Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Navigating the Information Security Landscape: Mapping the Relationship Between ISO 15408:1999 and ISO 17799:2000

Cynthia Hoxey
University of Detroit Mercy, choxey@alum.udmercy.edu

Dan Shoemaker
University of Detroit Mercy, dshoemaker1@twmi.rr.com

Navigating the Information Security Landscape: Mapping the Relationship between ISO 15408:1999 and ISO 17799:2000

Cynthia Hoxey
University of Detroit Mercy
choxey@alum.udmercy.edu

Dan Shoemaker
University of Detroit Mercy
dshoemaker1@twmi.rr.com

ABSTRACT

It is crucial for corporations operating in a multinational economy to have a seamless understanding of the security process. For information assurance, ISO 15408:1999 (i.e. Common Criteria) and ISO 17799:2000 are the key standards, both of which are needed for implementing a global approach to security. They provide a definition of the necessary elements of the process as well as the basis for authoritative certification. However, the standards are entirely different in focus. The former is product-oriented while the latter is strategic and organizational. That divergence is an obstacle to creating secure enterprises and it causes disagreement about the meaning and value of the certifications. Mapping the relationship between ISO 15408 and ISO 17799 demonstrates their strengths and weaknesses and encourages organizations to use these standards effectively. The results of our study indicate that while there are overlaps between these two standards, there are also significant gaps.

Keywords

information assurance, information security, common criteria, ISO 15408, ISO 17799, certification, multinational economy

INTRODUCTION

Information assurance involves technology, people and processes. Each has a discrete role and each contributes differently to the ultimate goal of securing the organization. The assurance process blends the most effective factors from each domain into a single effective response. Ideally, the outcome is multi-faceted and holistic, meaning that every conceivable threat is addressed by an appropriate countermeasure.

Adequate protection requires adopting the right set of security practices, which typically requires specialists' expertise. Accordingly, the most practical way to achieve this is by the process outlined in Figure One:

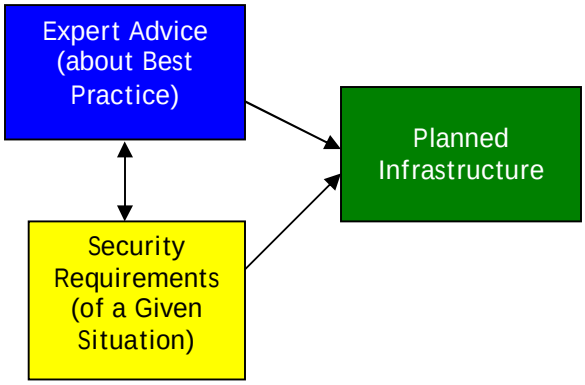

Figure 1: Fundamental Components of Practical Information Assurance

The box labeled "Expert Advice" denotes the fact that the collective body of knowledge can be tapped to provide recommendations about the best way to do something. When a best practice is formally documented, it is known as a standard or model. The box labeled "Security Requirements" highlights the fact that all requirements of the security situation must be satisfied, a situation known as information assurance. Information assurance is embodied through some form of infrastructure that contains sufficient detail to allow workers to understand how to perform tasks. Figure Two illustrates how expert advice and the requirements of the situation combine to produce that tangible outcome.

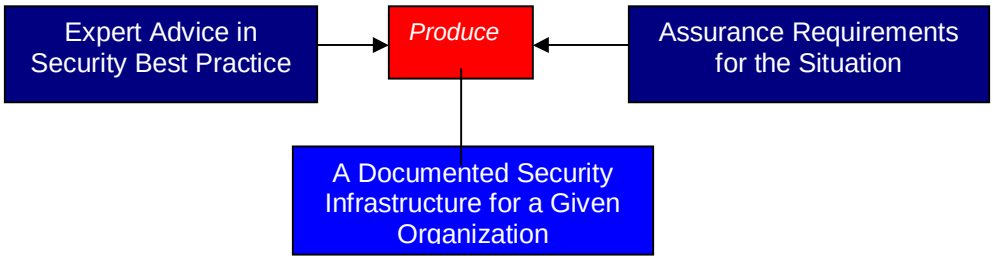

Figure 2: Relationship of the Concepts of Best Practice and Governance to Infrastructure

The embodiment of the information assurance scheme is a documented security infrastructure. This infrastructure is the means to transform expert advice into practical, day-to-day organizational security behavior. In order to accomplish this, the generic best practices specified in the expert model have to be adapted to the specific environment, a process known as tailoring or customization. Tailoring creates a tangible, complete and rational set of procedure specifying all necessary security functions down to the level of explicit tasks. The end product conveys the exact form of the assurance process (e.g., assigned activities) to every employee.

