Implementing an ISO compliant Information Security Management Framework

besecure
Managed E-Business Security™

When referring to information this is the equivalent of valuing the confidentiality, integrity and availability of it, and hence when managing the security of information we need to consider these three aspects – much more than the common layman understands by the word ‘security’!

Organizations that wish to manage their information security arrangements typically introduce a set of policies and procedures that help them exercise a degree of control to provide assurance with regards to these three aspects. This is generically described as an information security management system

Companies will be driven by at least two factors: the requirements of their stakeholders and/or customers, and the need to remain competitive. Many sectors have regulators that demand some form of information management. There are requirements through governance regimes that information and information processing arrangements are subject to control to enable directors to discharge their duties effectively and with high profile governance failures in the headlines this is an area that will only grow in pressure to comply.

With the increasing trend to rely on business partners for key services and processes, the need for some form of information security assurance is growing rapidly. Outsourcing and other contracts are now increasingly starting to specify compliance with some form of information governance regime as a mandatory requirement. The other key driver is that of maintaining a competitive edge. An effective information security management system needs to address issues relating to personnel, facilities, suppliers and cultural issues in addition to the area of Information Technology, and so information security is a topic that goes well beyond the remit of the IT department. The next stage of an effective information security management system is to identify exactly what areas and aspects of the organization will be affected. Starting with the source of the challenge, we need to include all of our information, which means including all the equipment on which that information sits how it is moved/transmitted and any aspects of the business that can affect them. This therefore involves setting both physical and logical perimeters for our information security management system. In practice this means that it is necessary to consider dependencies and interfaces of all aspects of the system and the information it controls. For example, if we consider information that is sent by courier to another office of the same organization then we need to include the reliance on the selection of the courier company and the requirements of the contractual relationship with them. With regards to confidentiality it is necessary to consider all those who have access to the information and the equipment on or in which it is stored. This is likely to include cleaners and maintenance staff, in addition to directly employed staff.

The system also needs to address the management of information in different formats, including electronic form and hardcopy records. With information in transit, whether it be in the form of papers being taken outside, or records being sent to archive, it becomes obvious that these warrant a similar degree of protection as electronic copies. If a trade secret is accessed by a competitor it does not matter whether it is in an email attachment or on a printed piece of paper – the information that was meant to be kept confidential is out and so any value attached to maintaining its confidentiality is compromised. The value of information is in the content, not the format it is stored or available in.

Considering these issues, one way or another, the ISMS needs to define how it addresses relationships with suppliers, business partners, customers, and staff. In defining the remit of the ISMS this way the organization is stating the scope of the assurance the system provides. Given the personnel, facilities, suppliers and cultural issues that need to be considered and addressed within the system, it is obviously a topic that goes well beyond the remit of the IT department. As with most topics, there are International Standards that deal with information security management, and the main one is ISO 27001:2005. This standard defines a project approach to aid the design and implementation of an ISMS, and uses the well recognized Plan-Do-Check-Act model (P-D-CA) to structure the tasks required to introduce an effective ISMS.

The P-D-C-A cycle can be summarized as:

- Plan what you need to do to achieve the objective (which can include defining the objective);
- Do what you planned;
- Check that what you have done achieves what you had planned for it to achieve and identify any gaps or shortfalls; and
- Act on the findings of the plan phase to address the gaps.

Typically this last stage will involve making a Plan, Do-ing what that plan entails, Check-ing that the objectives were achieved and identifying any shortfalls and then Act-ing on the findings by Plan. And so with the introduction of an ISMS using P-D-C-A, the initial cycle of continuous improvement is effected.

One common misunderstanding is that the planning stage is limited purely to planning the project. As far as ISO 27001 is concerned the planning stage includes all the work required to determine what is required of the ISMS, and how this is to be achieved. This is a significant undertaking, to the extent that it can take up to half of the time through to having a full ISMS in place. The other main resource demanding stage is implementation.

There are a number of requirements for a management system to operate that are as applicable to an ISMS as for any other management system, and these include:

- Document control. This is an arrangement to manage the availability of documents within the ISMS, typically including:
    - the corporate level policy;
    - operating procedures which describe the
    - processes that support the policy and explain
    - who does what, where and when;
    - work instructions that detail how certain
    - tasks should be conducted; and
    - forms which capture the information that is
    - essential for the purposes of review and as

  The aim of the document control procedure is to ensure that all these documents have been written and approved by the right people and that only the latest approved versions are available to those who need to be aware of and follow them.

