ENISA ad hoc working group on risk assessment and risk management

Reference source for threats, vulnerabilities, impacts and controls in IT risk assessment and risk management

Deliverable 3
Version 1.0

Date: 26/04/2007

Contents

1 Introduction

Effective IT risk assessment and management, using the process described on the ENISA website (www.enisa.europa.eu/rmra/rm_process.html), requires the input of information about IT security assets, about threats to these and about their vulnerabilities, about potential impacts on assets, and about controls that can be put in place. Such information is essential to all of the tools, good practices or methodologies for risk assessment and risk management that are catalogued in the inventory on the ENISA Website (http://www.enisa.europa.eu/rmra/rm_ra_methods.html).

Inventoried here are therefore a number of sources of information concerning:

- Assets
- Threats
- Vulnerabilities
- Impacts
- Controls.

The preliminary inventory has been compiled by members of the ENISA ad-hoc working group on risk assessment and management. ENISA intend to extend and improve this inventory and regularly review entries. Suggestions for additional entries, or changes to existing entries, are welcomed – please contact: riskmngt@enisa.europa.eu.

Each entry in the inventory contains a short description of the information source referenced and the following data:

Location: Where the referenced information can be found in the source document.

Version and Date: Version and date of the referenced source document.

Last updated: Date when ENISA last updated the entry.

FoC: Although all referenced documents are publicly available, some may incur an access charge or fee. Where no such charge is made, this is indicated by use of the abbreviation FoC (Free of Charge).

The inventory can be used to provide input to support the use of individual tools, good practices or methodologies for risk assessment and risk management. Or it can be used to support individual processes selected from a number of such tools, good practices or methodologies, as chosen according to the system described in the ENISA methodology for evaluating usage and comparison of risk assessment and management items. The table below indicates where inputs and outputs into the 15 processes referenced in the benchmark used by that methodology will benefit from the information presented in this inventory.

	Asset	Threat	Vulnerability	Impact	Control
Inputs	I.2.3	I.2.1	I.5.1	I.4.1	I.6.4
	I.4.1	I.5.1	I.5.2	I.5.1	
	I.4.2	I.5.2		I.5.2	
	I.6.2			I.5.3	
Outputs	O.2.3	O.5.1	O.5.2	O.5.3	O.6.3
	O.4.2	O.5.7	O.5.7	O.6.4	O.9.1
	O.5.2	O.6.2	O.6.2	O.6.6	
	O.5.4				
	O.6.1				
	O.6.2				
	O.6.3				
	O.6.4				
	O.6.5				
	O.6.6				
	O.9.1				

2 Table of reference sources

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
1	**title** : Austrian IT Security Handbook ("Österreichisches IT-Sicherheitshandbuch") **version & date** : Version 2.2, November 2004 **description** : While part 1 of the handbook gives guidelines for the establishment of an IT security management process in on organization, part 2 "Security Measures" gives a comprehensive summary of technical and organizational security controls. **hyperlink** : http://www.cio.gv.at/securenetworks/sihb/ **free of charge** : yes **language** : German **last update** : 16.04.2007					**location :** part 2 "Security Measures" **description :** comprehensive summary of technical and organizational security controls, comprising: physical and infrastructure security, human resources security, security management, security in system development, technical controls, security in operation, business continuity. **hyperlink** : http://www.cio.gv.at/securenetworks/sihb
2	**title :** C.E.R.T. **version & date :** continuous **description** : web site on vulnerabilities **hyperlink :** http://www.cert.org/nav/index_red.html **free of charge** : yes **language** : English **last update** : 16.04.2007			**location** **description** : gives support on remediation on the vulnerabilities **hyperlink** : http://www.cert.org/nav/index_red.html		
3	**title :** CobiT 4.0 **version & date :** Version 4.0, 2005 **description :** CobiT is an IT governance framework supporting business alignment of IT and IT auditing. It defines 34 IT processes and about 215 detailed control objectives, providing generic information on security controls, as well as efficiency and compliance.	**location** : refer to the ISACA brochure "COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0" **description** : several parts of the Cobit framework must be considered				**location** : refer to the ISACA brochure "COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0" **description** : several parts of the Cobit framework must be considered **hyperlink** : www.isaca.org

