EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS

TECHNICAL COMMITTEE 7 **RELIABILITY, SAFETY & SECURITY**	**Document Number: WP 5016 V1**

Plenary		**O**	**Category:**	**Workplan**	**O**
Subgroup	**Curr**	**O**		**Minutes**	**O**
	FM	**O**		**Technical**	**O**
	MeD	**O**		**Review**	**O**
	MDS	**O**		**Briefing Paper**	**X**
	RA	**O**		**External**	**O**
	Sec	**X**			

Author(s):
Peter Daniel

Address:
Marconi Selenia Secure Systems
Wavertree Technology Park
Liverpool L7 9PE / United Kingdom
Phone: ++44 151 282 5200
Fax: ++44 151 254 1194
e-mail: pete.daniel@marconiselenia.com

Updates: -

Replaces: -

Pages: 16

Title:

Briefing Paper on Information Security Management
Version 1 (February 2003)

Contents / Abstract: -

Acknowledgements: -

BRIEFING PAPER

Information Security Management
Version 1 (February 2003)

INDEX

1. INTRODUCTION

Increasingly, safety critical information, including monitoring, control and technical design data, is being transferred over networks both nationally and internationally. This information is also being stored electronically. Remote real-time monitoring and control employ Information Communication Technology (ICT) systems. Because electronic information is vulnerable to loss of confidentiality, integrity or availability, secure IT and communication systems need to be implemented and managed. These systems have requirements for both safety and security that could potentially conflict.

The System Security Subgroup was set up within EWICS TC7 over ten years ago to provide guidance to purchasers and groups responsible for secure operation on what to specify with regard to security and how to undertake the specification process; to suppliers on how to satisfy the security requirements, while maintaining project security during the project lifecycle and to users on how to manage and maintain security in their industrial safety critical computer systems. In 1994, the EWICS TC7 System Security Group was involved with the European IT Advisory Experts Group on Information Systems Security (ITAEGV) Working Group investigating whether a standard for a code of practice for IT security would be beneficial for the European Union and the required standardisation activities. The working group reviewed activities being undertaken by international and national organisations in standardisation, industrial and commercial sectors such as banking. Part of its recommendations were that:

a) An international standard for a code of practice for IT security should be developed, based on the UK Code of Practice for Information Security Management.

b) An international standard for basic protection should be developed, based on the German IT Baseline Protection Manual [Ref. 3].

Since 1994, the UK Code of Practice for Information Security Management was developed into a British standard BS 7799. Part 1 of this British standard was used as a basis for the International standard ISO/IEC 17799.

This Briefing Paper progresses this activity by reviewing ongoing work in Europe and internationally on standards and guidelines for the information security management and the required minimum or baseline security measures. Where applicable, information contained in this briefing paper can be used in the implementation of security in these safety systems.

2. TECHNOLOGY DESCRIPTION

The following documents, produced within Europe and internationally, are relevant to Information Security Management:

a) ISO Guidelines for the Management of IT Security (GMITS) [Ref. 4]
b) Information Security Forum's Standard of Good Practice [Ref. 7]
c) UK CCTA Baseline Security for IT Systems [Ref. 2]
d) IBAG Framework for Commercial IT Security [Ref. 5]
e) UK BS 7799:1999 Code of Practice for Information security management [Ref. 1]
f) German IT Baseline Protection Manual [Ref. 3]
g) IT Sicherheitshandbuch (IT Security Handbook) [Ref. 6]
h) ISO/IEC 17799:2000 Code of practice for information security management [Ref. 8]

These documents have been reviewed and the recommendations presented in section 5. Section 2.1 gives an overview of the international activities (i.e. a, b & h), section 2.2 gives an overview of the national activities (i.e. c & d), section 2.3 describes BS 7799 (i.e. e) and section 2.4 describes the German IT Baseline Protection Manual (i.e. f).

