5

INFORMATION SECURITY ACCREDITATION - THE ISO 9000 ROUTE

R. von Solms[a] and L.R. Meyer[a]

[a]Faculty of Computer Studies, Port Elizabeth Technikon, Private Bag X6011, Port Elizabeth, 6000, South Africa

1. INTRODUCTION

Information systems services have never before been under such enormous scrutiny. Massive advances in technology, as well as greater demand for access to necessary data by users are just two of the many reasons that have brought about this situation. Global communications between organizations as well as across countries have uncovered the lack of cost-effective security measures at national and international level.

There is a need for widespread acceptance of security standards by all concerned, not only to protect investments, such as destruction and misuse of data and information, but also to instil confidence in business partners. Organizations involved in electronic trading need to know that their respective clients are reliable and secure. This task can be accomplished through a process of certification.

Gary Hardy [1] defines system certification as:
"the process whereby a (written) opinion is provided by a (widely) accepted body that particular information systems meet the [security] objectives, and are thereby fit, from a security standpoint, for a specific set of uses under specifically defined circumstances.[1]

In the same paper, Gary Hardy identified the requirement for a general certification scheme which is focused on the overall security management process in an organization. This would be similar in some respects to the ISO 9000 certification for quality assurance which considers the overall process but not specific products.

This paper focuses on this issue - "How can information security within an organization be certification with respect to a quality assurance model that is receiving such strong worldwide attention, namely ISO 9000?".

What must be very clear is that there are currently very few certification processes that are internationally exposed and accepted with a great deal of confidence. This paper suggests a possible solution to this problem, one which will not only allow an organization to certify its IT security in a relatively short time period, but also one which is widely known and commonly accepted.

2. INFORMATION SECURITY

The first step towards achieving successful Information Security within an organization is to ensure that an *Information Security Policy* is on hand. Management needs to define an acceptable security policy for securing the company's information, and to ensure its implementation. The policy is a statement by top management on the security stance to be adopted by the organization.

However, management's job does not end upon installation of the policy. They are to

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

ensure that it is adhered to, maintain and update it, if necessary, as well as taking corrective actions following any deviations from the policy. The heart of information security is the maintenance of confidentiality, integrity, availability and accountability, which, if correctly maintained, will result in a greater degree of assurance by the users for the information.

In order to meet these demands, technical security measures (passwords, etc) as well as non-technical aspects (secure operating procedures for personnel, etc) are needed. ITSEC [2] refers to the technical security measures as security enforcing functions. It is in these functions that users will place their trust.

These technical security measures are controls or countermeasures which are needed to minimize risks threatening the information resources and also to detect and prevent disasters, or to help recover from adverse affects resulting from a disaster. A *risk analysis* exercise is involved in identifying all possible risks related to an organization and risk management is the process that manage these risks, i.e. introducing security controls to defer affects resulting from identified risks.

Contingency planning and *disaster recovery* result due to the fact that no matter what you do or say, it is highly unlikely that your organization will never be affected by some or other disaster. A contingency plan prepares for such a disaster situation and includes a disaster recovery plan which will be activated as soon as a disaster has been declared.

Although information security will normally be unique to each organization, organizations would still like to be assured that their respective "trading partners" have some or other form of information security measures in place. If these security measures could conform to a set of international guidelines, then even if different organizations have unique security concerns, at least one would be able to not only recognize these measures, but also be able to understand and relate directly to them.

3. INFORMATION SECURITY CERTIFICATION

Gary Hardy [1] addresses system certification as a two step process - advice (from a widely accepted body with regards to your organizations information security), followed by management decision (whether or not a system shall be accepted for operational use). The identification of such widely accepted body will receive particular attention in this paper.

3.1. Product Certification

ITSEC [2] clearly distinguishes between an IT system and an IT product. "An IT system is a specific IT installation with a particular purpose and known operational environment. An IT product is a hardware and/or software package that can be bought off the shelf and incorporated into a variety of systems." It is important that whatever security criteria are used, it should pay equal attention to both the IT system as well as the IT product.