There are two globally recognized models of expert advice. The first one is ISO/IEC 17799:2000 Information Technology - Code of Practice for Information Security Management and the second one is ISO/IEC 15408:1999, popularly known as the Common Criteria[1]. The former is the world's standard for implementing large-scale information security management systems (ISMS) whereas the latter is the international standard for evaluating the security functionality embedded within IT products and systems. Both models provide advice about information protection and both serve as the basis for formal certification.

While ISO17799 contains general advice about organizational security, the recommendations of the Common Criteria are detailed and focus on specifying the functions necessary to judge the trustworthiness of Information Technology products and systems. These differences in scope between ISO17799 and ISO 15408 are problematic because they are not universally accepted and employed in their appropriate domains.

There are financial, societal, and regulatory issues impacting standards implementation. Perceived or real costs associated with standards implementation can weigh heavily in any decision to implement ISO 17799 or ISO 15408. Corporate culture and the strategic approach to information security are philosophical factors influencing standards implementation. Differences between European and United States regulatory cultures and governmental mandates also impact the role and adoption of standards. European Union (EU) countries and Pacific Rim nations favor use of ISO/IEC 17799 as the basis for organizational security system formulation (OECD, 2004). The EU utilizes the ITSEC (Information Technology Security Evaluation Criteria) for product certifications whereas in the United States, ISO 17799 is rarely used. In the U.S., the Generally Accepted Information Security Principles (GAISP) or the OECD (Organization for Economic Co-operation and Development) security domains—embodied in the International Information Systems Security Certification Consortium (ISC[2)] (and even some NIST[2] standards)—are the basis for security system formulation. U.S. companies generally prefer the Common Criteria as the standard advice about product evaluations.

Wylder (2004) comments on the small number of U.S. companies committed to developing a comprehensive information security program. This situation originates from a lack of understanding of the value of information security in the post 9/11 environment. Wylder lauds those companies that understand the crucial relevance of information security in the global environment as well as its root in the core of the business. The fiduciary responsibility of executive management compels leaders to demonstrate how the organization is attentive to standards compliance and implementation.

Wylder cites the technical fixation prevalent in many corporate settings. The problem here is one of perception and mindset, where security personnel and business persons alike tend to focus on the technical view of information security. This myopic vision reduces broader considerations of security to shorter-term views of immediate solutions, product features and

[1] These two names (ISO 15408 and Common Criteria) are used interchangeably. This paper uses the Common Criteria, Version 2.1, August 1999.

[2] National Institute of Standards and Technology

implementation. Wylder understands that properly informed business and security professionals perceive information security as more than an appendage to the core business drivers.

Organizations may adopt specific standards without a firm commitment to the spirit of the standard, without which they cannot gain ongoing benefits of continuous improvement (Spafford, 2003). This philosophy mitigates against adoption of ISO 17799 when companies persist in developing and implementing market-driven, ad-hoc policies and standards, typically without an appreciation for those advanced by international bodies (Ross, 2001). But the solution is more than a simplistic, blind adoption of a standard such as ISO 17799. Walsh (2002) notes that the loose structure and vagueness of ISO 17799 might lead an organization into a false sense of security.

Organizations are not limited to scratch-built security constructs. By combining standards' best practices with specific business knowledge, firms can develop policies that combine security with business needs (Berg, 2004). Hurley (2003) suggests that it is wise to adopt a strategy where only one risk assessment covers all regulations. Such standards' adoption can yield credibility to the processes, technologies, and controls key to an information security environment (Moulton, 2004).