2.1 Overview of International Activities

2.1.1 Guidelines for the Management of IT Security (GMITS)

This technical report [Ref. 4] was developed by ISO/IEC SC27 Project GMITS (Guidelines for the Management of IT Security). The report provides management guidance on network security. The report consists of five parts:

Part 1 Concepts and models for IT Security [ISO/IEC/TR3 13335-1:1996]
- Concepts for the management of IT security
- Security elements
- Processes for the management of IT security
- Models

Part 2 Managing and planning IT Security [ISO/IEC/TR3 13335-2:1997]

Part 3 Techniques for the management of IT Security [ISO/IEC/TR3 13335-3:1998]
- IT security strategy, objectives, policies
- Strategic risk analysis considerations
- Baseline controls
- Risk analysis technique
- Implementation and testing of the IT security plan
- Life cycle management techniques
- IT security awareness programme
- IT security architecture

Part 4 Selection of Safeguards [ISO/IEC/TR3 13335-4:2000]

Part 5 Management guidance on network security [ISO/IEC/TR3 13335-5:2001]

2.1.2 Information Security Forum's (ISF) Standard of Good Practice

Since its formation in 1989, the Information Security Forum (ISF), previously known as the European Security Forum (ESF), considers itself as the provider of high quality, business-driven information security solutions. The ISF is an independent, not-for-profit association of the world's leading organisations who recognise the importance of protecting their business information. The ISF produces many publications and reports on IT security. Information on the ISF can be found on the web at www.securityforum.org.

The ISF Standard of Good Practice [Ref. 7] provides a practical, business-focussed, and achievable statement of good practice for information security. The standard is divided into four parts with an appendix on Major Incidents:

Part A Introduction

Part B Controlling the business risks

Part C Setting the Standard

Part D The Standard of Good Practice
- Summary
- Security Management
  - High-level direction
  - Security organisation
  - Risk identification
  - Secure environment
  - External dependencies
  - Management review

- Critical Business Applications
  - Security requirements
  - Risk identification
  - Application management
  - Business users
  - System management
- Information Processing
  - Installation management
  - Production environment
  - System operation
  - Access control
  - Change management
  - Security management
  - Service continuity
- Communications Networks
  - Communications management
  - Network Services
  - Network operations
  - Security management
  - Voice, fax & video
- Systems Development
  - Approach
  - Business requirements
  - Design & build
  - Testing
  - Implementation
  - Change Management

2.1.3 ISO/IEC 17799 Code of Practice for Information Security Management

This standard [Ref. 8] based on the UK BS 7799 Part 1 standard [Ref. 1] was published on 1st December 2000. ISO/IEC 17799:2000 has the following structure:

1. Scope
2. Terms and Definitions
3. Security policy
   - Information Security Policy Document
   - Review and Evaluation
4. Organisational Security
   - Information Security Infrastructure
   - Security of Third Party Access
   - Outsourcing
5. Asset Classification and Control
   - Accountability for Assets
   - Information Classification
6. Personnel Security
   - Security in Job Definition and Resourcing
   - User Training
   - Responding to Security Incidents and Malfunctions
7. Physical and Environmental Security
   - Secure Areas
   - Equipment Security
   - General Controls
8. Communications and Operations Management
   - Operational Procedures and Responsibilities
   - System Planning and Acceptance
   - Protection against Malicious Software

- Housekeeping
- Network Management
- Media Handling and Security
- Exchanges of Information and Software

9. Access Control
   - Business Requirement for Access Control
   - User Access Management
   - User Responsibilities
   - Network Access Control
   - Operating System Access Control
   - Application Access Control
   - Monitoring System Access and Use
   - Mobile Computing and Teleworking
10. Systems Development and Maintenance
   - Security Requirements of Systems
   - Security in Application Systems
   - Cryptographic Controls
   - Security of System Files
   - Security in Development and Support Processes
11. Business Continuity Management
   - Aspects of Business Continuity Management

12 Compliance
   - Compliance with Legal Requirements
   - Reviews of Security Policy and Technical Compliance
   - System Audit Considerations

2.2 Overview of European National Activities

The Baseline Security for IT Systems (BSITS) [Ref. 2] was produced in 1993 by the UK Government Central Computer and Telecommunications Agency (CCTA). Since 1994, no further work has been undertaken on the BSITS. Its main objectives were to provide:

- a methodology to check, whether Baseline Security is sufficient for a given installation;
- a guideline for the selection of Baseline Security Measures;
- a Library of Baseline Security Measures.

