GvIB Expert Letter – September 2006
ISSN 1872-4884, Volume 1 – No. 2

Security Management KPI's from raw process information to relevant steerage information

Henk Bel

Bart Bokhorst

Lex Dunn

Ben Elsinga

Ronald van Erven

Hotze de Jong

Karin van de Kerkhof

Tonne Mulder

Fred van Noord

Ernst Oud

Frank van Vonderen

This expert letter has been prompted by the growing need for measurement of Security Management. Many published measurement approaches are derived from checklists of security standards. Often they are abstract and, in practice, difficult to implement. Collecting the right information requires a substantial effort and requires experts to make translation leaps. The expert group poses the question if, without too much extra effort, objective Key Performance Indicators (KPI's) can be derived from a process wise approach to security; and can both approaches be positioned against each other?

http://www.gvib.nl/
✉ expertbrief@gvib.nl

2

INTRODUCTION SECURITY MANAGEMENT KPI'S

What prompted this expert letter is the growing need for measurement of Security Management. Many published measurement approaches are based on checklists derived from security standards such as Cobit or ISO17799. They are often very abstract and, in practice, prove difficult to implement, or resultant measurements provide no relevant steerage information. Collecting relevant information requires a substantial effort and requires experts to make translation leaps. The expert group poses the question if it is possible, without too much extra effort, to derive objective and directly employable Key Performance Indicators that have been derived from a process wise approach to security. And can both approaches be positioned against each other? This expert letter is the first step to initiating a thought process about this.

The need for KPI's is clear. In an increasing measure new laws and regulations such as the Sarbanes Oxley Act (SOX) demand adequate 'corporate governance'. In order to illustrate that an organisation is 'in control' of its procedures, regular measuring and reporting must take place. Results can be utilised for external reports, but are primarily meant for direction steerage and internal procedures. Clearly defined KPI's can contribute to an improved sense of understanding and communication between ICT departments and the company management.
Within the realm of corporate governance Security Management becomes more important and in turn reveals a need for KPI's. The new ISO standard derived from the BS799 part 2, release date spring 2005, also points to defining security management KPI's.

Practice teaches us that defining utilisable security management KPI's is not so simple and many organisations do wrestle with them. That is why it is interesting to take practical experiences and place them under the microscope for critical questioning. Is it possible to detect a common thread within the muddle of security related KPI's? Do present KPI's live up to the information demands of various target groups? If not, what is the reason? What are the steerage variables in the different maturity phases of Security Management? Which KPI's prove effective in practice?

Gathering measurement information about Security Management appears to be more complicated than with other ITIL procedures as the security management procedure is defined at a higher abstraction level. The reliability of measurement information is also largely dependent on the quality of the basic processes of which the security level should be controlled.

The accumulation and interpretation of information for each report requires a large amount of effort and is a source of cost. One of the challenges, therefore, is to research the possibility of deriving KPI's from day-to-day security management processes, such as incident settlement and application change management, with less effort and at lower costs.

A group of security experts encompassing a wide range of experience from the Information Security Practitioners Association and the Platform for Information Security, on the basis of the above-mentioned questions and their own experiences came up with present-day practices. Research extended to preconditions and basic factors that determine the effectiveness of KPI's, and the way in which KPI's come about and can be brought about.

This publication is an illustration of these results and has come about with the cooperation of those persons as mentioned on the front page; Bart Bokhorst as problem owner, Ben Elsinga as facilitator, Tonne Mulder as co-facilitator, and Henk Bel as ghost writer.

THE RESEARCH QUESTIONS

The questions the expert team eventually aims to answer are:

- Is it possible to define a set of objective measurements for security management that stem from a process wise approach to security? And what is their range?
- Is it possible to position the 'checklist' approach and the 'systematic' approach in relation to each other?
- Is it possible to make an outline of guidelines?

The expert group did not aim to define a new process model to which KPI's can be related. Many articles have already been published on the subject of security management processes, e.g. by the NIST.
The Plan-Do-Check-Act model (Demming circle) as described in BS7799 part 2, offers sufficient leads to relate KPI's to an Information Security Management System.
The expert group also does not wish to answer the question of which norms are precisely good and which presentation forms are the best. The assumption is that norms are present and that the presentation form is free of choice.

