A COMPARATIVE STUDY OF STANDARDS AND PRACTICES RELATED TO INFORMATION SECURITY MANAGEMENT

Evangelos D. Frangopoulos [1,*] and Mariki M. Eloff [2,]**

1 Electrical Engineer (M.Sc.) / Postgraduate Student, Dept. of Computer Science and Information Systems, UNISA.

2 Associate Professor, Department of Computer Science and Information Systems, UNISA.

[*] 40B, Mohamed Mazhar, Zamalek, Cairo, Egypt. Tel.: +20 10 639-6819.
eMail: vfrangopoulos@hol.gr

[**] 8-100 Theo van Wijk Building, UNISA, Muckleneuk Pretoria, South Africa.
Tel.: +27 12 429-6336. eMail: eloffmm@unisa.ac.za

ABSTRACT

The need for Information Security in organisations, regardless of their type and size, is being addressed by emerging standards and recommended best practices. The various standards and practices which evolved in recent years and are still being developed and constantly revised, address the issue of Information Security from different angles. Some of these have gained world-wide recognition through adoption by international standards' organisations, while others base their wide level of acceptance on the reputation of the bodies responsible for their compilation.

This paper attempts to provide an overview of Information Security Standards and Practices by briefly discussing some of the most popular ones. Through a comparative study their similarities and differences are shown and, thus, some insight can be obtained on how their combination may lead to an increased level of Information Security.

KEY WORDS

information security management, information security standard, ISO 17799, BS 7799, ISO 15408, Common Criteria, CERT, , GASSP, GAISP.

A COMPARATIVE STUDY OF STANDARDS AND PRACTICES RELATED TO INFORMATION SECURITY MANAGEMENT

1 INTRODUCTION

The issue of Information Security within an organisation is very broad and is definitely not limited to IT security. At present, there is an ongoing effort towards the standardisation of practices and processes in order to ensure a high level of security with respect to all forms of information handled within an organisation's scope of operation. Furthermore, it is only recently that standards dealing with the issue of security auditing and certification beyond the limits of IT security, began to emerge and gain broad acceptance.

The fairly recent introduction of ISO 17799 [ISO17799], a standard addressing the broader spectrum of Information Security threats within an organisation, provides a comprehensive set of directions/practices to ensure a high degree of security.

In this document, an attempt will be made to carry out a brief comparative study of various security standards/sets of practices against ISO 17799. The goal of this exercise is to identify how other standards and practices relate to ISO 17799 and provide some insight on whether the recommended practices of ISO 17799 can be further enhanced by elements of the other documents.

The remainder of this paper is structured as follows: Section 2 gives a brief overview of ISO17799, followed by brief discussions of the Common Criteria, CERT Security Practices and GASSP/GAISP in Section 3. Section 4 contains the comparison between the different standards and practices, followed by a conclusion.

2 GENERAL COMMENTS ABOUT THE ISO 17799 "CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT".

ISO 17799 resulted from the British Standards Institution's (BSI) BS7799 code of practice, which was introduced in 1995 and revised in 1999. Part 1 of BS7799 became ISO standard 17799 in 2000 after being adopted by Joint Technical Committee ISO/IEC JTC 1 – Information Technology. During its transformation to an international standard, all elements of BS7799-1 specific to British law were removed. Part 2 of BS7799 "Information security management systems - Specification with guidance for use" has not yet been adopted by ISO as such, but has been accepted by many national standards' organisations, among which the South African National Standards (SANS) organisation. It must also be clarified that the initial BS7799-2 document of 1999 was thoroughly revised in 2002 and became BS7799-2:2002 [BS7799-2]. It is the 2002 revision of BS7799-2 that will be referred to in this document.

ISO 17799, contrary to other security standards or proposed practices for IT systems, does not only cover IT security. It attempts to identify vulnerabilities and suggest controls for the security of information, irrespective of the form, method of handling and level of this information within an organisation.

ISO 17799 forms an invaluable tool in identifying possible areas of vulnerabilities throughout any corporate structure. It does so by providing guidelines for the establishment of security requirements, the assessment of security risks and the selection of controls for identified vulnerabilities. However, ISO 17799 can definitely not function as a technology guideline because it does not provide practical solutions to security-related problems of a technical nature.