Caralli & Wilson (2004) chide organizations where the mindset relegates information security to the information technology department or to substitute compliance with regulations for an intentional security strategy. The reasons they cite for this problem include the perception that information security is simply overhead or subject to a purely technical approach. These perceptual problems are common, they conclude, because information is too closely associated with the hardware that stores, transports and processes it. Ross (2004) argues that ISO 17799 is severely limited by its conceptual focus and failure to account for technologies that drive risks. He concedes that ISO 17799 can help determine if an organization is secure insofar as it helps define security by use of metrics.

METHODS

The mapping methodology between ISO 15408:1999 (the source document) and ISO 17799:2000 (the target document) is conceptual-literary. This entails a qualitative rather than a strictly quantitative analysis. Reading the narratives of each standard and then comparing/contrasting involves subjective assessment. Biases arise from a researcher's interpretive understanding of the practical and functional differences between the standards. Consequently, the mapping schema could vary based on a researcher's understanding of the similarities and differences between the standards.

Each standard is organized in a hierarchal structure of four levels. The first two levels of each standard are the highest levels whereas levels three and four are more detailed. In ISO 17799, level one consists of principles. A principle is a grouping of control objectives (level 2) that share a common focus. The control objectives are further defined by elements (level 3), some of which are further defined by even more detailed elements (level 4).

In ISO 15408, a class (level 1) is a grouping of security requirements that share a common focus; members of a class are referred to as families. A functional family (level 2) is a grouping of security functional requirements that share security objectives but may differ in emphasis or rigor; the members of a family are referred to as components. Components (level 3) are a specific set of security requirements that are constructed from elements (level 4). Components are the smallest selectable set of security requirements and may be ordered to represent increasing strength or capability.

Mapping is performed in two layers: 1) a high-level map, (level one and two); and 2) a detailed-level map (level three and four). The high-level map compares the first two levels of ISO 15408 (classes and families) with the first two levels (principles and control objectives) of ISO 17799. The detailed-level map compares the last two levels of ISO 15408 (components and elements) with the last two levels (elements and detailed elements) of ISO 17799.

The mapping is not always one-on-one because ISO 17799 operates at a higher level than the Common Criteria. ISO 17799 was broken down at each level into smaller bits called information requirements. Items at all levels in ISO 15408 were then mapped to the information requirements. No level from ISO 15408 covers a level in ISO 17799 completely. In a few cases, a component or element will map to an information requirement at a higher level in ISO 17799. For the most part, ISO 15408 components and elements were excluded from the mapping because of their granularity. Due to space constraints, the detailed mapping is not presented. The table below depicts the relationship between the two standards.

SOURCE DOCUMENT				TARGET DOCUMENT			
ISO 15408:1999 PART 2				ISO 17799:2000			
Map Level	**Level**	**Title**	**Total**	**Level**	**Title**	**Total**	**Map Level**
High Level	1	Class	11	1	Principle	10	High Level
	2	Family	67	2	Control Objective	36	
Detailed Level	3	Component	136	3	Element	127	Detailed Level
	4	Element	250	4	Detailed Element	11	

Table 1: Relationship between ISO 15408 and ISO 17799

RESULTS

All of the ISO 15408 functional and assurance requirements are either directly or indirectly related to the ISO 17799 control objectives, but most only partially fulfill the objective.

The areas of ISO 17799 with the highest match are:

* Security policy – ISO 17799 requires that organizational security policies provide references to more detailed security policies for specific systems. ISO 15408 requires that the organizational security policies relevant to the IT product or system are listed in the Protection Profile. ISO 15408 does not address how or when these polices should be reviewed.
* Asset classification – Asset management (identification, classification and assessment) is a key component of an information security management system and of evaluating a Protection Profile (PP) or Security Target (ST). ISO 15408 does not explicitly address the BS 7799 Information Security Management System Requirements but it does require this information for input into the evaluation criteria.
* Access control – Both ISO 17799 and ISO 15408 address the access policy and rules. ISO 15408 does not address the allocation, administration, and storage of passwords, user's responsibilities or access to unattended user equipment.
* System development and maintenance – The security requirements analysis and specification and change management embodied in ISO 17799 are fulfilled in ISO 15408. However, the Common Criteria does not address technical reviews, outsourced software development or modifications to commercial off-the-shelf software (COTS).