The Trusted Computer Security Evaluation Criteria, commonly known as the TCSEC or "Orange Book", is a widely known and accepted basis for the security evaluation of operating systems. It was developed by the US Department of Defense (DoD) in the US product evaluation scheme operated by the National Computer Security Centre (NCSC). The TCSEC criteria is intended to match the security policy of the US DoD. The policy is primarily concerned with maintaining the confidentiality of nationally classified information. The main areas covered by TCSEC are Security Policy, Accountability, Assurance and Documentation.[2]

A major problem with TCSEC is that it takes a very long time to receive a rating, and by the time the rating is given, the organization could have undergone many changes which would affect the TCSEC rating. Also, TCSEC is very much driven by security for the IT product.

Information Technology Security Evaluation Criteria (ITSEC) was developed by four European countries (Germany, The Netherlands, The United Kingdom and France), and have been cited as being more suitable for commercial systems security evaluation in addition to military usage. ITSEC is a document or book setting out "IT security evaluation criteria". The criteria set out in this book (sometimes called the white book), permit selection of arbitrary security functions, and define security evaluation levels representing increasing confidence in the ability of a Target of Evaluation (TOE) to meet its security target. TOE refers to a product or system being evaluated. Thus these criteria can be applied to cover a wider range of possible systems and products than the TCSEC.[2]

Although ITSEC does pay more attention to IT system security than TCSEC, the feeling is that ITSEC is not widely accepted enough for international certification purposes.

Gary Hardy [1] states that an ITSEC evaluation assesses the validity of claims made about the security features of a system or product, whereas accreditation measures whether a particular operational information system meets the organization's security objectives. Basically, ITSEC evaluation results could be one of the inputs into the certification process.

The Canadian Trusted Computer Product Evaluation Criteria were developed by the Canadian System Security Centre (CSSC) which addressed issues unique to the Government of Canada.[3]

A common goal shared by most of these security criteria is that by maintaining functionality in the form of integrity, availability, accountability and confidentiality, you can obtain users trust or assurance of the IT security. As can also be noticed, another common goal that they share is their place of origin. They were written by specific countries for their own specific use, and to measure their own specific criteria. For instance one of the purposes of TCSEC is to "Provide DoD Components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information".[7]

The mere fact that there are a number of different information security criteria (eg: ITSEC, TCSEC, CTCPEC, etc) suggests that no consensus has been reached internationally. None of these mentioned sets of criteria is used worldwide. ISO 9000 is recognized and used by 87 countries worldwide. In South Africa close to 1000 companies are already ISO 9000 certified, fourth to the United Kingdom, the United States and Australia. TCSEC, ITSEC and CTCPEC is little known is South Africa, a spokesperson from the South African Bureau of Standards, an ISO 9000 accreditation body, he had never heard of ITSEC or TCSEC.

3.2. Information Security Management Model (ISM^2)

ISM^2 [6], an information security evaluation model, defines five different operational security environments (OSE's), arranged in a particular hierarchy. These are:

- The *Ideal OSE* is an environment as described in the information security policy. It is the ideal environment in which to operate, but not attainable.

- The *Baseline OSE* is the information security goal of the organization. This is the environment that top management has set as a goal and is reachable according to the information security officer.

- The *Prescribed OSE* is an environment as dictated by external parties such as business partners, insurance brokers, etc.

- The *Current OSE* is the current state of security within the information services department.

- The *Survival OSE* is the minimum set of information services and security measures needed to stay operational.

Each of these takes a specific position on a socalled security axis, and Information Security Management is defined as the process of managing these five OSE's "in step". All of these, except the Ideal OSE, are dynamic and will move higher or lower depending on circumstances in the enterprise. [6]

The problem with ISM^2 is that no set of international criteria exists to describe and interpret each level of security for each information security category. This makes it difficult for an organization to compare its information security level with that of another organization.

Neither product and or system certification, as introduced by ITSEC, TCSEC, etc, nor ISM^2 solve the problem of evaluating and ensuring that an organization has protected its IT systems satisfactory. To accredit the information security of an organization, the non-technical measures described by ITSEC [2] need to be addressed. It seems as if ISO 9000 may provide some guidelines in this regard and will be discussed in the next paragraph.

"The number of supplier company quality systems that are registered to ISO 9001, ISO 9002, or ISO 9003 is reported to be 40 000 and increasing daily." [5] This sort of figure supports the authors view that ISO 9000 could well be this "widely accepted body" to form an integral part in IT accreditation.

4. ISO 9000 STANDARDS

4.1. Aim

A principal factor in the performance of an organization is the quality of it's products or services. There is a world-wide trend towards more stringent customer expectations with regards to quality. Accompanying this trend has been a growing realization that continual improvements in quality are often necessary to achieve and sustain good economic performance.