ISO 17799 attempts to be as broad as possible. This is probably the result of a strategy to guarantee ISO 17799's wide acceptance. In this sense, small and medium enterprises may decide to deal with a subset of controls instead of considering the full list. It is interesting to note the number of commercial packages emerging which are presumed compatible to ISO 17799 and claim to provide for and support all security issues addressed in ISO 17799. This trend also verifies the degree of acceptance of the standard.

ISO 17799 is self-described as "*a starting point for developing organisation specific guidance*". This signifies the fact that ISO 17799 is not self-sufficient in providing for a total security solution. Consequently, the need for additional guidance in the form of a technical standard is highlighted.

Finally, ISO 17799 addresses 10 major topics in terms of policies and general good practices.

These are:

1. Security policy
2. Organisational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance.

3 STANDARDS/PRACTICES FOR COMPARISON TO ISO 17799/BS7799-2.

The choice of sets of recommended best practices and standards for comparison to ISO 17799/BS7799-2, was based on the level of acceptance of these sets by the comp uter society.

These are:

- ISO 15408 / Common Criteria
- CERT Security Practices
- GASSP/GAISP

3.1 ISO 15408 / Common Criteria

Given that ISO 17799/BS7799-2 was never meant to be a technical standard, in the sense that it does not relate the particularities of various technologies to the security requirements it addresses, other standards need to come in and fill the void.

One such Standard is the tri-partite ISO 15408 [CC-1],[CC-2],[CC-3] “Evaluation criteria for information technology security”, also known as "Common Criteria for Information Technology Security Evaluation". ISO 15408 was produced by a consortium of North American and European Union government bodies. It effectively evolved from, encompassed and replaced ITSEC in Europe, US’s Federal Criteria, known as “Orange Book”, as well as the Canadian Criteria. It has also been accepted as a working standard by many other countries including Russia, Japan and Australia. ISO 15408’s adoption is yet another step in the ongoing effort to align local and national IT security standards and practices to a standard with worldwide acceptance.

ISO 15408 presents a lot of principal differences when compared to ISO 17799/BS7799-2, especially since it does not address the whole IT structure but is rather focused on the technical aspect of computer systems involved in the handling and processing of information. However, due to its worldwide acceptance it is deemed necessary to be included in this comparative study.

Combined use of the two standards where, perhaps, non-IT security controls are handled by ISO 17799/BS7799-2 while security requirements of the individual system components be evaluated according to ISO 15408, may provide the “best of both worlds” in designing and evaluating a system for security.

3.2 CERT Security Practices

The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University (www.cert.org).

Among other activities, CERT provides technical advice and coordinates responses to security compromises, works with other security experts to identify solutions to security problems, and disseminates relevent information to the broader community. One method of such dissemination is the compilation of the “CERT Security Improvement Modules” based on a collection of “Computer Network Security Practices” [CERT]. All this information is freely available on the Internet.

These Modules and Practices address in a concise and quite detailed manner a comprehensive set of issues related to IT security. The described practices have gained acceptance among the Network Administrators’ Community because they systematically address common security problems. A set of implementations for particular operating systems is also provided, although this set, is, at present, dated, if not obsolete.

The CERT Security Practices only address issues relating to the security of Networked computers. They do not address all aspects of information handling within an organisation as the ISO 17799 recommendations do. However, being one of the prominent set of practices in the field, there is merit in their comparison to the ISO 17799.

3.3 Generally Accepted System/Information Security Principles (GASSP / GAISP)

The GASSP committee was formed in 1992. This committee was sponsored by the International Information Security Foundation. The committee's objective was to "promulgate comprehensive generally accepted system security principles". The committee's international composition constitutes a key factor of the level of international acceptance of the proposed principles.