The areas of ISO 17799 with limited match are:

* Personnel – Personnel security is addressed as an assurance requirement for EAL level three and up and in a Protection Profile or Security Target evaluation. The assurance requirements of ISO 15408 address the threats and countermeasures regarding personnel. The security roles addressed in the functional requirements are dependent on the allocation of security responsibilities required in ISO 17799. ISO 15408 does not explicitly address personnel screening, confidentiality agreements, education and training, or the human response to security incidents.
* Communications and operations – ISO 15408 only partially addresses this area with audit trail, segregation of duties, fail safe mechanism, network control and nonrepudiation and cryptography. "The robustness of cryptographic algorithms or even which algorithms are acceptable is not discussed in the [Common Criteria (CC)]. Rather, the [CC is] limited to defining requirements for key management and cryptographic operations" (Herrmann, 2003 p. 11). ISO 15408 does not address system planning and acceptance, facilities management, document security, media handling, or information in non-IT physical transport.
* Compliance - While ISO 15408 partially addresses security audits, privacy, and user data protection, it does not address legislation, Intellectual Property Rights, or organizational records.

The areas of ISO 17799 with little to no match are:

* Organizational security – ISO 15408 does not address the organizational infrastructure, third-party access or outsourcing.

* Physical security – "Physical security is addressed in a very limited context, that of restrictions on unauthorized physical access to security equipment and prevention of and resistance to unauthorized physical modification or substitution of such equipment" (Hermann, 2003, pg. 11). ISO 15408 does not address secure areas outside of development, general physical security controls, equipment accessories or disposal and reuse of equipment.
* Business continuity - While ISO 15408 addresses fail safe mechanisms in IT products, it does not address the business processes surrounding disasters and security failures.

DISCUSSION

Both ISO 17799 and ISO 15408 clearly state that they are neither isolated nor all inclusive. They are intended to be used in conjunction with other guidelines. Users of either standard are encouraged to decide which controls and requirements will be used or extended. As part of a larger information security management system, both standards agree that selection of control objectives or security requirements be based on the business objectives of the organization. The Common Criteria lists several items that are considered out of its scope but are addressed in ISO 17799. Two of them are highlighted below.

Personnel Security

The disparity between the two standards regarding personnel security is alarming. According to the 2004 e-Crime Watch Survey, current or former employees or contractors were cited as a close second to hackers as the greatest cyber security threat. The survey shows 36% of respondent organizations experienced unauthorized access to information, systems or networks by an insider compared to 27% committed by outsiders. The 2004 CSI/FBI Computer Crime and Security Survey indicated that respondents from all sectors do not believe that their organization invests enough in security awareness. As Kevin Henry notes, "Properly trained and diligent people can become the strongest link in an organization's security infrastructure. However, while a machine will enforce a rule it does not understand, people will not support a rule they do not believe in. The key to strengthening the effectiveness of security programs lies in education, flexibility, fairness, and monitoring (2004, pg. 663)."

Compliance

The 2004 e-Crime Watch Survey advised that among policies and procedures, conducting regular security audits are the most effective method to combat e-crime. However, the 2004 CSI/FBI Computer Crime and Security Survey found that the use of security audits is far from universal. The CSI/FBI survey noted that the Sarbanes-Oxley Act (SOX) is having an impact on some industries, but the majority of respondents in other sectors reported that SOX did not raise the level of interest in information security or shift the focus from technology to corporate governance.

Rasmussen (2003) cites the complexities of managing and validating compliance to a confusing variety of regulations and standards. His solution is to distill requirements down to a common, taxonomic base. Rasmussen cites the need for this reduction simultaneously paired with an understanding of the elements common to all the standards, which then can be mapped back to individual standard/regulation. (Rasmussen, 2003).