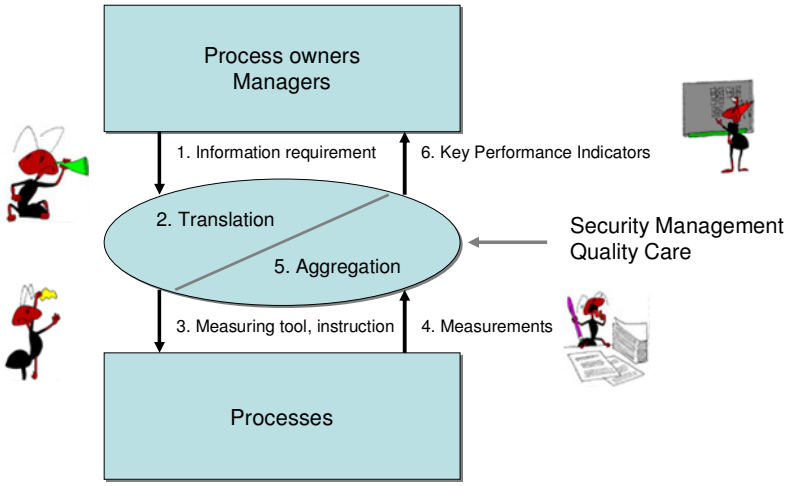
PRECONDITIONS FOR DEFINING KPI'S

Who are the stakeholders and what are they trying to steer?

With some effort an organisation can produce an enormous stream of raw measurements. Processing this information however is time-consuming, which is why it is important to be selective and accumulate specific information in conjunction with a clearly defined information requirement.

This illustration depicts a generic picture of the information gathering procedure.

4



In order to gather measurements in a cost-effective way and to define useful KPI's, two questions must be answered clearly:

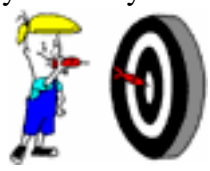
- For whom is the KPI intended and what information requirement does this person or role have?
- Which process or aspect must be steered on the basis of the KPI?

It is of little effect to define a KPI without considering which process must be steered on the basis of the KPI and how this steerage is meant to take place.

Eventually, the costs induced for reporting on the KPI must be justified by intended improvements resulting from the procedure steerage.
The KPI must be defined in such a way that the person responsible for steerage of a process can manage it and recognise its importance. If the definition of the KPI is not at the right level aligned with the process in need of steerage, the KPI will not be used effectively.

The information requirement of various roles in the organisation is largely dependent on the process for which the designated role is responsible. KPI's for managers on strategic or tactical levels will vary in character from those for employees on an operational level. Recognising different target groups is important.

Information security is a tricky theme for many process owners and especially for many business managers. Practice teaches us that process owners often experience difficulties in defining the correct information requirement. Good communication about the meaning of a KPI is essential. In this way, the process by which the definition of a KPI is reached can be more useful than the exact definition of the KPI itself.



The context is important

'**Measuring does not mean knowing**' when it comes to KPI's. Without knowing the context a raw measurement will tell you very little about the desired steerage.

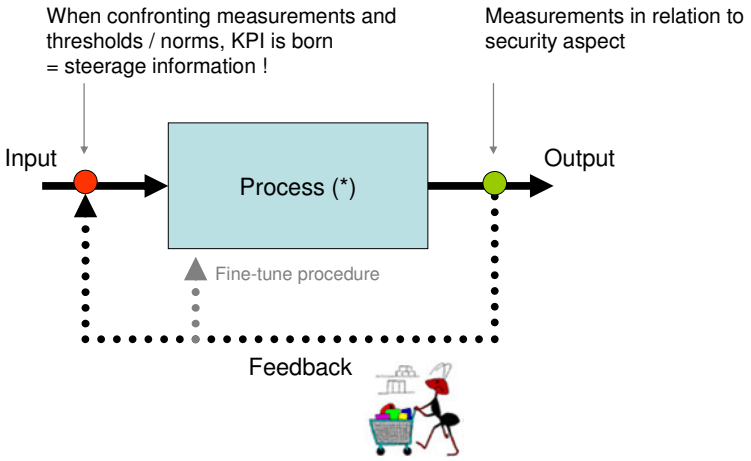
A KPI will tell you nothing without knowing the context!