Although an extended background/history of the GASSP is beyond the scope of this document, it has to be noted that version 1 of GASSP was published in 1997 and version 2 in 1999 [GASSP]. Version 2 covered two out of the projected three core parts of the document, namely the Pervasive Principles section and the Broad Functional Principles. The third part, that of the Detailed Security Principles was not included in GASSP ver. 2. After a 4-year near-dormancy period, the work of the GASSP committee was taken over by the Information Systems Security Association (www.issa.org) and the new name for the set of principles became "Generally Accepted Information Security Principles" or GAISP. GAISP takes over from the point where GAASP left off. Thus, the two sections on Pervasive Principles and Broad Functional Principles will remain at their present status, while, according to GASSP committee chairperson, Mr. Will Ozier who was contacted in early December 2003, "work on drafting the Detailed Security Principles is about to get under way". Hence, the validity of GASSP ver. 2 is not at all compromised and still provides significant insight in the area of Information Security.

GASSP is not a technical document. Furthermore, it does deal with the complete picture of information security in an organisation, not just with the IT aspect of it. In this sense it shares a lot in character with the ISO 17799 standard, and this is why it is included in this comparative study.

4 COMPARATIVE STUDY OF SELECTED STANDARDS/PRACTICES AND ISO 17799 / BS7799-2

The selected standards/practices will be compared against ISO 17799/BS7799-2. ISO 17799 being the broader of all standards/practices under examination, it can provide a good reference for comparison.

4.1 ISO 15408:1999 / Common Criteria v. 2.1

For reasons of simplicity, "7799" will be used in this section of the document to describe both ISO/IEC 17799:2000 and BS7799-2:2002. Where necessary, the distinction between the two will be explicitly made. "CC" will be used as a shorthand notation to denote the ISO 15408/Common Criteria standard.

As a general comment about the relative qualities of the two documents, it must be pointed out that CC, being more technical than 7799, is a lot more difficult to follow by those who are not actively involved in the technical aspect of the organisation's security project. It must also be stressed that the terminology and notions used in the two documents are far from being identical. On the contrary, there exist many cases where identical terms are used to convey different ideas

As it has already been stressed, 7799 deals with the notion of a **System** in terms of the complete environment of an organisation within which information is handled. This includes document handling, building (and location in general) issues and all types of assets within the organisation in addition to its traditionally defined IT systems. On the contrary, CC practically deals only with the narrower notion of an IT system. In CC–Part1 [CC-1], section 2 "Definitions", a System is defined as *"a specific IT installation, with a particular purpose and operational environment"*. I.e. in this context, a System is limited to a particular IT installation within clearly defined bounds.

In the same context as above, as far as the concept of **Information Security Management** is concerned, in section 3.4 of BS7799-2, the definition of an information security management system (ISMS) begins with: *"(the ISMS is) that part of the overall management system, based on a business risk approach…"*. Thus, clearly, in BS779-2, Security Management again refers to the complete organisation environment and every aspect of information handling within the organisation. On the other hand, according to CC-part 2 [CC-2], section 8, Security Management is one of many Functional Requirement Classes which deals with the secure operation of a particular IT System (according to the CC definition of the term). Thus, CC's scope is limited in comparison to that of 7799.

The idea of **evaluation and certification** also differs between 7799 and CC. The complete definition of the ISMS in BS7799-2 is that it constitutes *"part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"*. The second part of the ISMS definition, makes it clear that an ISMS is, by default, of a dynamic nature. This notion of continual re-evaluation is one of the key aspects of BS7799-2. Every one of the document's principal sections (sections 4,5,6,and 7) begins by re-stating in one way or another this principle of improvement of Information Security through iteration.

For the above purpose, the Plan-Do-Check-Act (or PDCA) model is introduced, according to which a virtuous circle of continual improvement of the ISMS is established. According to BS7799-2, it is, thus, assumed that changes in the organisation's environment occur continually and as a consequence, a monitoring system must be established. The core function of this system (the system being the ISMS) is to make new risk assessment, identification of new vulnerabilities and implementation of new controls, as automated a process as possible. Hence, one of the main characteristics of the ISMS is that it is "free running". It does not rely on a triggering event of some sort to begin the re-evaluation procedure. It must be stressed, however, that it is only in BS7799-2 that this notion of continual change is introduced and hence the need for an ISMS.