The IBAG Framework for Commercial IT Security [Ref. 5] was developed by the INFOSEC Business Advisory Group (IBAG), consisting of user, vendor, auditor, commercial, and standardisation organisations. IBAG terminated its activities a few years ago without a successor. The document covers the spectrum of commercial IT security, adaptable to different organisations and environments. Its main objectives are to:

- propose a high level framework for IT Security;
- use the framework to identify areas where security gaps exist;
- recommend priority areas where work needs to be done

2.3 BS 7799 : Code of Practice for Information Security Management

In 1993, a Code of Practice for Information Security Management was developed by the UK Department of Trade and Industry (DTI), industry and the British Standards Institute (BSI). The intended audience is managers and employees, responsible for initiating, implementing and maintaining information security within their organisation, who can use the Code of Practice as a reference document. This Code of Practice was developed as a result of industry, government and commerce demand for a common framework to enable organisations to develop, implement and measure effective security management practice and to provide confidence in inter-company trading. It is based on the best current information security practices of leading British and international businesses and has met with international acclaim.

In 1995, the Code of Practice became the UK BS 7799 standard and in 1999 a revised version was produced. The standard [Ref. 1] consists of two parts:

BS 7799 Part 1 (1999): Code of Practice for Information Security Management
BS 7799 Part 2 (1999): Specification for Information Security Management Systems

In the UK, a scheme has been introduced to certify organisations against Part 2 of the standard. A new draft Part 2 was produced for consultation by BSI. This is being proposed as a new part of ISO/IEC 17799.

Selection of Controls

In the original standard, ten key controls were given. In the revised version, there is more emphasis on using risk assessment to determine the required controls. A number of software tools are available to support risk assessment (e.g. ISF OSCAR, UK CRAMM), which is concerned with the identification and measurement of the impact of uncertain events upon organisations that depend on computer and communications facilities. The steps leading to a risk assessment are:

- Value Analysis
- Threat Identification Analysis
- Vulnerability Analysis
- Risk Analysis

The value analysis determines the relative value of a facility or operation and its components for the purpose of evaluating its susceptibility to exploitation. The objective is to achieve an understanding of the likelihood that the facility, the information handled by that facility, and/or the function performed by that facility would be singled out for exploitation.

The threat identification analysis identifies threat agents as they relate to the particular facility or operation and the manner by which they may be manifested. A EWICS TC7 briefing paper on Information Warfare [Ref. 9] contains more information on threats. Threats may be actual in which case there is documented evidence of a threat or class of threats, or they may be postulated based upon an assumed capability for which there is no hard evidence.

The vulnerability analysis identifies possible weaknesses in the defences of a facility, system or operation. Vulnerabilities are weaknesses in defensive mechanisms, exposing that which is being protected. Vulnerabilities are generally under the facility control and thus can be modified to limit the effectiveness of an attack.

The risk analysis identifies specific undesirable events through analysis of the possible impacts of previously identified threats and vulnerabilities. The primary objective is to determine the effect on the facility or operation caused by the interaction of threats and vulnerabilities.

The risk assessment summarises all previous activities and presents these findings to appropriate levels of management for their review and evaluation. The identified risks are evaluated to determine their relative impacts upon the facility, the information handled, and the processing performed. The primary objective is to assess the severity of the identified risks and weigh the likelihood of occurrence so that they may be ranked according to degree of acceptability or unacceptability.