A good example to illustrate this problem concerns the registration of a number of incidents. An increase in the number of registered incidents can result in different reactions, such as:

- Security measures must be sharpened as the number of incidences is increasing.
- Because signalling and registration is improved, a concise picture is given concerning the amount of incidences taking place.

In order for a KPI to be effective, the KPI must be accompanied with a *clarification of the context and an explanation of the trend.* The KPI must be *related to a norm in order to steer*. Eventually, many process owners will be helped immensely in their steerage if advice is included on which measures should be taken.

The figure below illustrates again how a KPI is used as a process steerage element in the feedback loop of a process.



(*) with a to-be-defined security aspect to be measured

6

WHICH FACTORS INFLUENCE THE CHOICE OF KPI'S?

The expert group has posed the question of which factors influence the choice of the type of KPI's and the effectiveness thereof.

KPI's must be aligned with a business goal:

- KPI's must be in accordance with risk or aims that are recognised by the various stakeholders. When the (business) risk or objective is not lucid a KPI will not come alive.
  KPI's are measured by measures. It is desirable to not define the KPI too specifically so as to avoid the KPI influencing the selection of measures still to be implemented.
- Are the KPI's meant for internal use or for external communication to customers, partners, shareholders, affiliated organisations, certifying bodies, etc.? Must they be connected to other standards in the sector so that KPI's are somewhat comparable between organizations or is an organization free to choose their own definition?
  N.B.: Even when using the same framework (for example Cobit) the comparability of KPI's will never be optimal. Organisations will always, in practice, make a translation to their own situation.
  An example of use of KPI's for external communication concerns the definition of service levels with outsourcing. Well-defined KPI's assist in gaining a grip on the level of service provided from the (outsourcing) partner. Reports about the number of screened system administrators, the number of incidents that are stifled by preventative measures etc., provide more insight into the efforts of the service provider than a statement that provision of service will take place according to best-effort.
  The buying party must be sure to stay in the lead of the KPI's definition to avoid being saddled by the other party with KPI's that are meaningless and leave them with insufficient steerage.
  Seeing that defining unambiguous security KPI's is already tricky, this last aspect is even more relevant here.
- How generic or how specific must a KPI's definition be? Are they applicable to the whole company or just for a department?
  In a centrally run organisation a KPI can be much more generically defined across different process than in a de-centrally run organization. After all in a de-centrally organised organisation similar processes will differ more and therefore so will the measurability and steerage possibilities. And KPI's must fit optimally with a process in order for it to be effective.
- Are KPI's stable during the life cycle of the subject to be measurement?
  During the life cycle of an application, for example, the need for measurements shifts. KPI's that play a role in the development phase of applications differ from those in the operational phase. Also the target group being reported on can shift during the life cycle.

Measurements must be trustworthy and meaningful

- What maturity level does an organisation or a process have and which KPI's are useful for this maturity level? Controlled measurement of certain KPI's demands reproducibility and a tight canvas in the execution of administration processes. KPI' s meant for tuning of an administration process that is not (yet) there have little additional value. The accumulation of detailed measurements and trend information

concerning intrusions, for example, is of little use when an organisation does not have its basic incident management process in order.

- The measurability of the desired information is important.
  The filling in of a security paragraph in a project phase document is simple to measure. Whether the quality of the paragraph is sufficient, is already more difficult to determine and without the involvement of security experts will probably not lead to accurate and objective information.
- In all scenarios the integrity of measurements is of great importance. And the costs of the measuring must be in balance with the eventual objective. Often tooling is required to keep measurements cost-effective during a longer period of time, to guarantee integrity and to keep reports consistent. With manual aggregation of information, manipulation is possible and reliability cannot always be guaranteed.