In ISO 17799, section 3.1.2, it is stated that *"The policy should have an owner who is responsible for its maintenance and review according to a defined review process. That process should ensure that a review takes place in response to any changes affecting the basis of the original risk assessment…"*. Hence, ISO 17799 has no provision for continual re-evaluation. It is the certification against BS7799-2 that requires a pre-existing, properly functioning ISMS. In the case of certification against CC, this is not so either. Given the relatively limited scope of CC and the clearly-bounded IT systems it is applied on, it is assumed that once an IT system has been evaluated and certified as compliant to CC, it stays so until a change is made to it. This assumed "static" nature of IT systems is made clear in section 4.5 of CC – part 1. The idea of Assurance Maintenance is introduced in section 4.6 of the same document. According to this, Assurance Maintenance *"is carried out against the* *evaluation criteria contained in Part 3 (of ISO 15408) using a previously evaluated Target of Evaluation (TOE) as the basis. The goal is to derive confidence that assurance already established in a TOE is maintained and that the TOE will continue to meet its security requirements as changes are made to the TOE or its environment*". In practice, the changes referred to in this definition, must be somehow identified. This identification will function as the trigger event for the relevent Maintenance Assurance procedures to be called upon and the re-evaluation of the TOE to begin. However, with the lack of an ISMS, the identification of changes is not systematic, and without sufficient alternative identification procedures, a change that could lead to the compromise of Information Security may go unnoticed for indeterminate periods of time with detrimental effects.

The manner in which the notion of **risk** is grasped in the two documents justifies the general approach to evaluation and certification discussed above: in BS7799-2 risk has a dynamic quality. It is never assumed constant. It is, by default, assumed to be changing with time (hence the need for the existence of an ISMS). In CC, on the other hand, the risk involved in a system, is assumed static as long as the system does not undergo any changes or until new threats and vulnerabilities emerge.

The differences described above clearly mirror the **disparities in the mentality** of the two documents. 7799 is a mainly conceptual document, while CC is technical standard. 7799 is a tool in the hands of an organisation's Management that helps achieve a higher degree of overall information security. Software products and equipment that are certified against CC to certain functional and security requirements can be used as building blocks and relied upon for further 7799 implementation and certification. The information security controls called upon by 7799 will have to -at one point or another- imply usage of CC-certified equipment or implementation of Information Security guidelines and concepts such as those described by CERT, NIST, GASSP and others.

This brings forward another major distinction between 7799 and CC: In the "Scope" section (section 1) of ISO 17799 it is clearly stated that "*This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization*" –hence the **responsibility for security** lies within the organisation. In the case of CC, in part 1, section 3.2.1 "Consumers", it is stated that "*The CC plays an important role in supporting techniques for consumer selection of IT security requirements to express their organisational needs*". Also in CC-part 1, section 3.2.2. "Developers" it states "*The CC is intended to support developers in preparing for and assisting in the evaluation of their products or systems and in identifying security requirements to be satisfied by each of their products or systems*". Clearly, these two statements show that in CC the responsibility for security lies with the developer of the systems under evaluation.

Furthermore, regarding the **evaluation phase in the life cycle of a system**, in CC it is implied that evaluation is part of the design and development of the system. The whole CC approach does not seem applicable to pre-existing systems. It rather applies to a system while that is still in its construction phase. 7799 has no such limitation. On the contrary, certification of a system against BS7799-2 assumes an existing system where new controls are applied and constantly re-evaluated and improved.

Despite these discrepancies, it is without doubt that any policy which is based on 7799, can be further strengthened by the inclusion of elements from CC. CC being geared towards the "pure" IT aspect of the security requirements, it can help resolve security issues that would otherwise be left "hazy" at best.

During the definition of the security policy according to ISO 17799 and/or the definition of the ISMS policy according to BS7799-2, organisational security policies that apply to the system can be identified according to CC-part1, section 4.3. These will form an integral part of the subsequent risk analysis also.

Furthermore, during the control selection phase of the project, the security functional requirements pertaining to IT components and the relevant controls can be identified according to CC-part2.

Finally, if an evaluation phase according to BS7799-2 is in order, this process can be enhanced with respect to the IT aspect of the project, by defining supplemental security assurance components, based on CC-part3 [CC-3].

4.2 CERT Computer System and Network Practices

The CERT Coordination Center has compiled a set of recommended "Best Practices" for the Improvement of Security in a Computer Network System [CERT].