- Internal audit. Internal audits can be used for many purposes, but one of the main objectives for deploying an internal audit regime is to monitor compliance between the management system requirements and working practice. The internal audits are commissioned by the organization, for the organization and provide an opportunity to review and enhance the level of compliance within the ISMS by examining what actually happens across a sample of events and processes and comparing this to what the documented management system describes. The identification of any mismatch during an audit provides the opportunity to put it right, either by changing the system description of what happens, or enhancing working practices. Internal audits can also be used to investigate specific areas of concern or for the purpose of identifying opportunities for improvement.

- Management review. Given that management initiate the ISMS by approving the use of resources to undertake the project, and issuing the corporate Information Security Policy, it is reasonable to expect them to review the progress of the implementation project and the effectiveness of the ISMS thereafter. The management review is typically held once every six or 12 months and is intended to achieve exactly these objectives. Typically a number of reports would be prepared for the meeting covering key indicators of how the ISMS is operating. These reports include an analysis of the outcome of audits (internal, second and third party), significant security-related incidents, some form of indicator of awareness of information security issues and the ISMS across all those affected by it, and an indication of the amount and timeliness of any improvement work undertaken.

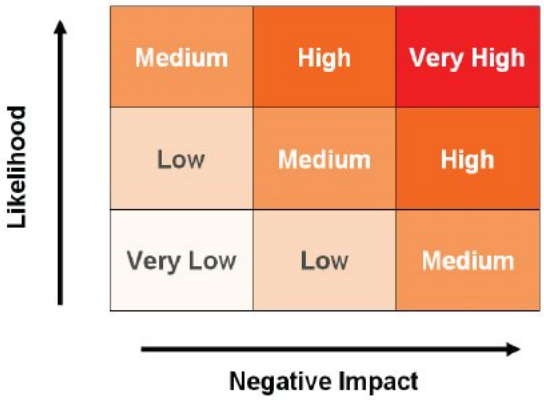
An information security risk assessment is the key to any ISO 27001 ISMS, forming the lion's share of the Plan phase of the initial P-D-C-A cycle for implementation. To undertake the risk assessment it is necessary to have defined the scope of the ISMS, and of to have understood the concept of information security assets: it is the value of these individual assets that is the subject of the risk assessment.

For the risk assessment to be effective a comprehensive information asset register needs to be produced. That is to say, a list of everything that has value to the organization, including information, information processing and storage equipment (every server, computer, laptop, PDA, mobile phone), systems, staff, buildings, etc. It goes well beyond the more common fixed asset register. Each item on this list needs to be risk assessed using a common methodology. The value for each asset is estimated for the three information security attributes: confidentiality, integrity and availability. The value assigned for each reflects the total cost to the organization if that attribute was compromised for the asset concerned, from the cost of replacement, through the consequences for the process(es) it is involved in, to the impact on the organization's reputation. This is normally best estimated by those involved in the relevant business processes.

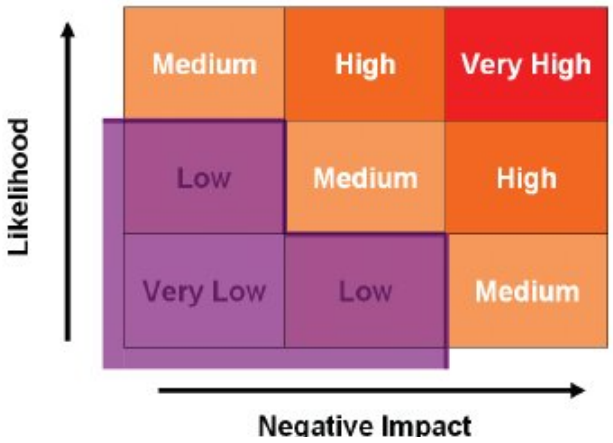
These values provide the impact aspect of the classic

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

relationship. The likelihood value comes from the possibility of a threat exploiting a weakness or exposure, or, in information security terms, a vulnerability. For this to be undertaken against the values associated with the three attributes for all the assets on the register once again requires a common methodology and access to a comprehensive list of threats. The risk assessment then uses these estimates to determine the risk value for each asset. The relationship between likelihood, impact and risk is demonstrated in the following diagram, in this case showing three levels of likelihood and three levels of impact, which together give five levels of risk varying from 'Very Low' through to 'Very High'.