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
	hyperlink : www.isaca.org **free of charge :** yes **language :** English, French, German, Italian, Japanese, Portuguese, Spanish **last update** : 29.03.2007	**hyperlink** : www.isaca.org				
4	**title :** Common Criteria for Information Technology Security Evaluation **version & date :** Version 3.1, revision 1, September 2006 **description :** Common Criteria for Information Technology Security Evaluation (shortly CC) is not a Risk Analysis and Management methodology: it is primarily intended as a guide to assist the user in individuating and formally defining security requirements for a given TOE (Target Of Evaluation). It provides the users with a guidance suitable to describe with different degrees of formality how security requirements are individuated (may be using a RARM method), how they are fulfilled and how related countermeasures are set-up. The deliverables of such a standard are the typical ones able to enter a certification process, which is the ultimate goal of CC usage. Keep in mind that a security certification scheme like the CC one doesn't certify the capability of a product or a process or an organisation to contrast all possible attacks, but merely certifies that declared countermeasures **free of charge** : yes **language** :English, German **last update** : 16.04.2007			**location** **Description** : Due to its non-RARM methodology nature, CC have very little if none consideration of vulnerability, considered only at glossary level **hyperlink** : www.commoncriteriaportal.org	**location** : **Description** : Due to its non-RARM methodology nature, CC have very little if none consideration of impact. **hyperlink** :www.commoncriteriaportal.org	**location** : Part 2 **Description** : Are widely covered (grouped in an exhaustive number of functional classes) **hyperlink** : www.commoncriteriaportal.org
5	**title :** CSI/FBI survey **version & date :** published each year **description :** The Computer Crime and Security Survey is conducted by the Computer Security		**location** : can vary each year **description** : result on a survey in the United States	**location** : can vary each year **description** : result on a survey in the	**location** : can vary each year **description** : result on a survey in the United	

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
	Institute (CSI) with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. It is based on the responses of computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. **hyperlink :** http://www.gocsi.com/ **free of charge :** yes **language :** English **last update :** 29/03/2007		**hyperlink** : http://www.gocsi.com/	United States **hyperlink** : http://www.gocsi.com/	States **hyperlink** : http://www.gocsi.com/	
6	**title** : DTI Information Security Breaches Survey – Technical report (PricewaterhouseCoopers) **version & date** : April 2006, carried out every two years **description :** Survey of UK businesses, provides information on security incidents suffered by businesses, both large and small**.** **hyperlink :** www.dti.gov.uk/sectors/infosec/index.html **free of charge :** yes **language :** English **last update** : 29.03.2007				**location : Part** "Security Breaches" **description** : **hyperlink** : www.dti.gov.uk/sectors/infosec/index.html	**location :** Part "Security Controls" **description** : **hyperlink** : www.dti.gov.uk/sectors/infosec/index.html
7	**title :** ISO/IEC 17799:2005 "Information technology –Security techniques - Code of practice for information security management" **version & date :** 2005 **description :** This international standard gives guidelines and general principles for establishing and maintaining information security management in an organization. It provides a list of 133 generic security controls. **hyperlink :** http://www.iso.org and national standardization bodies (http://www.nia.din.de/sixcms/detail.php?id=5195					**location** : chapters 5 to 15 refer also to the ISACA brochure "COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0" **description** : Implementing ISO/IEC 17799 (27002) will give the guidance of implementing controls to be able to provide certification against the ISO/IEC 27001 **hyperlink** : http://www.iso.org