These practices cover a wide range of computer network-related security issues, bearing in mind the Internet-oriented nature of the CERT CC. However, since, today, most, if not all, of the computers found in an organisation are of the networked type, these recommendations have a broader application field than one might initially assume.

The set of approximately 60+ recommended security practices is subdivided in six groups, each group focusing on one aspect of IT security as it applies to networks. The practices are grouped under the following headings:

A. Practices about hardening and securing systems

B. Practices about preparing to detect and respond to intrusions

C. Practices about detecting intrusions

D. Practices about responding to intrusions

E. Practices about improving system security

F. Practices related to outsourcing managed security services

Judging from the group titles, there is no clear alignment (if any at all) between the CERT practices and the ISO 17799 proposed controls. On closer inspection of the particular CERT practices, though, it is easily seen that there is a lot of common ground covered by both documents.

On further study, it becomes self-evident that, with respect to the two documents' common issues, the combination of CERT practices or elements thereof, with the ISO 17799 controls and recommendations, will yield a higher degree of security than that which would be achievable by stand-alone application of either document's directives.

In an effort to align the two documents, an attempt will be made to relate the CERT practices to the ISO 17799 recommendations. Since the CERT practices do not form part of a standard, they may change without notice. Hence, a listing was made according to the grouping of practices as it appeared on the CERT website at the end of 2003. This list is presented in Annex A of this document and the reader is urged to refer to it for the sake of clarity.

As it has already been stated, apart from dealing with the IT aspect of security, the CERT practices are heavily internet-oriented in many respects. As expected, there are many areas where there is no overlap between the CERT practices and ISO 17799. The ISO 17799 topics that are **not covered** by related sections of the CERT practices are those of:

- Security policy (section 3 of ISO 17799)
- Asset classification and control (section 5)
- Business continuity management (section 11)

and

- Compliance (section 12)

Also,

- Systems development and maintenance (section 10)

is not covered in detail in any of the CERT recommendations, although general notions and ideas presented in the CERT document can definitely apply to the principles discussed in that section.

These topics set aside, the relation of the remaining ISO 17799 topics to the CERT practices, was examined and the results of the standards' comparison are summarised in table 1.

4.3 GASSP / GAISP

Although the GASSP project was recently taken over by the Information Systems Security Association (www.issa.org) and was renamed into GAISP, the definitive document still is GASSP ver.2. In short, it will be referred to as GASSP, for the remainder of this document.

GASSP currently comprises two main sections: A) Pervasive Principles and b) Broad Functional Principles. The Pervasive Principles *“provide general guidance to establish and maintain the security of information*”. The Pervasive principles form the basis of both the Broad Functional Principles that are also discussed in v.2.0 of the GASSP as well as the Detailed Principles which are being drafted.

From a qualitative point of view, all principles are presented in a three-part format. In the first part, a concise definitive statement is given for the principle. In the second part, rationale, the principle s discussed in greater detail and the underlying logic examined. In the third part, a practical example is used to drive home the principle’s central points. This makes the GASSP document very “marketable” with any organisation’s administration and guarantees the wide level of its acceptance

GASSP and ISO 17799 share two common characteristics: a) neither is a technical document, b) both deal with the complete picture of information security within the bounds of an organisation, i.e. they are not limited to the IT aspect of it.

The terminology of the two documents is quite similar and this makes their comparison easier. The results of the comparison of the two standards are summarised in table 1.

4.4 Comparison data of ISO17799, CERT Practices and GASSP/GAISP

In an effort to provide a quick overview of the relation between three of the standards examined in this document (namely ISO17799, the CERT Practices and GASSP/GAISP), the following table is given. ISO 15408/CC deals with different aspects of Information Security when compared to the three mentioned standards and its content is not in direct correspondence to that of the other standards. Thus, CC can not be included in the tabulation.