Other aspects

- KPI's on different levels must be correlated and provide a consistent view. Multiple KPI on a lower level can be translated to one KPI on a higher level. Because these KPI's are usually geared towards another target group with a higher aggregation level, word usage in the explanation must often also be adjusted. The word usage must fit in with the actual world and interests of the target group. Higher management may for example be more accountable for the percentage of application development projects where a risk analysis was carried out in due time, than for the completeness and depth of an analysis carried out for a specific development project.
- Aside from standard reports there must be a mechanism for exception reports. Exceptions are important to keep people awake. In the case of exception reports it is often effective to give people **'the naked truth**'. Allow the shop floor to speak and do not try to make the reality prettier than it actually is. If for example, the management of a department does not tackle events that structurally occur and remains vague about it in his reports, it can be worthwhile to magnify an incident with more than average impact. Diligence and care for disclosure of sensitive information remains an important factor.
- The chance that Security Management KPI's are effectively used is greatest when applied to processes where people are already used to reporting other quality aspects buy means of KPI's.
  This is reason to define Security Management KPI's based on a process approach and to assure that KPI's are built into processes where security is relevant, such as incident management and change management.

DEFINITION OF KPI'S: HOW TO START?

When an organisation wants to begin to define KPI's it can generally choose two approaches, the top-down approach, which requires management commitment, and the bottom-up approach whereby initial reports based on measurements at hand are the stimulant for more and sharper reports.

Top-down

As an example, the choice was made here to use the Security Metrics Guide for Information Security of the NIST which depicts a model with a top-down approach. The figure below

depicts a component model, for which is stated that all components need to be filled in when setting up an effective security metrics system.
The basis and starting point in the model is obtaining a strong top-level management commitment. Subsequent policies and measurements must be defined.

The work group only partially shares this vision and is of the opinion that this approach is often far from optimal.

The top-down approach will work especially when management is experiencing great pressure, like for complying with SOX regulation on time. This is only attainable in the short run with sufficient management commitment. This approach will, in nearly all cases, be based on checklists from existing models like Cobit.

However, as indicated before, practice teaches that process owners find it difficult to define correct information requirements for KPI's. There is a large chance that the whole process of defining a KPI takes too long, the whole construction becomes too complex and theoretical, costs too much money, leads to great frustration, and eventually leads to nothing.

Bottom-up
An alternative approach is to 'just start anywhere' with presentation of easily obtainable measuring results from operational processes. In this way management is made aware of the interesting information reported from processes which can be used for steerage. Initially the information offered will not suitably comply with the information requirement of the process owner, but the imagination of the process owner will be stimulated and he will be in a better position to define a modified KPI which is more in line with the requirement.
By means of an iterative process, KPI's can be constantly improved. Important in this bottom-up approach is that expectations must be well managed to avoid the threat of a process owner quitting prematurely and losing his confidence.

N.B. It must be noted that also during a top-down approach multiple iteration hits are necessary to define usable KPI's. Many firms that force SOX reports within their organisation via the top-down approach experience this. Also in this alternative the risk exists that process owners lose their confidence when they see that huge reporting efforts do not lead to satisfying results fast enough.

The top-down method runs the risk that reporting takes up vast amounts of time because measuring does not naturally align with existing processes. The bottom-up method runs the risk that KPI's provide steerage information largely on an operational level, and insufficiently on tactical and strategic levels for higher management.