Most organizations produce a product or service intended to satisfy a user's needs or requirements. Such requirements are often incorporated in "specifications". However, technical specifications may not in themselves guarantee that a customer's requirements will be consistently met, if there happen to be any deficiencies in the specifications or in the organizational system to design and produce the product or service. This has led to the development of quality system standards and guidelines that complement relevant product or service requirements given in technical specifications. Information security is definitely a contributing factor to quality and should thus be pulled in under the ISO 9000 umbrella.

The aim of the International Standards Organization's (ISO) ISO 9000 is to provide a comprehensive set of generic standards that apply to all phases of design, development,

production installation and servicing of software and hardware products. They are standards to enforce uniformity of quality systems. They are generic and independent of any specific industry or economic sector. The design and implementation of a quality system will be influenced by the varying needs of an organization, its particular objectives, the products and services supplied, and the processes and specific practices employed.[4]

There is a great thrust for "open systems" in the industry at present. OSI and EDI are growing exponentially in the field of business and financial transaction. OSI and EDI call for standardization, provided by ISO 9000. Many organizations are beginning to insist that their trading partners comply to the ISO 9000 series, in recognition of the quality of the ISO 9000 standards and the benefits that they can deliver. OSI and EDI have brought many information security oriented problems with it. Business partners need "proof" of satisfactory level of information security before EDI transactions are introduced. ISO 9000 certification might just be the long awaited solution in this regard.

4.2. Structure

The International Organization for Standardization's (ISO) ISO 9000 certification standards establish quality processes that have direct and indirect benefits for certified companies, as well as customers and industry. ISO 9000 are for the research, manufacture, testing and support operations involved in producing goods and services.

Usually an external auditor will come in to the organization and lead the ISO 9000 certification process. Once the appropriate ISO 9000 standard has been selected, the criteria accompanying this standard must be fulfilled in detail. Initially the external auditor will have a large role in ensuring all necessary criteria are satisfied.

This is not an overnight process, and could take anywhere from six months to more than two years, depending on the nature of the organization. Once compliance with the selected standard has been accomplished, the organization is officially recognised as an ISO compliant company and certified as such. The certification process is not a once off process, but is repeated annually or more often, sometimes even as often as every four months.

Companies who comply with the ISO 9000 standards must provide documentation for every facet of their production process. ISO 9000 requires large amounts of manpower and paper expense, but companies benefit from the organised procedures and have less product defects. Customers of ISO 9000-certified companies are assured quality services and products and may easily check process documentation for the new manufacturing procedures, design changes or product upgrades. If ISO 9000 certification can be used for quality assurance, why not for information security? Information security contributes to quality.

5. INFORMATION SECURITY ISSUES ADDRESSED IN ISO 9000

ISO is developing a collection of standards for software processes called Software Process Improvement and Capability Determination (SPICE). These standards support ISO 9000 quality standards, and will help the software processes by making sure the processes are aware of business goals of the organization. By bettering the software engineering process, many problems facing the IT personnel of today can be resolved.

ISO 9000 was not developed initially with software development in mind. ISO 9000-3 is a set of guidelines developed that relate directly to software preparation, but that on its own

is still not the ideal in terms of information security.

Using the ISO 9000 standards, a lot of possible security problems could be "resolved" by various interpretations of the wording in the standards. However, IT terminology is specific and should not have to be "revised" in order to fit into a specific category. No specific standard in the ISO 9000 series directly address IT security and all the relevant aspects discussed up to now.

6. ISO 9000 STANDARDS AND INFORMATION SECURITY CERTIFICATION

The demand for information security certification has been identified a long time ago, especially where organizations interconnect with one another's information systems. This demand for certification is closely linked to an underlying requirement for standards defining minimum acceptable IT security requirements. These standards must allow the certification process to be straightforward, credible, affordable and achievable. Companies will be driven towards certification due to peer pressure (from distributors and suppliers) and competitive market forces.

The above mentioned facts all relate to a standard such as ISO 9000. There are actually five ISO 9000 Series international standards: ISO 9000 is the master guide, ISO 9001 covers design, manufacturing, installation and service, ISO 9002 covers production and installation, ISO 9003 covers final product inspection and test, and the ISO 9004 helps in the development of internal quality systems that comply with ISO 9000. ISO 9000 is readily acceptable just about all over the world, and compliance is not an 'impossible' task. It usually involves a couple of consultants, an external auditor, a sum of money, a number of months (anywhere from six to more than twenty four), and you are there - ISO 9000 certified. Most organizations supporting ISO 9000 also insist that their trading and business partners are also ISO 9000 compliant.