Table 1. Comparison of Standards

ISO17799	CERT	GASSP
3. Security policy	Not covered	BFP 2.2.1
3.1 Information security policy	Not covered	BFP 2.2.1
4. Security organisation	Limited overall coverage	Limited coverage
4.1 Information security infrastructure	Limited coverage, Practice no. 13	Accountability Principle (sec.2.1.1), Multidisciplinary Principle (sec.2.1.4)
4.2 Security of third party access	Elements found in Practice no. 56	Not covered
4.3 Outsourcing	Elements found in Practice no. 56	Not covered
5. Asset classification and control	Not covered	BFP 2.2.4
5.1 Accountability for assets	Not covered	Accountability Principle (sec.2.1.1)
5.2 Information classification	Not covered	BFP 2.2.4
6. Personnel security	Some aspects covered in varying depth	Partial coverage in 2.1.2, 2.2.2 and 2.2.6
6.1 Security in job definition and resourcing	Practically no coverage	BFP 2.2.6
6.2 User training	Limited coverage in Practice no.13	Awareness Principle (sec.2.1.2), BFP 2.2.2
6.3 Responding to security incidents and malfunctions	Covered in detail in practices no. 33, 44, 45, 52, 53 and 54	Timeliness Principle (sec.2.1.7)
7. Physical and environmental security	Several issues covered	Not covered
7.1 Secure areas	Issue covered in Practice no. 10 but not in practical terms	Not covered
7.2 Equipment security	Various aspects covered in Practice no. 42	Some alignment with BFP 2.2.7
7.3 General controls	Various aspects covered in Practice no. 42	Not covered
8. Communications and operations management	Coverage of many, but not all, issues	Not covered
8.1 Operational procedures and responsibilities	Limited coverage, Practices 55-62	Not covered
8.2 System planning and acceptance	Not covered	Some alignment with BFP 2.2.7
8.3 Protection against malicious software	Practice no. 8	Some alignment with BFP 2.2.7
8.4 Housekeeping	Value-adding discussion in practices no. 1, 7, 12 and 21	Not covered

8.5 Network management	In-depth discussion in many practices, such as nos. 1, 2, 4, 11, 14, 16 and 23-32	Some alignment with BFP 2.2.7, Some common elements with BFP 2.2.12
8.6 Media handling and security	Not covered	Not covered
8.7 Exchanges of information and software	Some insight can be found in Practices no. 15, 18, 20, 21 and 22	Not covered
9. Access control	Covered in CERT but not as systematically	Some coverage in BFP 2.2.9
9.1 Business requirements for access control	Significan portion covered in Practice no. 1	Partial alignment to BFP 2.2.9
9.2 User access management	Elements covered in Practice no. 5	Not covered in detail
9.3 User responsibilities	Elements covered in Practice no. 5	Not covered in detail
9.4 Network access control	In-depth discussion in many practices, such as nos. 1, 2, 4, 11, 14, 16 and 23-32	Some common elements with BFP 2.2.12
9.5 Operating system access control	Elements covered in Practice no. 5	Partial alignment to BFP 2.2.9
9.6 Application access control	Elements covered in Practice no. 6	Partial alignment to BFP 2.2.9
9.7 Monitoring system access and use	Covered in Practices no 9, 17, 33 to 35, 39 and 40	BFP 2.2.3
9.8 Mobile computing and teleworking	Not covered	Some common elements with BFP 2.2.12
10. Systems development and maintenance	No detailed coverage – general notions present	Partial coverage
10.1 Security requirements of systems	No detailed coverage	Some elements covered in BFP2.2.7
10.2 Security in application systems	No detailed coverage	Not covered
10.3 Cryptographic controls	No detailed coverage	Not covered
10.4 Security of system files	No detailed coverage	Not covered
10.5 Security in development and support processes	Not covered	BFP 2.2.8
11. Business continuity management	Not covered	BFP 2.2.5, BFP 2.2.10
11.1 Aspects of business continuity management	Not covered	Not covered
12. Compliance	Not covered	Partial coverage
12.1 Compliance with legal requirements	Not covered	Ethics Principle (sec.2.1.3), BFP 2.2.13
12.2 Reviews of security policy and technical compliance	Not covered	Assessment Principle (sec.2.1.8)
12.3 System audit considerations	Not covered	Not Covered

As it can be seen from the tabulated data, there are many areas of ISO 17799 that are not addressed by either the CERT Practices or GASSP/GAISP. For GASSP/GAISP this is most probably the case because the relevant work has paused at the Broad Functional Principle level and controls are expected to appear in the finished “Detailed Principles” section (currently being drafted). A completed list of Detailed Principles will presumably have more issues in common to ISO 17799. As far as the CERT recommended practices are concerned, their scope is definitely more narrow than the scope of ISO 17799 and geared towards the practical side of applying controls to the IT aspect of a business. As such they can not be expected to cater for the organisational and managerial aspects of information security.