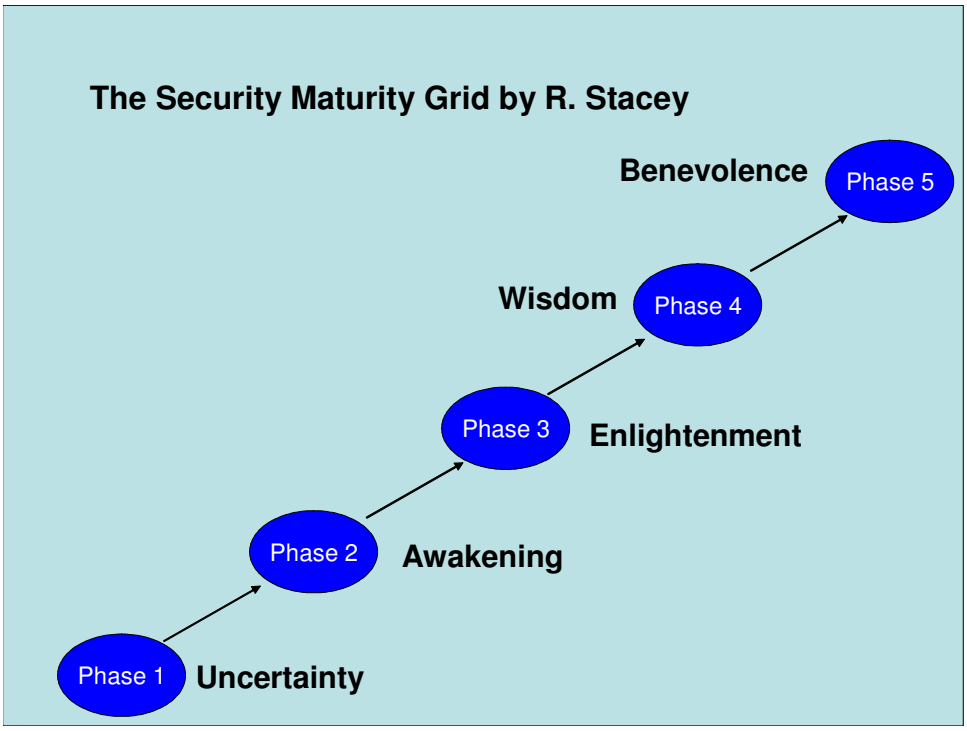
Simple action plan for bottom-up approach

For organisations that do not work with Security KPI's and where management does not require security KPI's, the expert group suggests opting for the bottom-up method, in which case the next list of action items can be useful:

1	[Optional] Determine security maturity e.g. by examining Stacey's security model (see below)
2	Keep registration of: • Incidents (reactive) • Identified risks (proactive) Classify these e.g. by sort, object, department. Also think outside the IT department
3	Personalise reports to target groups For example: Legal matters, HRM, financial affairs Aim is to increase awareness
4	Explaining reports per part area - Point out consequences per responsibility area Refer to damage table, in which damage categories are defined
5	Expand this: • Formalise KPI's: Where is the threshold? • Ascertain trends • Provide steerage by coupling trends to advised measures.

Security Maturity Models

Maturity models help an organisation to take a look at itself in the mirror to determine how mature its processes are. Per level typical characteristics are provided of the extent to which an organisation controls its processes. The Security Maturity model by Stacey is a simple model that can be used in the area of security.



Uncertainty	The enterprise does not understand why it keeps having problems with its information assets. It has a high error rate; its information assets appear vulnerable, unstable and imprecise. Company secrets appear to be public information.
Awakening	The enterprise in phase 2 does not understand why it keeps having problems with the security of its information assets. It has a high incident rate, the information assets appear vulnerable and her secrets seem unprotected.
Enlightenment	Through management commitment and focused development of security, the organization identifies, prioritises and secures its information assets. The organisation seeks to prevent instead of exclusively reacting to incidents as they arise.
Wisdom	The information security activities of the enterprise are planned, budgeted and routine. Through the use of an enterprise specified threat model and focused risk analysis this enterprise comprehends its vulnerabilities and protects its information assets.
Benevolence	The enterprise in phase 5 knows that her information assets are protected and that they will remain so in the future. These assets remain protected because the enterprise actively steers its information security activities and optimizes its strategies.

Naturally other models can also be utilised such as the security maturity model by Gartner.

CONCLUSIONS AND FOLLOW-UP

In light of the research questions the expert group has as yet drawn very few real conclusions. It is certainly possible to define KPI's that evolve from measurements of existing security management processes. It is, however, still unclear if, and to what extent, these KPI's are objectively measurable and are generically meaningful for different environments.
In this expert letter a positioning is provided of the top-down 'checklist' approach against the bottom-up 'process wise' approach, with their accompanying pros and cons. There is still a need for further depth in both approaches.
It is still too soon for the definition of an outline with guidelines for KPI's in different situations. More experience data is required for this and further depth is desirable.

Some useful observations have been made in the discussion and the expert group suggests a further assessment of the process wise bottom-up approach, as this complies most naturally with the processes in an organisation. Because security in the long run will become more like a 'normal' quality aspect, it is desirable to align as much as possible with quality reporting organisations are already familiar with.

The work group realises that the definition of Security KPI's is still in infant shoes and that this expert letter is no more than a prompt to further discussion.