In the standard, a number of controls are considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security. Controls considered to be essential to an organisation from a legislative point of view include intellectual property rights, safeguarding of organisational records, data protection and privacy of personal information

Controls considered to be common best practice for information security include:

- Information security policy document
- Allocation of information security responsibilities
- Information security education and training
- Reporting of security incidents
- Business continuity management

2.4 GISA IT Baseline Protection Manual

The IT Baseline Protection Manual [Ref. 3] is a document developed by the German Information Security Agency (GISA). The aim of IT baseline protection is to achieve a security standard for IT systems which is adequate and sufficient for medium-level protection requirements and can serve as a basis for IT applications requiring a high degree of protection. This is achieved through appropriate application of standard organisational, personnel, infrastructure and technical security measures.

Thus, the IT Baseline Protection Manual recommends safeguard packages for typical IT configurations, environments and organisational set-ups. In preparing this Manual, GISA assumed risk assessment estimates based on known threats and vulnerabilities and developed packages of measures suited for this purpose. Consequently, the users of the Manual do not have to repeat these time-consuming analyses regarding IT baseline protection; they only have to ensure that the recommended measures will be consistently and fully implemented. At the same time, this helps to ensure that IT security as regards medium-level protection requirements can be achieved in an efficient manner, especially since individual system security policies can refer to the IT Baseline Protection Manual. Thus, IT baseline protection becomes a common basis of agreement on measures to meet medium-level protection requirements.

Though not required, a complete risk analysis and definition of a security concept (e.g. for high-level protection requirements) is supported by the GISA IT-Security Handbook (IT-Sicherheitshandbuch, 1992) [Ref. 6]. In the last few years, the GISA IT Baseline Protection Manual has been updated and republished annually. It is available on paper, CD-ROM and online (http://www.bsi.bund.de). Also, a GISA-tool for creating IT-Security Concepts based on the Baseline Protection Manual is available. As of October 2002, the IT Baseline Protection Manual was distributed to more than 4000 registered users worldwide (about 3500 in Europe, 3000 in Germany).

Currently, GISA is working on the implementation of a three-level basic protection certificate. It defines three variants of IT Baseline Protection qualification:

Of the three variants of IT Baseline Protection qualification, the IT Baseline Protection Certificate constitutes the highest degree of assurance and the highest security level. Certification authorities accredited to issue IT Baseline Protection Certificates issue the certificate. It is a precondition that the implementation of those standard security safeguards, described in the IT Baseline Protection Manual, relevant to a given case is confirmed by a licensed auditor.

To be eligible for the self-declared "IT Baseline Protection higher level", it is necessary that the agency or company has implemented the most important standard security safeguards contained in the IT Baseline Protection Manual. The necessary preliminary work and information gathering can be performed either by third parties or else by employees of that organisation. The self-declaration is made, based on this premise, by a representative of the organisation who is authorised to sign.

IT Baseline Protection entry-level qualification is achieved when the agency or company has implemented only the essential standard security safeguards contained in the IT Baseline Protection Manual. As in the case of higher level qualification, the preliminary work and information gathering can be performed either by third parties or else by employees of the organisation. Once again the self-declaration is given by a representative of the organisation who is authorised to sign. The level of security represented by the self-declared "IT Baseline Protection entry-level" is the least demanding of the three variants.

2.4.1 Structure

Introduction

- IT Baseline Protection: The Aim, Concept and Central Idea
- Structure and Interpretation of the Manual
- Using the IT Baseline Protection Manual
- Brief Outline of Existing Modules
- Additional Aids
- Information Flow and Points of Contact

Using the IT Baseline Protection Manual

- IT Structure Analysis
- Assessment of protection requirements
- IT Baseline Protection Modelling
- Basic Security Check
- Supplementary Security Analysis

Implementation of IT Security Safeguards

- IT Baseline Protection Certificate

IT Baseline Protection of Generic Components

- IT Security Management
- Organisation
- Personnel
- Contingency Planning Concept
- Data Backup Policy
- Data Privacy Protection
- Computer Virus Protection Concept
- Crypto Concept
- Handling of Security Incidents