5 CONCLUSION

This comparative study has shown that all four of the examined documents approach the issue of security from different angles and with different mentalities.

ISO 17799 and BS7799-2 attempt to provide a total solution for Information Security, reaching a practical level of implementation in the form of controls. ISO15408 (CC) deals only with the IT aspect of information security and it does so in a very formalised and detailed manner. The CERT practices are guidelines for any and all parties interested in increasing the level of security of their computer systems and networks, but they do not deal with all aspects of information security. Finally, the GASSP / GAISP, have not yet reached the level of proposing controls, but the principles they are based upon, are clearly aligned with the directives and overall information security mentality of ISO 17799/BS7799-2.

It is concluded that a policy implementation which is based on the ISO 17799/BS7799-2 directives can be further (and in certain areas significantly) enhanced by elements taken from all three other standards/sets of practices.

For an Information Security Management System implementation to be truly effective, one should be able to objectively measure its compliance to the directives and principles by which it is designed. The issue of security compliance and measuring still remains open and a great amount of research effort is expected to be directed in this area.

6 BIBLIOGRAPHY

[BS7799-2] SOUTH AFRICAN NATIONAL STANDARD, 2003, *SANS 17799-2:2003, Information security management systems - Part 2: Specification with guidance for use.* Edition 2. Pretoria: Standards South Africa.

[CC-1] INTERNATIONAL STANDARD, 1999, *ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.* Geneva: ISO/IEC.

[CC-2] INTERNATIONAL STANDARD, 1999, *ISO/IEC 15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements.* Geneva: ISO/IEC.

[CC-3] INTERNATIONAL STANDARD, 1999, *ISO/IEC 15408-3, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements.* Geneva: ISO/IEC.

[CERT] CERT, *Security Improvement Modules*. Available on the Internet at: http://www.cert.org/security-improvement/index.html , last accessed on December 18, 2003.

[GASSP] INTERNATIONAL INFORMATION SECURITY FOUNDATION (I^{2}SF),1999, *Generally Accepted System Security Principles*, version 2.0. Available on the Internet at: http://web.mit.edu/security/www/GASSP/GASSP.ZIP, last accessed on 18.11.03

[ISO17799] SOUTH AFRICAN STANDARD, 2000, *SABS ISO/IEC 17799, Information technology — Code of practice for information security management*. SABS edition 1/ISO/IEC edition 1 2000. Pretoria: South African Bureau of Standards.

[PFL00] PFLEEGER, Charles P. 1997, *Security in Computing*. Reprinted with corrections February, 2000. New Jersey: Prentice-Hall.

General References

BRODERICK, S. 2002, A Definitive Introduction to Information Security Policies, Standards and Procedures (parts 1 to 4), in *Symantec Security Expert Series*. Accessed on 19/10/03
Part 1: http://ses.symantec.com/article.cfm?articleid=1155&EID=0
Part 2: http://ses.symantec.com/article.cfm?articleid=1165&EID=0
Part 3: http://ses.symantec.com/article.cfm?articleid=1179&EID=0
Part 4: http://ses.symantec.com/article.cfm?articleid=1193&EID=0

CARLSON, T. 2001, Information Security Management: Understanding ISO 17799. Accessed on 16/8/03
http://www.ins.com/downloads/whitepapers/ins_white_paper_info_security_iso_17799_1101.pdf

HMSO, 1998, Data Protection Act 1998. Accessed on 16/9/03
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

JARVIS, R. ISO 17799 And The UK Data Protection Act 1998. Accessed on 16/9/03
http://www.iso17799software.com/7799-dpa.htm

NIST, 2002, International Standard ISO/IEC 17799:2000 Code of Practice
for Information Security Management: Frequently Asked Questions. Accessed on 16/9/03. http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