Important observations:

- Condition for defining security KPI's is that it must be clear what the steerage variables are in an organization and which role is responsible for this steerage. KPI's must be compatible with this.
  The KPI must be defined in such a way that the employee responsible for steerage of the process can do so effectively and recognises its importance.
- It. is important to recognise that different target groups have different information requirements and that KPI's must be available per target group.
- With the choice of KPI's, the goal must be lucid, the organisation must have an idea of its own security maturity level and it must be ascertained whether the KPI is cost-effective, reliable and controllable.
- "Measuring does not mean knowing". A KPI has little meaning without knowing the context.
- The two main approaches for defining KPI's as illustrated in this article, each have their own specific pros and cons. This choice is partially dependent on the objective (external comparison or exclusively internal procedure steerage).
- For organisations that have not yet defined security KPI's and experience little external pressure to define them, the bottom-up method seems a good way to start to realise a number of quick wins as soon as possible.

How further?

Due to the complexity of the material and limited time-frame to discuss this subject, many questions still remain unanswered:

- Are we able to make an outline with practical guidelines?
- A number of pitfalls have been mentioned. What other pitfalls can still be distinguished?
- Are there any generic KPI's recognised as applying to all organisations?
- Can we ascertain a top 10 list of KPI' s that work well in practice?
- What are the steerage variables in the different maturity phases of Security Management?
- Can we link KPI's to target groups in the INK model?
- Can audit processes become faster and cheaper if good KPI's are defined as the focus of the audit process can then shift to the KPI measuring procedure? Can it shift the character of audits from taking a snapshot in time to due course control?
  Or: From digital flash box to due course control
  …. And we all know how effective course control is ☺

This article is no more than a first attempt to prompt a broader discussion in which the input of as many related persons as possible is desired. The expert group invites you to respond.

We would like to thank the **Information Security Practitioners Association** (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

LITERATURE

In order to bring about the expert letter 'Security KPI's – From raw procedure information to relevant steerage information', the work group consulted the following literature:

NIST, Security Metrics Guide for Information Technology Systems

IT Governance Institute, *Cobit*

A Koot, *Enhanced Security Management*

A Koot, *Beveiliging: Balanceren tussen vraag en aanbod,* Information security May 2004

Ernst Oud, *Kosten en baten Informatiebeveiliging*, article Yearbook 2002

A van Gils, Philips, *Meten op basis van Cobit*, presentation GvIB 19 March 2002

ISO, *ISO/IEC 1st WD24742 Information security management metrics and measurements,* 2004

Robert Veenstra, NFI, *Meten is weten, Evaluatie van Informatiebeveiliging, Balanced Scorecard*

GIGA Group, *A Balanced Scorecard for Security*

SABSA limited, *White paper Systems and Business Security Architcture*

Peter van der Wulp, Erasmus Universiteit, *referaat Het meten aan security*, KoSMoS

Ben Elsinga, Presentation *Overwegingen en voorbeeld modellen/ kapstokken. KPI's ten bate van informatiebeveiliging*.

The Information Security Program Grid", Timothy R. Stacey, Data Security Management, Auerbach Publications 1996

14

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.

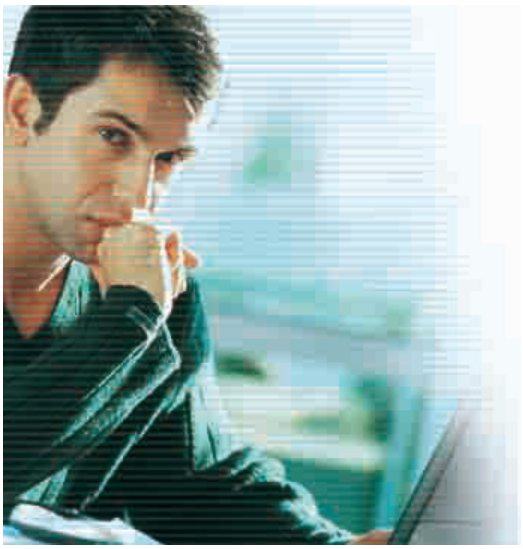
- For any reuse or distribution, you must make clear to others the licence terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

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.