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
	) **free of charge** : no **language :** English, French, Russian, German **last update** : 29.03.2007					and national standardization bodies
8	**title :** ISO/IEC 27005 "Information technology – Security techniques - Information security risk management (draft)" **version & date :** draft **description :** This international standard provides guidelines for information security risk management in an organization. **hyperlink :** http://www.iso.org and national standardization bodies (http://www.nia.din.de/sixcms/detail.php?id=5195) **free of charge :** not yet published (restricted to ISO experts), published standard will not be free of charge **language :** English **last update** : 29.03.2007	**location** : Annexes B1 and B2 **description** : In Annex B1 (Asset identification) sorts assets are sorted into: 1. Primary assets - 1.1Business process & activities, -1.2. Information 2. Supporting assets -2.1 Hardware -2.2 Software -2.3 Network -2.4 Personnel -2.5 Site -2.6 Organization. Annex B2 (Asset valuation) gives a list of criteria. **hyperlink**:	**location** : Annex C **description** : Annex C contains a list of about 40 typical threats and their possible origin (accidental, environmental or deliberate). For deliberate threats a description of possible threat sources (hackers, insiders, terrorists,...) and threat actions is given. **hyperlink**:	**location** : Annex D **description** : Annex D gives examples of vulnerabilities and corresponding threats and some methods for vulnerability assessment **hyperlink**:	**location** : Section 7.2 (Basic criteria) p11. Annex B3 (Impact assessment) p47. **description** : Section 7.2 p11 "Basic criteria" proposes a list of 6 impact criteria. Annex B3 (Impact assessment) p47 proposes a characterization of an operational impact: direct (4 items) or indirect (5 items) **Hyperlink**:	**location** : Section 9 Information security risk treatment. **description** : This section sorts risk controls into: 1. Risk avoidance 2. Risk transfer 3. Risk reduction (refers to ISO 27002), 4. Risk retention (referring to ISO27001-4.2.1 **hyperlink**
9	**title** : IT-Grundschutz **version & date** : December 2006 **description** : The IT-Grundschutz Catalogues provide lists of typical relevant threats and the respective standard security measures for standard asset-types. Technical, organisational, personnel and infrastructural issues are encountered. The information is publicly available and free of costs. **hyperlink** : http://www.bsi.de/gshb/deutsch/index.htm (German), http://www.bsi.de/english/gshb/index.htm	**location :** Chapter "Catalogues of Modules" **description** : In IT-Grundschutz the assets addressed are handled in "modules". Each module describes a standard use of the asset and the relevant threats and security measures. The modules are grouped into the layers: generic aspects,	**location** : Chapter "Catalogues of threats" **description** : IT-Grundschutz provides a list of the threats that are considered to be relevant for the addressed assets (modules). The version 2006 of the IT-Grundschutz Catalogues contains more than 400 threats. For each threat a detailed description		**location** : IT-Grundschutz Methodology, BSI-Standard 100-2, Page 39 **description** : The IT-Grundschutz Methodology provides a list of high-level impacts as a basis for the definition of the protection	**location** : Chapter "Catalogues of Safeguards" **description** : IT-Grundschutz provides a list of thesafeguards that are considered to be relevant for the addressed assets (modules). The version 2006 of the IT-Grundschutz Catalogues contains more than 1000 safeguards. Each safeguard is provided with a detailed description, the responsible roles

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
	(English) **free of charge (yes or not) :** yes **language** : German, English **last update** : 29.03.2007	infrastructure, IT systems, network, applications. Version 2006 of IT-Grundschutz Catalogues contains 70 modules. **hyperlink** : http://www.bsi.de/gshb/deutsch/baust/b01.htm	is given. **hyperlink** : http://www.bsi.de/gshb/deutsch/g/g01.htm		requirements of the assets. **hyperlink** : http://www.bsi.de/literat/bsi_standard/index.htm	for initiation and implementation and a set of check questions. **hyperlink** : http://www.bsi.de/gshb/deutsch/m/m01.htm
10	**title** : kes/Microsoft-Sicherheitsstudie 2006 - Lagebericht zur Informations-Sicherheitsicherheit **version & date :** October 2006 **description** : The magazine “kes” carries out a survey on the IT security status in Germany every 2 years. The last study provides information on IT risks, IT security attacks and IT security status in Germany. The survey can be purchased from SecuMedia Publishing House **hyperlink** : http://www.kes.info/ free of charge (yes or not) : no **language** : German **last update** : 16.04.2007				**location :** Part 1 **description :** The first part of the survey contains statistical information on kind, extend and costs of IT security damages during the last 3 years. **Hyperlink :** http://www.kes.info Access requires password	**location** : Part 2 **description** : The second part of the survey contains statistical information on the IT security measures already implemented. **Hyperlink** : http://www.kes.info Access requires password
11	**Title** : **EBIOS** **Version & Date :** **version 2, 2004-02-05** **Description :** **EBIOS-Guide :** **-Section 4 "Tools for assessing ISS risks".** **-Section 5 "Tools for treating ISS risks"** These 2 sections contain the following EBIOS knowledge bases: 1. A classification of entities according to types and sub-types, 2. A classification of 42 generic attack methods, with a detailed description (corresponding threat	**Location** : **EBIOS-Guide Section 4 "Tools for assessing ISS risks" pp 7-23.** **Description:** In EBIOS, an asset is composed of an essential element (ie. immaterial part that carries the asset value) and entities (ie. concrete parts that support the asset). The essential elements are of 2 types: 1. Function (ie. business	**Location** **EBIOS-Guide Section 4 "Tools for assessing ISS risks" pp 24-53.** **Description :** Classification of 42 generic attack methods, according to 8 types: 1. Compromise of information, 2. Compromise of functions, 3. Technical failures, 4. Unauthorised actions,	**Location** **EBIOS-Guide Section 4 "Tools for assessing ISS risks" pp 54-188.** **Description :** Classification of generic vulnerabilities according to 42 attack methods that can exploit them, and with cross-references to type or	**Location :** **EBIOS-Guide Section 3 "Techniques" pp 21-22.** **Description** Table of 22 (proposed) relevant impacts. These impacts on business processes are used to assess the security needs of each asset with respect to security criteria and	**Location :** **EBIOS-Guide Section 5 "Tools for treating ISS risks" pp 1-198.** **Description** 1. Knowledge bases of generic security objective, arranged according to entity types. 2. Knowledge base of functional security requirements, integrating: -ISO-IEC-15408 (11 types), -ISO-IEC-17799 (10 types), -DCSSI-PSSI (Information-