Infrastructure

- Buildings
- Cabling
- Rooms
  - Offices
  - Server Rooms
  - Storage Media Archives
  - Technical Infrastructure Rooms
- Protective Cabinets
- Working Place At Home (Telecommuting)

Non-Networked Systems

- DOS PC (Single User)
- UNIX System
- Laptop PC
- PCs With a Non-Constant User Population
- PC under Windows NT
- PC with Windows 95
- Stand-Alone IT Systems Generally

Networked Systems

- Server-Supported Network
- UNIX Server
- Peer-to-Peer Network
- Windows NT Network
- Novell Netware 3.x

Novell Netware 4.x
Heterogeneous Networks
Network and System Management

Data Transmission Systems

Exchange of Data Media
Modem
Firewall
E-Mail
WWW Server
Remote Access

Telecommunications

Telecommunications System (Private Branch Exchange, PBX)
Fax Machine
Answering Machine
LAN connection of an IT system via ISDN
Fax Servers
Mobile Telephones

Other IT Components

Standard Software
Databases
Telecommuting

Safeguards Catalogues

Infrastructure
Organisation
Personnel
Hardware & Software
Communication
Contingency planning

Threats Catalogues

Force Majeure
Organisational Shortcomings
Human Error
Technical Failure
Deliberate Acts

2.4.2 Limits of IT Baseline Protection

The general approach taken to recommended measures, which are admissible in the case of IT baseline protection, cannot readily be applied to IT systems requiring high-level protection. In such cases, individual security analyses provide more detailed results, especially on selection of appropriate security measures taking account of cost/effectiveness. Such analyses can give recommendations for augmenting the IT baseline protection measures by developing additional or qualitatively more effective measures. It is essential that IT applications requiring high-level protection, have individual security analyses are carried out in addition to the enforcement of IT baseline protection.

2.4.3 Comments

The IT Baseline Protection Manual is a large, but well structured guide for baseline protection. It defines areas of application (e.g. a UNIX network) and lists for each area of application, the possible threats, the suggested countermeasures and the responsibilities. A method to determine whether a baseline protection for a given area is adequate is presented in the beginning of the Guide. In case of requirements for protection above baseline, a detailed risk analysis according to the GISA IT Security Handbook [Ref. 6] is mandated.

3. EUROPEAN NATIONAL ASPECTS

The BS 7799 standard has been in use in several European countries including Belgium, Denmark, Germany, The Netherlands, Norway, Sweden and Switzerland. The international standard ISO/IEC 17799:2000 will be probably adopted by these and other European countries. In The Netherlands this is for instance the case.

Section 3.1 covers the UK aspects of BS 7799, section 3.2 covers the German aspects of their Baseline Protection Measures and section 3.3 covers the national aspects of BS 7799 and the Baseline Protection measures in the other European nations.

3.1 United Kingdom

BS 7799:1995 has been revised and a new version was produced in 1999. A three level hierarchy of documents is being considered comprising a management overview at the top level, BS 7799 at the next level and the lower level being sector specific implementations of BS 7799. In 1996, a scheme for certification against BS 7799 Part 2 was developed by UK Department of Trade and Industry (DTI), industry, the UK Accredited Certification Service (UKAS) and the British Standards Institute (BSI). The scheme is similar to ISO 9000, where compliance is assessed by independent accredited certifiers who award a certificate to successful companies. The accredited certification scheme for BS 7799, was launched on 28th April 1998 and developed by DISC (Delivering Information Solutions to Customers), the department within the British Standards Institute (BSI) that manages the IT and telecommunications standardisation. BSI has also produced Proteus a software tool to enable organisations to develop an information security management system compliant with BS 7799. Another compliance tool is Cobra (http://www.iso17799world.com/compliance.htm) which makes recommendations where appropriate.