The growing acceptability of ISO 9000 standards is what make it creditable for IT security certification. The only problem, and the problem that this paper serves to solve, is that the ISO 9000 standards don't cater for information security specifically, or not nearly as well enough for complete accreditation purposes. The bottom line is:
ISO 9000 provides a comprehensive set of generic standards that apply to all phases of design, development, production, installation and servicing of software and hardware products. These standards are generic and independent of any specific industry or economic sector. These standards can be used with great effect in introducing and managing information security in an organization and an internationally accepted body (ISO) can put their stamp on it.

Although the ISO 9000 standards do not cater completely for information security certification currently, a limited form of information security certification can already be accomplished using ISO 9000 in its current form.

Four important aspects of information security management; namely, 1) the information security policy, 2) risk analysis, 3) contingency planning and 4) logical access control, are addressed indirectly. In each case the way in which the mentioned information security aspect is introduced, conducted and managed within the organization can be 'measured' and probably certified for compliance to ISO 9000 standards.

ISO 9000 states:

The supplier's management with executive responsibility shall define and document its policy for quality, including objectives for quality and its commitment to quality. The quality policy shall be relevant to the suppliers organizational goals and the expectations and needs of its customers. The supplier shall ensure that this policy is understood, implemented and maintained at all levels of the organization. [9]

ISO 9000 forces the organization and its top management to put their policy regarding quality on paper and to adhere to it. If the details of the **information security policy** could be incorporated into this document, then the importance if information security could receive a lot more attention and top management will be forced to get involved in information security.

ISO 9000 states further:

In order to meet its objectives, the organisation should ensure that the technical, administrative and human factors affecting the quality of its products will be under control, whether hardware, software, processed materials or services. [8]

ISO 9000 forces the organization identify control measures that ensure that quality of products are maintained. This could be related to some sort of **risk analysis**, where all risks affecting the information systems of the organization are identified.

The responsibility, authority and interrelation of personnel who manage, perform and verify work affecting quality shall be defined and documented. [9]

This goes on to identify non-conformities and problems that may affect the product, and to provide solutions to the problems, as well as ensuring that the solutions are implemented. This relates not only to risk analysis, by identifying possible risks, but also to **contingency planning**, by ensuring that solutions are on hand and implemented. This relate directly to the product, and information security is not the main issue here.

Documented procedures may make reference to work instructions that define how an activity is performed. [9]

Well documented contingency plans will ensure that recovery from a disturbance is established and orderly. The introduction and effective management of passwords as used in **logical access control** can also be included under this point.

Other related aspects addressed by ISO 9000:

The supplier's management with executive responsibility shall appoint a member of the supplier's own management who, irrespective of other responsibilities, shall have defined authority for,

- *ensuring that a quality system is established, implemented and maintained in accordance with this International Standard, and*
- *reporting on the performance of the quality system to the supplier's management for review and as a basis for improvement of the quality system. [9]*

This could relate to the whole information system of the organization, ensuring that performance is optimal and that new and improved ideas are always been sought.

The supplier shall establish, document and maintain a quality system as a means of ensuring that the product conforms to specified requirements. [9]

Once again, in context of the whole computer system, by maintaining a "quality information system", one can be assured that the requirements imposed on the system have a good chance of been met.

The supplier shall establish and maintain documented procedures for inspection and testing activities in order to verify that the specific requirements for the product are met. [10]

This could refer to tests on the safety equipment to ensure that they work correctly (ie. fire

extinguishers), as well as tests to ensure that access control security on the database is working and correct.

The supplier will establish and maintain documented procedures for implementing corrective and preventive action. Any corrective and preventive action taken to eliminate the causes of actual or potential non-conformities shall be to a degree appropriate to the magnitude of problems and commensurate with the risks encountered. [12]

Risk analysis, contingency planning, disaster recovery, all could be included under this paragraph. Determine the risks to the organization, protect the organizations against these risks, and have procedures to recover from disasters. The main issue here is that these documents and procedures are not static, and need to be updated constantly.