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
	agent profiles and impacts, …), 3. A classification of generic vulnerabilities, cross-referenced to attack methods and entities knowledge bases. 3. A classification of security objectives and security requirements for risk treatment, with cross-references to attack methods base and vulnerabilities base, together with coverage tables. Theses security objectives and requirements are recompiled and rearranged from major ISO standards, DCSSI-PSSI and EBIOS-Club-Best-practices. All these knowledge bases are implemented and intertwined in EBIOS software. Cross-references are then automatically carried out by the software tool, giving real added value to consultant when filling up an EBIOS study. Those knowledge bases result from experience feedback of DCSSI experts or EBIOS club members, and from various ISO standards. They are constantly maintained for relevance and exhaustiveness. Consultants may also use a base of 13 best practices guides, convenient when producing deliverables in accordance with a specific template: NATO (CSRS, SSRS, SISRS, SECOPS…), ISO- 15408 (Protection Profile, Security Target), ISO-17799 (Security Policy) ISO-27001 (Risk Treatment Plan, Statement of Applicability). **nyperlink :** http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html **Free of charge: yes** **Language** : **French, English, German, Spanish.** **Last update** : 29.03.2007	process) 2. Information (inputs/outputs of functions). EBIOS provides with a classification of entities into types and subtypes with detailed description and examples. The 7 entities types are : 3. Hardware, 4. Software, 5. Network, 6. Personnel, 7. Site, 8. Organization 9. System These classifications are compliant to (draft) ISO/IEC27005. **hyperlink** : http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section4-outillageappreciation-2004-02-05_en.pdf	5. Physical damage, 6. Natural events, 7. Loss of essential services 8. Disturbance due to radiation. (classification compliant to ISO/IEC27005) All attack methods are described with the following details: 1. Affected security needs criteria, 2. Threat agent profiles with type of intentionality (natural, human, environmental), 3. Resources needed for him to act (time, money, skills,…), 4. Feared consequences, 5. Examples. **hyperlink :** http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section4-outillageappreciation-2004-02-05_en.pdf	sub-type of entities (Entity sub-types inherit of vulnerabilities of their entity type). **hyperlink** : http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section4-outillageappreciation-2004-02-05_en.pdf	the corresponding scales of security needs. These proposed impacts are also referred to as "consequences" in each attack method description given in EBIOS Guide section 4 §3 (pages 26-53). **hyperlink** : http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section3-techniques-2004-02-05_en.pdf	System-Security Policy) (16 types) -Other sources (15 types). These requirements cover a wide spectrum of controls ranging from technical to organizational and training/awareness controls. 3. Coverage table of vulnerabilities by security objectives according to attack methods. 4. Coverage table of security objectives by security requirements according to types and subtypes of entities. Coverage tables are useful to ensure security controls are necessary and sufficient. They are also needed when dealing with defence in depth (resilience). **hyperlink** : http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section5-outillagetraitement-2004-02-05_en.pdf