DISC provides seminars on BS 7799 and has produced the following documents to support the scheme:

- Information Security Management: An Introduction (DISC PD 3000)
- Preparing for BS 7799 Certification (DISC PD 3001)
- Guide to BS 7799 Risk Assessment and Risk Management (DISC PD 3002)
- Are you ready for a BS 7799 Audit? (DISC PD 3003)
- Guide to BS 7799 Auditing (DISC PD 3004)

Also BSI provide translations of BS 7799 in both French and German.

The Department of Trade and Industry (DTI) set up a BS 7799 Users Club. The Club aims to promote the dissemination of good information security management practice, including the use of BS 7799 and the BS 7799 accreditation certification scheme. In 2001, the group changed its name to the ISO/IEC 17799 Users' Group.

In the UK the following recent changes in the law require action on information security management from a wide range of organisations:

- Data Protection Act
- Electronic Communications Act
- Computer Misuse Act

The current Data Protection Act was signed in July '98. This requires protection of personal data. The new legislation states explicitly what precautions data users must take. Under the new law appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing and disclosure of data. Reference to BS 7799 may help data users assess the adequacy of their current security regime.

The bill on E-Commerce started its legislation process early ’99 and became legislation in May 2000, as the Electronic Communications Act. This act recognises digital signatures and the licensing of cryptographic service suppliers, trusted third parties. The implementation of this legislation will probably require as a pre-requisite that organisations are certified to BS 7799.

The Police And Criminal Evidence (PACE) Act and Interception of Communications Act (IOCA) allows access by security services to evidence used in legal proceedings. This access could be used to put a case under the Computer Misuse Act. The integrity of the evidence provided would be enhanced if an organisation is shown to manage its information securely by being certified to BS 7799.

The tScheme (www.tscheme.org) is being established in the UK as a non-statutory self-regulating scheme to provide credible and effective systems and procedures for the approval of electronic trust services. Initially the tScheme will undertake the approval of services based on Public Key Infrastructure (PKI). The actual criteria used for approval will be a selection of elements from publicly available, and wherever possible international, technical or management standards including ISO/IEC 17799.

3.2 Germany

Due to the widespread dissemination of the GISA IT Baseline Protection Manual in Germany, the use of BS 7799 is very limited. Institutions and Companies are normally not willing to use more than one 'standard' though it might be useful because BS 7799 and GISA IT Baseline Protection Manual are complementary. Currently six companies have received an accredited BS 7799 certificate.

Since there is no widespread use of BS 7799, no links can be found in the Data Protection Act or the Multimedia law. There are no connections to the IT Baseline Protection Manual either, probably because there is no certification scheme or anything similar.

3.3 Other European Nations

An international register of organisations with BS 7799 accredited certificates is on the website www.xisec.com/register.htm. European Nations listed include Austria, Finland, Germany, Greece, Hungary, Ireland, Italy, The Netherlands, Norway, Spain, Sweden and the UK. EWICS TC7 members have provided information on the status of information security management in their countries including the adoption of standards such as BS 7799 and use of baseline controls such as GISA IT Baseline Protection Manual.

The Austrian IT-Security Handbook for Public Administration and Government Organisations has been produced. Part I on IT-Security Management was completed in October 1988 and Part II, a practical guide on security measures, was completed in June 2000. This handbook was initiated by the Ministry for Internal Affairs (BMI) and developed together with other ministries and the Prime Minister’s Co-ordination Office (BKA) together with external experts. It compiled, in concise form, the German IT Baseline Protection Manual, ISO TR 13335 and BS 7799 and takes into account Austrian Laws and habits. It is available on the net (www.it-koo.bka.gv.at).

In March 2000, the Belgium parliament passed a new computer crime law “Wet inzake informaticacriminaliteit” [Belgium Kamer van Volksvertegenwoordigers DOC 50 0214/007]. Classical crime on-line is processed like off-line. New crimes are informatics fraud. Penalties for insiders are a penalty class higher than for outsider. Preparation for computer crimes (e.g. possessing hacking tools) is a crime.