The main aim of an ISMS is to manage all risks to a consistent level of control, and so this is where management need to determine what level of risk is acceptable. For example, they may, using the parameters in the diagram above, decide that risks up to and including 'Low' are acceptable, and so it is only those risks that have been assessed as falling above that level of risk acceptance criteria that need managing. In terms of the diagram, the risk acceptance level can be demonstrated by the shaded area as shown here:



Each organization will have a different level of risk acceptance and this will relate to the organization's risk appetite – the degree of risk that the organization is happy to live with on a day-to-day basis. Risks assessed as falling above the acceptable level are treated with the selection of various controls that are designed to reduce risks. As different controls are selected for application to various assets the risk assessment is re-estimated and this process continues until all the assessed risks are estimated to fall within the risk acceptance criteria. The controls are normally taken from the list in ISO 27001 at Annex A. To effect the required level of assurance against information security risks the ISMS needs to ensure that the controls selected through the risk assessment process are in place and applied to the appropriate assets effectively. By informing the selection of information security controls with the risk assessment approach an organization can ensure that it is maximizing the effectiveness of its information security spend, and not leaving any one area of risk open to exploitation at the cost of an unreasonably enhanced level of control elsewhere.

ISO 27001 requires a document to be produced that details which controls are applied within the ISMS and which are not. This is known as the Statement of Applicability.

The whole risk assessment process requires a degree of central coordination, and often benefits from the use of a suitable software solution that can automate many of the potentially resource-intensive administration aspects of the process. The investment in such software really pays back when the ISMS gets into continuous improvement as the risk assessment needs to be revisited, either in part or as a whole, frequently.

Having an appreciation of the methodical approach to the selection of information security controls next step is to examine the controls defined in the international ISMS standards.

The standards themselves go to great pains to emphasize that the controls they detail are not exhaustive and that each organization should review them and add their own as required. But typically this would only come about in the early days of an ISMS if there were specific contract or sector requirements that went beyond what is already available.

In the standards there are over 130 controls split into 11 categories, but for the purpose of familiarization here we are considering them in six groups, and not in any detail. The six groupings are not significant in any way, and they could easily be formed differently.

Organization, structure and HR

This list includes the main controls off which the rest of the system hangs. There is a need for a corporate level Information Security Policy, which is a statement of the organization's commitment and objectives relating to information security. This needs to be available to everyone affected by it, which (as described earlier) includes suppliers, business partners, customers, and staff.

There is a need to define where responsibilities for information security lie within the organization and that the required forums and review bodies are in place to meet the needs of the ISMS. The human resources required to undertake all tasks relating to and affecting information security need to be sourced and managed appropriately. This includes considering the sourcing, vetting, management and exiting arrangements for staff, contractors and any other people who interact with the scope of the ISMS, including anyone who has physical access to any premises at or from which information-related assets can be accessed.

Assets, classification and access control

The register needs to go beyond the classic fixed asset register and include information assets. There is a control suggesting that assets are classified to an internally-defined labeling scheme, and the classification will indicate the level of protection required and who has approved access rights to them. Access control is also related to how to ensure that only those with approved access to the assets can actually access them, and this is subject to both logical and physical barriers.

Passwords and user IT accounts are typical logical access controls, and are only as robust as the practices to manage them, eradicating poor practices such as writing them down, or using sequences or easily-guessable combinations. Where access issues are risk assessed as requiring a greater degree of assurance, with regards to accessing a system or application remotely say, there is the possibility of two-factor authentication. This is where each unique user has to deploy both a physical key (token) and a logical key (password) in combination

to be granted access. An example here is a credit card being swiped in a store (the magnetic strip / smart chip being the physical key) and your Personal Identification Number (PIN, the logical key). There are also controls which can be deployed, such as session timeouts, that require the user to re-enter selected log-on criteria every so often and duress alarms that consist of a pre-determined series of innocuous key strokes which alert network / system monitors to a problem without making anyone in the vicinity of the user aware that an alarm has been activated.

Physical

Physical access is also a concern for information security. Anyone who has access to the equipment or medium on which information is stored could potentially walk out with that asset and the information assets stored on it. Whilst some protection can be offered to prevent access to information stolen in this manner, it will still affect the availability of that information and possibly the resulting integrity as well. With continuing advances in technology it is impossible to remain ahead of thieves and crackers / hackers. Passwords can often be broken and whilst encryption (the use of one numeric algorithm, or key, to scramble and the alternative of the key pair, another algorithm, to unscramble it) provides an enhanced level of unwanted access prevention (logical, not physical), there are incidents of encryption controls being beaten, almost exclusively due to the mismanagement of keys, and so the combination of logical and physical controls is essential to an efficient, effective ISMS. Perimeters around secure areas should be defined in all three dimensions – tunneling in through the floor, or using an air vent in the ceiling, may still allow enough access and egress for a theft to take place.