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
12	**title** : Mac Afee **version & date :** continuous **description :** **hyperlink :** http://us.mcafee.com/virusInfo/default.asp?WWW_URL=www.mcafee.com/anti-virus/default.asp **free of charge:** **language** : English, French **last update** : 29.03.2007					**location :** **description :** **hyperlink :** http://us.mcafee.com/virusInfo/default.asp?WWW_URL=www.mcafee.com/anti-virus/default.asp
13	**title** : MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información **version & date :**version 2, 2005 **description :** The first version of MAGERIT is dated in 1997. In 2005 Electronic Government Council (Consejo Superior de Administración Electrónica, CSAE) has prepared version 2 of the Risk Analysis and Management Methodology for the information systems of Public Administrations, MAGERIT (the Spanish acronym) and recently this version has been translated to English. **hyperlink :** http://www.csae.map.es/csi/pg5m20.htm **free of charge :** yes **language :** Spanish, English **last update** : 29.03.2007	**location** : Magerit methods, chapter 2 **description :** Relevant assets are identified and defined in respect to relation and operations they perform on data. Chapter 2 of the "Elements catalogue" gives a list of types of assets.The threats and safeguards are different according to the type of assets. The concept of "dependencies between assets" is introduced and explained.Value and dimensions of assets are also discussed. Furthemore, quantitative and qualitative valuations are explained with the pointers to chapters 8.1 and 8.2 that give analysis model based on these valuations.Finally, one exception (the valuation of the	**location** : Magerit methods, chapter 2 (page 20) and chapter 5 of the "Elements catalogue" that gives a list of typical threats. **description :** The valuation of threats is described with two aspects: degradation and frequency. **hyperlink :** http://www.csae.map.es/csi/pg5m20.htm	**location** : Magerit methods, chapter 2 **description :** In comparasing with Magerit v1.0, the "vulnerability" concept is now incorporated using the degradation measurements of the asset and the frequency with which the threat occurs. **Hyperlink :** none	**location** : Magerit methods, chapter 2, page 21 **description :** Direct derivation of impact is explained, as well as accumulated and deflected impact. These determine the impact of a threat on an asset in a certain dimension. This chapter also explaines how single impacts may be aggregated under certain conditions. **hyperlink :** http://www.csae.map.es/csi/pg5m20.htm	**location** : Magerit methods, chapter 2, page 23. Chapter 6 of the "Elements catalogue" gives a list of suitable safeguards for each type of asset. **description :** Procedures or technological mechanisms that reduce the risk are called safeguards or counter-measures in Magerit 2, although term security controls is also used for measuring effectiveness of these safeguards. These are described and classified in different terms (preventive, degradation limitation, according to their effectiveness...). In Appendix 1 (Glossary), page 99, several definitions for terms safeguard, countermeasures and controls are given. **hyperlink** : http://www.csae.map.es/csi/pg5m20.htm

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
		interruption of the availability) is described with a use of a more complex structure. **hyperlink :** http://www.csae.map.es/csi/pg5m20.htm				
14	**title** : NIST SP 800-30 : Risk Management guide for Information technology systems **version & date :** July 2002 **description :** The document provides a foundation for the development of a risk management and gives definitions and practical guidance. **hyperlink :** http://csrc.nist.gov/publications/nistpubs/ **free of charge** : yes **language :** English **last update** : 29.03.2007		**location :** chapter 3.2 **description :** It contains a list of typical human threats (threat source, motivation and threat actions) **hyperlink :** http://csrc.nist.gov/publications/nistpubs/	**location :** chapter 3.3 **description** : gives some examples for vulnerability/threat pairs **hyperlink :** http://csrc.nist.gov/publications/nistpubs/		**location :** chapter 4.4 **description** : a list of security control categories **hyperlink** : http://csrc.nist.gov/publications/nistpubs/
15	**title** : OCTAVE ("Operationally Critical Threat, Asset, and Vulnerability Evaluation") **version & date** : Version 2.0, **description** : OCTAVE is a comprehensive RA method and is supported by a number of papers outlining different aspects of RA, eg the White paper on "OCTAVE threat profiles" and the "Catalogue of practices", which can be regarded as list of generic security controls. **hyperlink** : http://www.cert.org/octave/methods.html **free of charge:** **language** : English **last update** : 29.03.2007	**location :** OCTAVE SM Method Implementation Guide Version 2.0, Volume 7: Process 5 – Identify Key Components **description** : Within Process 5 the key components of the infrastructure for each critical asset are identified .	**location :** White Paper "OCTAVE Threat Profiles" **description :** A list of generic security controls is given to build asset-based Threat Profiles **hyperlink** : http://www.cert.org/octave/pubs.html		**location :** OCTAVE SM Method Implementation Guide Version 2.0 Volume 9: Process 7 – Conduct Risk Analysis §10.1 Risk Impact Descriptions and Values for Critical Assets **description** : Contains a table with descriptions of impacts to the organization. **hyperlink** :	**location :** OCTAVE Catalog of Practices, Version 2.0 **description** :This document outlines the set of practices against which organizations can compare their own practices during OCTAVE. **hyperlink** : http://www.cert.org/archive/pdf/01tr020.pdf