BS 7799 is being recommended in Finland as a guideline for companies to include in their good quality practices. Some of the bigger Finnish companies have evidently put at least part of this in use.

A French version of the BS 7799 standard has been available since March 2000. Currently, there is no French company certified to be compliant with this standard although some French companies are preparing to be certified.

In the Netherlands, both the original (1994) and version 2 (2000) of BS 7799 have been translated into Dutch as the "Code voor Informatiebeveiliging" (publication by the Netherlands Standards Institute – NNI as SPE 200003:2000). Various companies like KPMG certify organisations under a scheme against Part 2 of BS 7799 and ISO/IEC 17799:2000.

The "Voorschrift Informatiebeveiliging Rijksdienst (1994)" and the "Handboek Informatiebeveiliging Rijksdienst (1995)" are respectively the mandatory and the handbook for security management for all government departments and agencies. Derived mandatory directives have been written for the Netherlands police.

On January 1, 2001 the Netherlands replaced the privacy law "Wet op de Persoonsregistraties (WPR)" [Staatsblad 1988, 665, last change Stb. 1994, 494] by a new law "Wet Bescherming Persoonsgegevens (WBP)" [Staatsblad 2000, 302] that implements the European privacy regulations. The computer crime law "Wet Computercriminaliteit (WCC)" appeared in 1994. The WCC is a law that changed and added articles to different the law books (crime, penalty, accounting). Since the end of 1999, an update was being processed by the Netherlands Parliament. Progress was halted because of the European Cybercrime Convention developments which will be integrated into the new WCC (WCC II). This WCC II deals for instance with network crimes, denial-of-service, e-stalking, payment smartcards and e-mail privacy.

In Poland, the creation of information system security management law is at an early stage. The first act containing some regulations in this area was the new penal code approved on June 6, 1997 and in force from September 1, 1998. The second relevant act is the decree of the Minister of Internal Affairs and Administration on the determination of basic technical and organisational requirements devices and information systems for personal data processing, issued on the basis of the Parliament Act of August 29, 1997 on the protection of personal data. The third relevant act is on protection of classified information. A chapter devoted to information system and data communications network security contains general requirements for security of data communications systems and networks used for acquisition and transfer of classified information constituting national and official secrets. The decree of the Minister of Internal Affairs and Administration can be considered the first national act that establishes the code of practice for information systems security. However, it only concerns information systems used for personal data. There are no similar government regulations on other applications of computer systems.

4. POINTS OF CONTACT

4.1 BS 7799

UKAS, UK Accredited Certification Service, Queens Road, Teddington, Middlesex TW11 0NA, United Kingdom Tel: +(44) 208 943 6052 Fax: +(44) 208 943 6664

BSI-DISC, 389 Chiswick High Road, London W4 4AL, United Kingdom
Tel:- +(44) 208 995 7799 Fax:- +(44) 208 996 6411 www:- bsi.org.uk/disc

Secretary ISO/IEC 17799 Users' Group, Information Security Policy Group, Department of Trade and Industry, Bay 226/ Red Zone, 151 Buckingham Palace Road, London SW1W 9SS, United Kingdom
Tel:+(44) 207 215 5000 www.dti.gov.uk/cii/

4.2 GISA IT Baseline Protection Manual

Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Tel.: +49 (0)228 9582-369 Fax: +49 (0)228 9582-405 Email: gshb@bsi.de
www.bsi.bund.de/gshb/

5. CONCLUSIONS

Information security is of increasing concern as public and private networks become more and more interconnected providing the communications for safety critical systems as a part of critical national infrastructures. There is currently no code of practice specifically covering the security management aspects of safety critical systems. Such a code of practice would provide a common basis for European safety critical industry to develop, implement and maintain effective security management practice. The document that is best suited as a basis for the European safety critical industry is the international standard ISO/IEC 17799:2000 [Ref. 8]. The standard is clearly structured and easy to read. Clear objectives are given for each major control item. However, the document concentrates exclusively on commercial information and its processing and requires some interpretation when applied to safety critical systems.