CONCLUSION

Explicating the relationship between ISO 17799 and ISO 15408 provides a foundation for understanding the variant conceptual territory of these international standards. The outcome of this comparison offers a means for distinguishing the places of common agreement as well as where the gaps lie. This is critically important for security personnel as well as high-level decision makers pursuing a unified approach to security problems.

Failure to adopt a worldwide vision of security creates the potential for miscommunication and misunderstanding of biblical proportions within the multinational security community. Lack of unification underscores the problem of disparate standards and practices. A solution is to adhere to a harmonized set of universally accepted recommendations utilized by corporations to underwrite security activities. As a first step in that process, we have attempted to understand how ISO 17799 and the Common Criteria fit together. We believe that this understanding is the essential first step for getting a common global definition of security. These are the only two major standards promulgated by ISO, which is the world's standard's body. So, any worldwide initiative starts with them.

If one country adopts a governance vision of security and another adopts a functional requirements view (and the gap can be demonstrated), we have the potential for highly insecure products because we will be integrating components developed on two incompatible security schemes. The governance approach is likely superior because it is the basis for tailoring out explicit architectures whereas the Common Criteria approach is not as amenable to associations outside the functional requirements. The Common Criteria are manifestly incomplete (against the recommendations of 17799) and therefore more likely to represent a short-sighted security approach. Businesses interested in assessing the feasibility of standards

implementation must know the relationship between standards, including knowledge of any gaps or overlaps between standards. This marks the initial rationale for why a map of the standards is necessary. Once armed with an understanding of what the standards can and cannot address, CIOs and other information security decision makers are then better able to launch more formal cost/benefit analyses.

APPENDIX: MAPPING DETAILS

Scope limitations preclude expansion of the Mapping Details. It is recommended that the reader obtain a copy of both ISO 17799 and the Common Criteria to facilitate understanding and implementation of information security.

ISO 17799 3.0 Security Policy

Match Analysis

ISO 17799 control objective *3.1 Information security policy* is partially addressed in ISO 15408:

FDP_ACC Access control policy

FDP_IFC Information control policy

ADV_SPM Security policy modeling

APE_ENV.1.3C Protection Profile security environment

ASE_ENV.1.3C Security Target security environment

Gap Analysis

ISO 17799 element *3.1.2 Review and evaluation of security policy document* is not addressed in ISO 15408.

ISO 17799 4.0 Organizational Policy

Match Analysis

ISO 17799 control objective *4.1 Information Security Infrastructure* is partially addressed in ISO 15408:

FMT_SMR Security management roles

Gap Analysis

ISO 17799 control objective *4.1 Information Security Infrastructure* is mostly not addressed in ISO 15408.

ISO 17799 control objective *4.2 Security of third-party access* is not addressed in ISO 15408.

ISO 17799 control objective *4.3 Outsourcing* is not addressed in ISO 15408.

ISO 17799 5.0 Asset Classification and Control

Match Analysis

ISO 17799 control objective *5.1 Accountability for Assets* and *5.2 Information Classification* is addressed by ISO 15408:

APE_DES Protection Profile Target of Evaluation (TOE) Description

ASE_DES Security Target of Evaluation Description.

Gap Analysis

ISO 17799 Asset Classification and Control is not covered specifically in ISO 15408 functional or assurance requirements, nor is it required for any of the evaluation assurance levels. It is only required in the Target of Evaluation Description of the Protection Profile evaluation and the Security Target evaluation.

ISO 17799 6.0 Personnel Security

Match Analysis

ISO 17799 control objective *6.1 Security in Job Definition and Resourcing* is partially addressed in the ISO 15408:

APE_ENV.1.1C Protection Profile security environment

ASE_ENV.1.1C Security Target security environment

ALC_DVS Development security

Gap Analysis

ISO 17799 control objective *6.1 Security in Job Definition and Resourcing* is partially not addressed in ISO 15408:

ISO 17799 control objective *6.2 User Training* is not addressed in ISO 15408.

ISO 17799 control objective *6.3 Responding to security incidents and malfunctions* is not addressed in the ISO 15408.