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
					http://www.cert.org/octave/pubs.html	
16	**title** : OWASP web site **version & date :** continuous **description** : The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. **hyperlink :** http://www.owasp.org/index.php/Main_Page **free of charge**: yes **language :** English **last update** : 16.04.2007		**location** : specific web page **description** : give general information on threat **hyperlink :** http://www.owasp.org/index.php/Category:Threat_Agent	**location :** specific web page **description :** give general information on vulnerability **hyperlink :** http://www.owasp.org/index.php/Category:Vulnerability		
17	**title** : Secunia web site **version & date** continuous **description :** this website is a portal that gives information on virusses and also news related to information security.It is not related to a specific supplier **hyperlink** : http://secunia.com/ **free of charge (yes or not) :** yes **language :** English **last update** : 16.04.2007		**location :** website **description :** advisories on viruses **hyperlink** : http://secunia.com/	**location n :** website **description :** advisories on system imperfections **hyperlink :** http://secunia.com/		
18	**title** : Securityfocus portal **version & date :** continuous **description :** portal related to information security **hyperlink** : http://www.securityfocus.com **free of charge**: ye**s** **language** : English **last update** : 16.04.2007			**location** : website **description** : allow search on several criteria for vulnerabilities **hyperlink :** http://www.securityfocus.com/vulnerabi		

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
				lities		
19	**title** : Sophos **version & date** : continuous **description** : Vendor website with relevant information **hyperlink** : http://www.sophos.com/security/ **free of charge:** yes **language** : English **last update** : 16.04.2007					**location :**specific web pages **description** : give informationon control to put in places **hyperlink :** http://www.sophos.com/security/
20	**title** : Symantec Internet Security Threat Report (ISTR) **version & date** : continuous **description :** Vendor website with relevant information **hyperlink :** http://www.symantec.com/enterprise/threatreport/index.jsp **free of charge :** yes **language** : English **last update** : 16.04.2007		**location :** website **description** : descriptions of threats **hyperlink** : http://www.symantec.com/enterprise/threatreport/index.jsp	**location** : website **description** : description and resolution of vulnerabilities **hyperlink :** http://www.symantec.com/enterprise/threatreport/index.jsp		
21	**title** : Systems Security Engineering — Capability Maturity Model (SSE-CMM) / ISO/IEC 21827:2002 **version & date :** 2002 **description :** The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. **hyperlink :** www.sse-cmm.org/index.html **free of charge:** yes **language :** English **last update** : 16.04.2007	**location :** several **description** : descriptions of threats **hyperlink** : http://www.symantec.com/enterprise/threatreport/index.jsp				
22	**title :** The IT-Security Situation in Germany in	**location** : Chapter 4,	**location** : Chapter 3 IT-			

Nr	Source	Assets	Threats	Vulnerabilities	Impacts	Controls
	title : **version & date** : **description** : **hyperlink** : **free of charge (yes or not)** : **language** : **last update** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :	**location** : (e.g. chapter, page etc.) **description** : **hyperlink** :
	2005 **version & date :** 2005 **description** : This report presents the current IT-security situation in Germany, provides lists of threats priorised according to their importance and their damage as well as statistics on IT security attacks. The report makes also a categorisation and evaluation of trends in IT security. The information is publicly available and free of costs. **hyperlink :** http://www.bsi.de/english/publications/securitysituation/lagebericht2005_englisch.pdf **free of charge**: yes language : German, English **last update** : 16.04.2007	Vulnerabilities of and Threats to IT Systems, Page 14 **description** : The report contains statistics on vulnerabilities and on the respective exploits. **hyperlink** : http://www.bsi.de/english/publications/securitysituation/lagebericht2005_englisch.pdf	Security Awareness and IT-security Competence in Society, Page 9 **description** : List o threats and statistics on their importance today and in the future **hyperlink** : http://www.bsi.de/english/publications/securitysituation/lagebericht2005_englisch.pdf			