For the organization, consideration has to be given to risks related to deficient products which lead to loss of image or reputation, loss of market, complaints, claims, liability and waste of human and financial resources. [9]

By identifying risks, and planning for them, the organisation will be able to assess the effects of the potential damage, and be prepared for it.

As seen from the extractions from ISO 9000, many information security issues are already covered by ISO 9000. In fact, clause 2.2.1b in ISO 9000-3 stating: "Each contract should be reviewed by the supplier to ensure that possible contingencies or risks are identified." can hardly be satisfied without conducting an risk analysis exercise. Many other such clauses call for a disaster recovery plan to be in place, information protection, risk management, data control, etc.

The fact remains, to obtain an ISO 9001 listing requires many information security management issues. Information security as a whole is not addressed.

7. SHORTCOMINGS IN ISO 9000

As mentioned before, the feeling exists that information security management is not given enough detailed attention in ISO 9000. The management and security of information in any company is essential to the successful operation of the organization. The ISO 9000 standards cater quite adequately under the banner "quality management systems", but fall short in the area "information security management". Its all well and fine to have good quality products emerge from your company, but if company information is lost or damaged, then the organization will not get as far as the production process, and quality will suffer.

As seen in the previous section, a lot of information security criteria can be handled in ISO 9000, but nothing is really handled directly, information security is addressed indirectly, but not directly. You have to manipulate the wording of certain sentences in order to allow information security to take the place of product quality, and this in not acceptable. Remember, software development was not covered initially under ISO 9000, but an additional set of guidelines, i.e. ISO 9000-3, was added to solve the problem. The authors would like to maybe even go as far as to have a set of guidelines prepared to interpret information security, maybe ISO 9000-5. This will ensure that, in obtaining an ISO 9001 certification, emphasis was placed thoroughly on information security. If this route is followed, information security per se will not be addressed, still quality assurance with more emphasis on security. ISO/IEC JTC1 SC7 has been busy for several years now and is now starting to release its first international standards for software quality and software engineering. If information security per se need to be certified, this group may create a specific topic for information security.

As stated earlier, information security will more than likely be unique for each organization, which would make it difficult to fully compare or understand the actual details of an organizations information security procedures. However, ISO 9000 sets out guidelines for enforcing *uniformity* of quality systems, and does not necessary stipulate how the actions under these guidelines are to be performed.

8. SUMMARY

The survival of an organization is dependant on its quality of service provided or the quality of product delivered. In either case, information security is crucial to the well being of the organization. International security standards will allow information security accreditation to take place on a corporate wide scale, enabling all related parties to "feel safe" about their relationships with others.

ISO 9000 is an internationally accepted standard, and by inserting specific, well laid out information security standards in ISO 9000, you will be assured of an internationally accepted form of accreditation that will not take an endless amount of time to produce a result. The end result would resemble a cumulation of the ideas and advantages expressed in ITSEC, TCSEC, CTCPEC and ISM^2, while eliminating the disadvantages mentioned with regards these standards.

REFERENCES

[1] Hardy, G., "Commercial Accreditation Of Information Security", Computers & Security, Vol 12, No 8, 1993.

[2] Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, Information Security Centre Research Centre, Research Collection, June 1991.

[3] The Canadian Trusted Computer Product evaluation Criteria, Canadian System Security Centre, Communications Security Establishment, Government of Canada, Ver 3.0e, April 1992.

[4] South African Bureau Of Standards, "A Comparison Between SABS ISO 9001 : 1987 and ISO/DIS 9001.2 : 1994".

[5] Durand I.G et al, "Updating The ISO 9000 Standards : Responding To Market Needs", Quality Progress, July 1993.

[6] Von Solms et al, Information And Management, "A Framework For Information Security Evaluation", Information And Management No. 26 (1994) Pages 143-153.

[7] Computer Control Quarterly, "Trusted Systems - White Book Versus Orange Book", Vol9, No 2, 1991.

[8] ISO 9001: 1994, Quality Management And Quality Assurance Standards - Part 1: Guidelines For Selection And Use.

[9] ISO 9001: 1994, Quality Systems - Model For Quality Assurance in Design, Development Production, Installation And Servicing.

[10] ISO 9002: 1994, Quality Systems - Model For Quality Assurance in Production, Installation And Servicing.
[11] ISO 9003: 1994, Quality Systems - Model For Quality Assurance in Final Inspection And Testing.
[12] ISO 9004: 1994, Quality Management And Quality System Elements.