Networks and IT

The largest category of controls relates to IT operations and network management. They cover issues including planning and testing new developments prior to implementation, capacity planning for all aspects of the network and systems, segregation, network design and technical vulnerability management. Issues such as back-up are mentioned here, along with testing of the back-up so that, as an example, any accidentally-deleted filed can be restored from the copy of all files (the back-up) run the previous night.

Incident Handling and Business Continuity

There are a number of categories which deal with the handling of problems, events and / or incidents. These are in addition to the improvement process requirements of maintaining an ISMS, and deal with what should be done in reaction to, and as recovery from, a security breach. The severity of information security breaches can vary massively. If the problem is likely to cause a significant challenge to the normal running of operations it is likely that some form of business continuity will be invoked. This area of control includes the need to regularly test the Business Continuity Plans (BCPs) so as to learn from the experience and improve the plans

ahead of whenever they may be invoked for real. Not all security incidents require such a dramatic response, but the degree of reaction and the method for determining escalation should be defined. All of these issues are key areas for information security awareness campaigns as the organization should be in a position to benefit from notification of a potential problem as soon as possible. This therefore means that awareness needs to be raised and maintained for all relevant parties, including suppliers, business partners, customers, and staff. Often cleaners will be among the first people at a site each day, or the last to leave it, and they should be trained and required by contract to report any security-related observations to an appropriate contact.

Compliance and Internal Audit

These categories are relatively self-explanatory: they deal with legal and technical compliance, requiring the organization to be aware of, and comply with, its legal obligations. Technical testing confirms that equipment, systems and software on the IT side are as they should be. The schedule can include checks to confirm that only the right approved equipment is connected to the network, that systems and software are as they should be – the approved mix and number for the licenses held – and can include penetration testing to confirm the resilience of the technical measures in place.

Certification

As with many other management system standards, there is a scheme that can be used by organizations to demonstrate their compliance with the internationally recognized standard for information security management, ISO 27001. Companies wishing to use this standard to demonstrate the robustness of their information security management arrangements need to subject themselves to an external audit.

For the assurance the outcome of the audit provides to be recognized it needs to be conducted in compliance with the recognized scheme, that is, the ‘accredited certification scheme’. This is a scheme which is administered by the United Kingdom Accreditation Service (UKAS) and certificates issued under this scheme will bear the UKAS logo. The audits are conducted by accredited bodies and those seeking to demonstrate compliance with the standard become certificated, not accredited.

Accreditation bodies around the world sign up to a Memorandum of Understanding that results in mutual recognition of each other’s schemes, and so a certificate issued by the Joint Accreditation System of Australia and New Zealand (JAS-ANZ) will be the equivalent of one issued by UKAS and hence a worldwide scheme exists. The scheme enables organizations to demonstrate a degree of assurance with regard to their information security practices. The integrity this scheme has can result in customers relying on certification rather than insisting on sending their own auditors in to provide the assurances required by their own

directors, stakeholders and clients. This can save a lot of time and disruption for both the auditing and audited parties – a benefit that contributes to the uptake of ISO 27001 certification.

However, claims of ISO 27001 certification are often misinterpreted, or used as a guarantee where they should not be. To gain certification the organization needs to comply with ISO 27001, which means that it must have a current Scope defining the extent of its ISMS (or at least the extent of the ISMS that is certificated) and a Statement of Applicability (SoA) that defines the controls that are applied across what aspects of the ISMS.