ISO 17799 7.0 Physical and Environmental Security

Match Analysis

ISO 17799 control objective *7.1 Secure areas* are partially addressed in ISO 15408:

ALC_DVS Development security

ISO 17799 control objective *7.2 Equipment security* is partially addressed in ISO 15408:

FPT_PHP Target of evaluation security function (TSF) physical protection

Gap Analysis

ISO 17799 control objective *7.1 Secure areas* is mostly not addressed in ISO 15408.

ISO 17799 control objective *7.2. Equipment security* is mostly not addressed in ISO 15408.

ISO 17799 control objective *7.3 General controls* is not addressed in ISO 15408.

ISO 17799 8.0 Communications and Operations Management

Match Analysis

ISO 17799 control objective *8.1 Operational procedures and responsibilities* are partially addressed in ISO 15408:

ACM Configuration Management (8.1.2)

FAU_SAA security audit analysis (8.1.3)

FAU_ARP security audit automatic response (8.1.3)

FAU_GEN Security audit data generation (8.1.3)

FAU_STG.1 Protected audit trail storage (8.1.3)

FMT_SMR security management roles (8.1.4)

ISO 17799 control objective *8.4 Housekeeping* is addressed in ISO 15408:

FPT_FLS Fail secure

FPT_ITA Availability of exported TSF data

FPT_ITI Integrity of exported TSF data

FRU Resource utilization

ISO 17799 control objective *8.5 Network management* is partially addressed in ISO 15408:

FDP_UCT Inter-TSF user data confidentiality transfer protection

FDP_UIT Inter-TSF user data integrity transfer protection

FPT_ITI Integrity of exported TSF data

FPT_ITC Confidentiality of exported TSF data

FPT_ITA Availability of exported TSF data

FPT_SSP State synchrony protocol

FPT_TDC Inter-TSF TSF data consistency

ISO 17799 control objective *8.6 Media handling, Security of system documentation*, is partially addressed in ISO 15408:

FDP_ACC Access Control Policy

FDP_IFC Information Control Policy

ADV Development

AGD Guidance documents

Mapping Note

This mapping is implicit. While ISO 15408 does not address the security of the document itself, it does contain sensitive information about the system that would be protected under ISO 17799.

ISO 17799 control objective *8.7 Exchanges of information and software* is partially addressed in ISO 15408:

FCO Communication

FCS Cryptographic Support

FIA Identification and authentication

Gap Analysis

ISO 17799 control objective *8.1 Operational Procedures and Responsibilities* is partially not addressed in ISO 15408.

ISO 17799 control objective *8.2 System planning and acceptance* is not addressed in ISO 15408.

ISO 17799 control objective *8.3 Protection against malicious software* is not explicitly addressed in ISO 15408.

ISO 17799 control objective *8.4 Housekeeping* is partially not addressed in ISO 15408.

ISO 17799 control objective *8.5. Network management* is partially not addressed in ISO 15408.

ISO 17799 control objective *8.6 Media handling and security* is mostly not addressed in ISO 15408.

ISO 17799 control objective *8.7 Exchanges of information and software* is mostly not addressed in ISO 15408.

ISO 17799 9.0 Access Control

Match Analysis

ISO 17799 control objective *9.1 Business requirement for access control* is addressed in ISO 15408:

FDP_ACC Access control policy

FDP_ACF Access control functions

FMT_SMR Security management roles

APE_DES Protection Profile Evaluation, Target of Evaluation (TOE) Description

ASE_DES Security Target Evaluation, Target of Evaluation (TOE) Description

FIA Identification and authentication

FMT_SAE Security attribute expiration

FTA Target of Evaluation access

ISO 17799 control objective *9.3 User responsibilities, Password use* is partially addressed in ISO 15408:

FIA_SOS.2 Generation of secrets

ISO 17799 control objective *9.4 Network access control* is mostly addressed in ISO 15408:

FDP_ACC Access control policy

FDP_ACF Access control functions

FTP Trust path/channels

FIA Identification and authentication

FCS Cryptographic Support

ISO 17799 control objective *9.5 Operating system access control* is partially addressed in ISO 15408:

