maintaining a supporting role. Nothing comes to an immediate halt if he isn't there.

The workgroup also consulted a Dutch classic in the area of function description, namely the overview 'Taken, Functies, Rollen en Competenties in de Informatica' [Tasks, Functions, Roles and Competences in Computer Science] by ir. Johan C. Op de Coul (ISBN 90-440-0343-7), that at the time, was published under the auspices of the NGI (Netherlands Society for Informatics). In the work group's opinion, the conclusions in this book are not fit for information security.

The playing field in which information security roams isn't well defined yet. What is it all about? Physical security, technical security, risk management, legal aspects, or HR aspects? Or does information security touch all of these and could the information security officer, depending on his personal ambitions and internal pressure, (or lack of it) create his own profile? Which expectations are, from the company's point of view, realistic? It seems that the future employer and his human resources department are still in the dark, and simply hope that the match between person and function fits.

### *Quotes about the individual*

Training has always intended to transfer knowledge. Thankfully, the switch is being made now to competence-aimed training. However, personal skills are hard to learn and personal growth is difficult to measure. Essential personal features such as loyalty, integrity, and persuasiveness are almost impossible to learn and only measurable in a limited sense. These are however, core concepts within personal features that a professional in the information security field needs. Perhaps these features have to be passed on from others. The behaviour component, for example, could receive input from a coaching role and, of course, by a display of exemplary behaviour.

Traditionally, education is equipped to disseminate knowledge and less for personal skills. However, the attributes 'personal skills and features' are, especially for security, of great importance. Doesn't this demand a more practically oriented training Information Security at a higher vocational education level? Or is this only a part of the solution?

It would be best for the industry to have the competences well established. What makes a security function special? The combination of knowledge, skills and attitude or behaviour was already mentioned. But isn't this really a *trusted* function, and should that aspect not be more accentuated?

Information security has, in addition to the field specific aspects, features from social science disciplines such as organisation development, organisational changes and psychology. That demands the capability to solve interdisciplinary problems in practice. Different aspects are involved: organisation, people, technical, and legal aspects. Both from the alpha (social sciences) as the beta (exact sciences) corner there is enough to experience.

Anyway, a bigger demand on personal features like integrity and loyalty can be seen everywhere around us. The American Sarbanes Oxley (SOX) legislation speaks out about the ethic of management, and the Dutch code Tabaksblat talks about the personal integrity of the manager. The picture gets clear: information security broadens! That demands specialties, new competences and an adjustment in training and training levels, not in titles. This broadening makes the domain of information security more interesting.



## CONCLUSION

The work group pleads for a limited number of educations. The titles should fit in with the existing international levels of Bachelors, Masters and Ph.D. The work group suggests using two 'Master' indications: the masters of information security management MIS-M, and the Masters of Information Security Technique, MIS-T. Both are post higher vocational education level. With respect to content and quality, the Master trainings should measure up to the RE trainings (certified EDP-auditors) and aim at the 'level 3' employees. Certification of the trainings of the two areas is necessary at an international level. The workgroup doesn't see the need for certifications at a personal level. There are simply too many and a certification doesn't indicate ones level of competence, necessarily.

As said before, this 'white paper' is but one step in a process. That's why the work group likes to receive comments and input to the following questions:

- Which task aspects are relevant/important in the two educations (MIS-M and MIS-T)??
- Idem, which knowledge, skills and attitude is expected?
- Which career paths do exist?
- Are two educations sufficient or are two matching educations needed at 'level 2' on a Bachelor level?
- What are the pros and the cons of the creation of a differentiated function for information security?
- With regard to information security, should there be training at an higher vocational education or university level, or can a post higher vocational education training combine these levels? How does this training link to the higher vocational education training for computer science?
- Is it important that the field specific expert (level 3) first go through the state of all-round professional (level 2)?

This article mainly describes the role and competence aspects of the information security officer, but how can the training and the tasks of the information security officer and the auditor be geared to one another? In which way can a person switch between the roles of information security officer and auditor?

This paper was originally published in Dutch. We would like to thank the **Information Security Practitioners Association** ([www.gvib.nl](http://www.gvib.nl)) for sponsoring the translation of this paper from Dutch to English.

If you like this paper or if you have important remarks, please send an e-mail to [expertbrief@gvib.nl](mailto:expertbrief@gvib.nl)

## LITERATURE

To achieve the expert letter 'Functions and roles in information security' the work group consulted the following literature:

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

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

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

ECABO (2004), *Beroepscompetentieprofiel Digitaal Rechercheur*, [www.ecabo.nl](http://www.ecabo.nl)

higher vocational education-I stichting (december 2004), *Bachelor of ICT, een competentiegerichte profielbeschrijving*, ISBN 90-9018970-x

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

(ISC)2 (2005), *Support throughout Your Information Security Career*, [www.isc2.org](http://www.isc2.org)

Meeuwisse Henk (oktober 2004) *Informatiebeveiliging vraagt sterke sturing*, Automatiseringgids 44, en cursusmateriaal NEN 7510 (Informatiebeveiliging in de Zorg)

Noord Fred van, Blankendaal Hans, (2004), *Nieuwe Opleidingen voor Informatiebeveiligers*, Informatiebeveiliging 4


Tittel Ed, Lindros Kim (2004) *Careers and Certification Tips, Charting a path through the security certification landscape*,

[http://searchsecurity.techtarget.com/tip/1,289483,sid14\\_gci990011,00.html?track=NL-105&ad=487582](http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci990011,00.html?track=NL-105&ad=487582)

## APPENDIX: LICENSE FOR THIS PUBLICATION

This expert letter has been published according to the following license:

<http://creativecommons.org/licenses/by-sa/2.5/>




**creativecommons**  
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:**


 **BY:** **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.