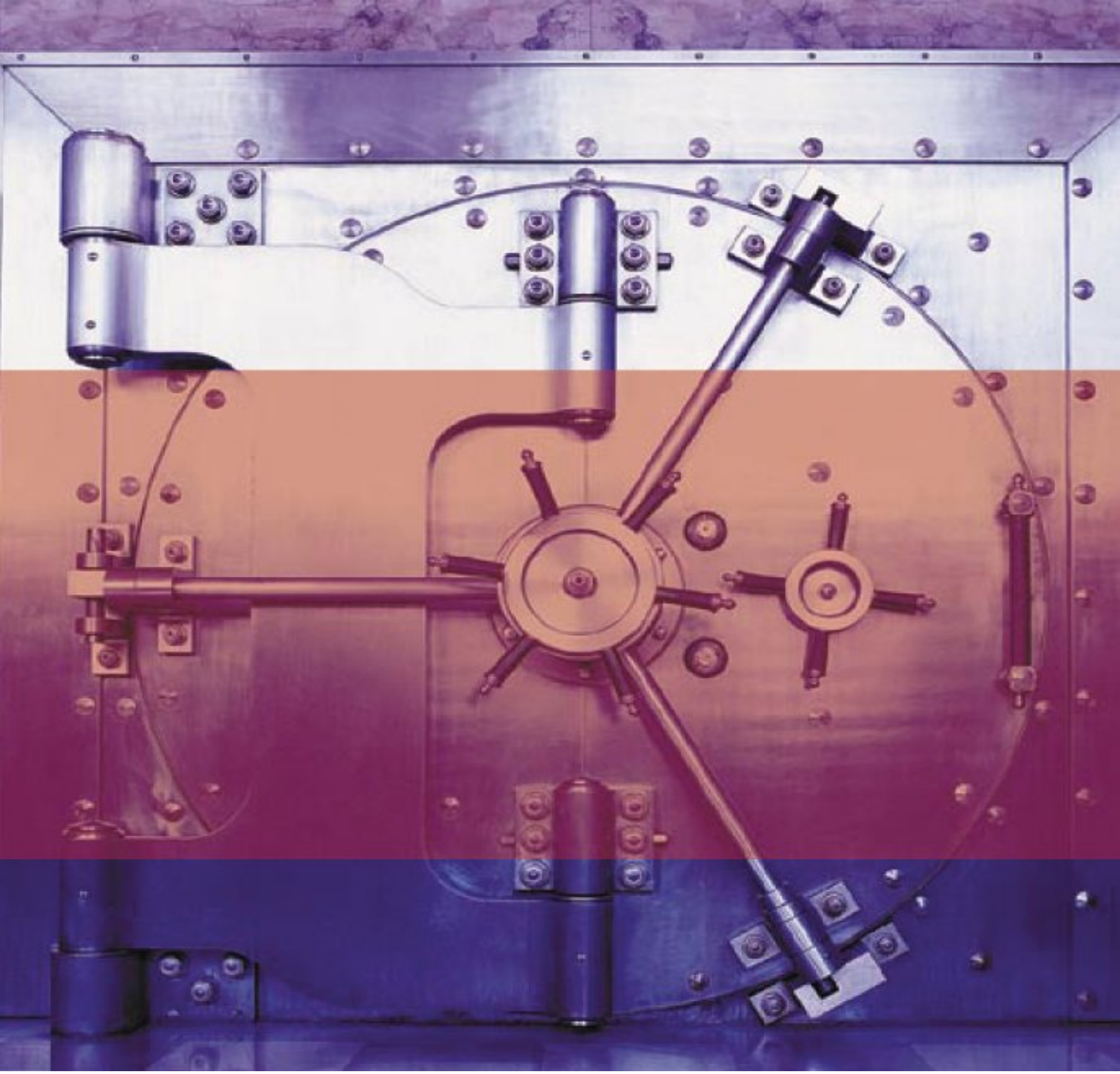
It is these two documents, together with the accredited certificate, that provide evidence of the level of assurance the organization's ISMS provides regarding its information security practices. ISO 27001 is not a product certification scheme, and to rely on it as such is nonsensical. Certification to ISO 27001 provides a service assurance.

Other audit applications

The provision of a specification for Information Security Management Systems lends itself to supplier or second party audits. This means that buyers can rely on the standard to provide a recognized and widely-available framework for supplier audits to be conducted against so as to assure them of the level of information security their suppliers are affording information that is available as a result of the contract between the two organizations. Second party audits can be used by both the auditing and audited parties along similar lines as first party and third party audits, to the benefit of both organizations and to drive continuous improvement through the supply chain.

About BESECURE

BESECURE founded in 2006 to address the increasingly complex issues concerning the security of information assets. We act as a trusted security advisor to enterprise clients from government, financial institutions and telecommunications sectors, helping them plan, implement and review security management strategies focused on people, process and technology resources. These strategies help reduce the cost and complexity in ensuring the confidentiality, integrity and availability of mission-critical information systems. BESECURE offers a range of consulting services to help organizations secure their information assets such as taking advantage of the development of an Information Security Management System based on industry best practices and ISO standards.



besecure
Managed E-Business Security™

TÜV AUSTRIA HELLAS
EN ISO 27001:2005
No. : 0808012

DIN EN ISO 9001:2008

19, Syggrou Ave.
GR - 117 43, Athens, Greece,
Tel.: +30 210 330 7 440
Fax: +30 210 330 7 441

e-mail: info@besecuregroup.com
web: www.besecuregroup.com

131, Gladstonos Street
Kermia Court, 3317 Limassol – Cuprus,
Tel. +357 25 376 800
Fax: +357 25 376 799