PATRICK, W. 2001, Creating an Information Systems Security Policy. Accessed on 9/10/03. http://www.sans.org/rr/papers/index.php?id=534

SYMANTEC, 2002, Building Effective Security Policies. Accessed on 19/10/03
http://ses.symantec.com/article.cfm?articleid=1128&EID=0

SYMANTEC, 2001, E-Security Begins with Sound Security Policies. Accessed on 19/10/03
http://enterprisesecurity.symantec.com/SecurityServices/factsheets/esecurityhandbook.pdf

WALSH, L. 2002, Standard Practice: ISO 17799 aims to provide best practices for security, but leaves many yearning for more. Accessed 13/9/03
http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml

ANNEX A – LIST OF CERT RECOMMENDED PRACTICES

A. Practices about hardening and securing systems

1. Develop a computer deployment plan that includes security issues
2. Include explicit security requirements when selecting servers
3. Keep operating systems and applications software up to date
4. Offer only essential network services and operating system services on the server host machine
5. Configure computers for user authentication
6. Configure computer operating systems with appropriate object, device, and file access controls
7. Configure computers for file backups
8. Protect computers from viruses and similar programmed threats
9. Configure computers for secure remote administration
10. Allow only appropriate physical access to computers
11. Configure network service clients to enhance security
12. Configure multiple computers using a tested model configuration and a secure replication procedure
13. Develop and promulgate an acceptable use policy for workstations
14. Configure computers to provide only selected network services
15. Isolate the Web server from public networks and your organization's internal networks
16. Configure the Web server with appropriate object, device and file access controls
17. Identify and enable Web-server-specific logging mechanisms
18. Consider security implications before selecting programs, scripts, and plug-ins for your web server
19. Configure the web server to minimize the functionality of programs, scripts, and plug-ins
20. Configure the Web server to use authentication and encryption technologies, where required
21. Maintain the authoritative copy of your Web site content on a secure host
22. Protect your Web server against common attacks
23. Design the firewall system
24. Acquire firewall hardware and software
25. Acquire firewall documentation, training, and support
26. Install firewall hardware and software
27. Configure IP routing
28. Configure firewall packet filtering
29. Configure firewall logging and alert mechanisms
30. Test the firewall system
31. Install the firewall system
32. Phase the firewall system into operation

B. Practices about preparing to detect and respond to intrusions

33. Establish a policy and procedures that prepare your organization to detect signs of intrusion
34. Identify data that characterize systems and aid in detecting signs of suspicious behavior
35. Manage logging and other data collection mechanisms
36. Establish policies and procedures for responding to intrusions
37. Prepare to respond to intrusions

C. Practices about detecting intrusions

38. Ensure that the software used to examine systems has not been compromised
39. Monitor and inspect network activities for unexpected behavior

40. Monitor and inspect system activities for unexpected behavior
41. Inspect files and directories for unexpected changes
42. Investigate unauthorized hardware attached to your organization's network
43. Inspect physical resources for signs of unauthorized access
44. Review reports by users and external contacts about suspicious and unexpected behavior
45. Take appropriate actions upon discovering unauthorized, unexpected, or suspicious activity

D. Practices about responding to intrusions

46. Analyze all available information to characterize an intrusion
47. Communicate with all parties that need to be made aware of an intrusion and its progress
48. Collect and protect information associated with an intrusion
49. Apply short-term solutions to contain an intrusion
50. Eliminate all means of intruder access
51. Return systems to normal operation
52. Identify and implement security lessons learned

E. Practices about improving system security

53. Take appropriate actions upon discovering unauthorized, unexpected, or suspicious activity
54. Identify and implement security lessons learned

F. Practices related to outsourcing managed security services

55. Content Guidance for an MSS Request for Proposal
56. Guidance for Evaluating an MSS Proposal
57. Content Guidance for an MSS Service Level Agreement
58. Transitioning to MSS
59. Managing an Ongoing MSS Provider Relationship
60. Terminating an MSS Provider Relationship
61. Considerations for Network Boundary Protection as Managed Security Services
62. Considerations for Vulnerability Assessment as a Managed Security Service