FIA Identification and authentication

FTA Target of Evaluation access

ISO 17799 control objective *9.6 Application system access control* is partially addressed in ISO 15408:

FDP_ACC Access control policy

FDP_ACF Access control functions

FDP_IFC Information Control Policy

FDP_IFF Information Control Functions

FMT_SMR Security management roles

APE_DES Protection Profile Evaluation, Target of Evaluation (TOE) Description

ASE_DES Security Target Evaluation, Target of Evaluation (TOE) Description

ISO 17799 control objective *9.7 Monitoring system access and use* is partially addressed in ISO 15408:

FAU Security audit

APE_DES Protection Profile Evaluation, Target of Evaluation (TOE) Description

ASE_DES Security Target Evaluation, Target of Evaluation (TOE) Description

FPT_STM Time stamps

Gap Analysis

ISO 17799 control objective *9.3 User responsibilities* is partially not addressed in ISO 15408.

ISO 17799 control objective *9.4 Network access control* is partially not addressed in ISO 15408:

ISO 17799 control objective *9.5 Operating system access control* is partially not addressed in ISO 15408.

ISO 17799 control objective *9.6 Application system access control* is partially not addressed in ISO 15408.

ISO 17799 control objective *9.7 Monitoring system access and use* is partially not addressed in ISO 15408.

ISO 17799 control objective *9.8 Mobile computing and teleworking* is not addressed in ISO 15408.

ISO 17799 10.0 Systems Development and Maintenance

Match Analysis

ISO 17799 control objective *10.1 Security requirements* is addressed in ISO 15408.

ISO 15408:1999 Part 2 Functional Requirements

ISO 15408:1999 Part 3 Assurance Requirements (including evaluations for Protection Profile, Security Target, and Target of Evaluation)

ISO 17799 control objective *10.2 Security in application systems* is addressed in ISO 15408:

FDP_RIP Residual information protection

FDP_ITT Internal Target of Evaluation (TOE) Transfer

FDP_ROL Rollback

FDP_SDI Stored data integrity

FRU Resource utilization

FCS Cryptographic support

FDP_UIT Inter-TOE-Security-Function (TSF) user data integrity transfer protection

FDP_ETC Export to outside TSF control

ISO 17799 control objective *10.3 Cryptographic controls* is addressed in ISO 15408:

FCS Cryptographic Support

FCO Communication

ISO 17799 control objective *10.4 Security of system files* is partially addressed in ISO 15408:

FMT Security management

FAU_GEN Security audit data generation

FAU_SEL Security audit event selection

FDP_ACC Access control policy

FDP_ACF Access control functions

FDP_RIP Residual information protection

FPT_AMT Underlying abstract machine test

FPT_SEP Domain Separation

FPT_TST Target of Evaluation Security function self-test

ISO 17799 control objective *10.5 Security in development and maintenance* is partially addressed in ISO 15408:

ALC_LCD Lifecycle definition

ACM Configuration management

ATE Tests

AVA_CCA Covert channel analysis

ADO Delivery and operation

Gap Analysis

ISO 17799 control objective *10.4 Security of system files* is partially not addressed in ISO 15408:

ISO 17799 control objective *10.5 Security in development and maintenance* is partially not addressed in ISO 15408:

ISO 11.0 Business Continuity Management

Match Analysis

None

Gap Analysis

ISO 17799 control objective *11.1 Aspects of business continuity* is not addressed in ISO 15408.

ISO 17799 12.0 Compliance

Match Analysis

ISO 17799 control objective *12.1 Compliance with legal requirements* is partially addressed in ISO 15408:

FAU Security audit

FDP User data protection

FCS_CKM Cryptographic key management

FPR Privacy

ISO 17799 control objective *12.2 Reviews of compliance* is partially addressed in ISO 15408:

APE_ENV Protection Profile security environment

ASE_ENV Security Target, security environment

ATE Tests

ISO 17799 control objective *12.3 System audit considerations* is addressed in ISO 15408:

FAU Security audit

Gap Analysis

BS 7799-2:1999 3.0 Information Security Management System Requirements

Match Analysis

BS 7799 control objective *3.2 Establishing a management framework* is partially addressed in ISO 1508:

APE_ENV Protection Profile security environment

ASE_ENV Security Target, security environment

Gap Analysis

BS 7799 3.0 Information Security management system requirements is mostly not addressed in ISO 15408.