There is also no standard or guideline that specifically recommends baseline security protection measures for safety critical systems. It would be helpful if there existed a common basis for European industry to determine appropriate baseline protection measures to counter security threats for these systems. The selection of baseline protection measures should include where appropriate measures recommended in the German IT Baseline Protection Manual [Ref. 3]. A risk assessment technology could be developed to determine if a higher level of security above the baseline is needed. An infrastructure may be required to certify an organisation's conformance to these standards and guidelines.

As well as producing the code of practice, a scheme may be required to certify an organisation's conformance to the standards, within the UK this is being done for BS 7799. This could be part of a quality assessment (ISO 9000) for the procedural requirements. Effectiveness of technical security countermeasures can be evaluated to ascending levels of confidence within predefined functionality classes or protection profiles by approved technical organisations through the IT Security Evaluation Criteria (ITSEC) or Common Criteria (CC) schemes. This would allow mutual recognition of a specified level of IT security for organisations within Europe and internationally.

It is intended that future EWICS TC7 Security Briefing Papers will provide guidance which security management controls should be selected and how to implement the controls for the protection of safety critical systems. Inputs and comments on this briefing paper are welcome and should be sent to either the chair or vice-chair of the EWICS TC7 Security Subgroup detailed on the EWICS website (www.ewics.org).

6. REFERENCES

1. BS 7799:1999 Code of practice for Information security management
2. Baseline Security for IT Systems - CCTA (June 1993)
3. IT Grundschutz Handbuch (IT Baseline Protection Manual) – GISA
4. Guidelines for the Management of IT Security - ISO/IEC/TR3 13335
5. The IBAG Framework for Commercial IT Security - IBAG (version 2.0/Sept '93)
6. IT Sicherheitshandbuch (IT Security Handbook) - GISA (BSI 7105, 1992)
7. Information Security Forum’s Standard of Good Practice
8. ISO/IEC 17799:2000 Code of practice for information security management
9. EWICS TC7 Information Warfare Briefing Paper

7. ABBREVIATIONS

BKI	Austrian Prime Minister's Co-ordination Office
BMI	Austrian Ministry for Internal Affairs
BS	British Standard
BSI	British Standards Institute
BSITS	Baseline Security for IT Systems
CC	Common Criteria
CCTA	UK Government Central Computer and Telecommunications Agency
CD-ROM	Compact Disk - Read Only Memory
CRAMM	CCTA Risk Analysis and Management Methodology
DISC	Delivering Information Solutions to Customers
DOS	Disk Operating System
DTI	UK Department of Trade and Industry
ESF	European Security Forum
GISA	German Information Security Agency
GMITS	Guideline for the Management of IT Security
GSHB	German Baseline Security Handbook
IBAG	Infosec Business Advisory Group
ICT	Information and Communication Technology
IEC	International Electrotechnical Committtee
Infosec	Information Security
IOCA	Interception of Communications Act
ISDN	Integrated Services Digital Network
ISF	Information Security Forum
ISO	International Organization for Standardization (www.iso.ch)
IT	Information Technology
ITAEGV	IT Experts Group on Information Systems Security
ITSEC	IT Security Evaluation Criteria
LAN	Local Area Network
NNI	Netherlands Standards Institute
OSCAR	ISF Risk Analysis
PACE	Police and Criminal Evidence
PBX	Private Branch Exchange
PC	Personnel Computer
PKI	Public Key Infrastructure
TR	Technical Report
UK	United Kingdom
UKAS	UK Accredited Certification Service
WBP	Wet Bescherming Persoonsgegevens (Dutch Data Protection Law)
WCC	Netherlands Computer Crime Law
WPR	(former) Dutch Data Protection Law
WWW	World Wide Web