REFERENCES

1. Berg, A. (2004) "Best Practices for Managing Compliance with Security Standards." TechTarget Security Media. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci958652,00.html. 2004-12-28.
2. Berinato, S. (2003) "After the Storm, Reform." *CIO Magazine*, Dec. 15, 2003. http://www.cio.com/archive/121503/securityfuture.html. 2004-12-28.
3. BS 7799-2 (1999). Information Security Management. Part 2: Specification for Information Security Management Systems.
4. BS ISO/IEC 17799. (2000). Information Technology-Code of Practice for Information Security Management.
5. CC 2.1 (1999). Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model. Available at http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2
6. CC 2.1 (1999). Common Criteria for Information Technology Security Evaluation. (1999) Part 2: Security Functional Requirements. Available at http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2
7. CC 2.1 (1999). Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Requirements. Available at http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2
8. CSO Magazine. (2004). 2004 E-Crime Watch Survey. CSO magazine/U.S. Secret Service/CERT Coordination Center. http://www.csoonline.com/releases/ecrimewatch04.pdf. 2005-01-29.
9. Caralli, R.; Wilson, W. (2004) "The Challenges of Security Management." Carnegie Mellon University, Software Engineering Institute, July 2004. http://www.cert.org/archive/pdf/ESMchallenges.pdf.
10. Caralli, R.; Wilson, W.. (2004) "Maturing your approach to 'Security Management'." Carnegie Mellon University, Software Engineering Institute. http://www.cert.org/archive/pdf/secureit_maturing_approach.pdf.
11. Greene, F. (2002). "A Survey of Application Security in Current in Current International Standards." *Information Systems Control Journal*, Volume 6, 2002.
12. Henry, K (2004). "The Human side of Information Security". Information Security Management Handbook, Fifth Edition, 2004 CRC Press LLC, page 663.
13. Herrmann, D.S. (2003), Using the Common Criteria for IT Security Evaluation. CRC Press LLC, Boca Raton
14. Hurley, E.. (2003). "A Holistic Approach to Compliance." *SearchCIO.com News Writer*, December 12, 2003. http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci940979,00.html 2004-12-13.

15. Institute for eGovernment Competence Center, (IfG.CC), (2004). "The Benefits of Standard IT Governance Frameworks." http://www.e-lo-go.de/html/modules.php?name=News&file=article&sid=2415 2004-07-16.
16. IT Governance Institute (2004). COBIT Mapping. Mapping of ISO/IEC 17799:2000 with COBIT.
17. Moulton, B. (2004). "IT Governance and Information Security". *BankInfoSecurity.com.* Icons, Inc. http://www.bankinfosecurity.com/?q=node/view/1001 2004-05-10.
18. Organization for Economic Cooperation and Development (OECD). (2004). "Summary of Responses to the Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. September 24, 2004. http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase. 2005-01-22.
19. Rasmussen, M. (2003). IT Trends 2003: Information Security Standards, Regulations and Legislation. CISO Analyst Reports. Giga Information Group. http://www.csoonline.com/analyst/report721.html, 2004-12-12.
20. Ross, S. J. (2001). "Standard Questions". *Information Systems Control Journal*, Volume 2, 2001.
21. Spafford, G. (2003). "Truly Benefiting from Standards". *CIO Update*, September 9, 2003. http://www.cioupdate.com/trends/article.php/3074521 2004-12-28.
22. Stevens, J.; Willke, B. (2004) "Which Best Practices are Best for Me?" Carnegie Mellon University, Software Engineering Institute. http://www.cert.org/archive/pdf/secureit_bestpractices.pdf.
23. Walsh, L. (2002) "Standard Practice." *Information Security Magazine*, March 2002. http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml
24. Wylder, J. (2004). Strategic Information Security. CRC Press LLC, Boca Raton, FL.