ExecIA LLP

Excellence in Information Assurance

Low Cost Information Risk Management

RINNO. Lisbon. 22nd January 2010

Dr Jeremy Ward

Agenda

1 Information security risk

2 Current Internet threats and vulnerabilities

3 ENISA Risk Management

4 Self-Assessed Risk Profiling

Information Security Risk

"The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."

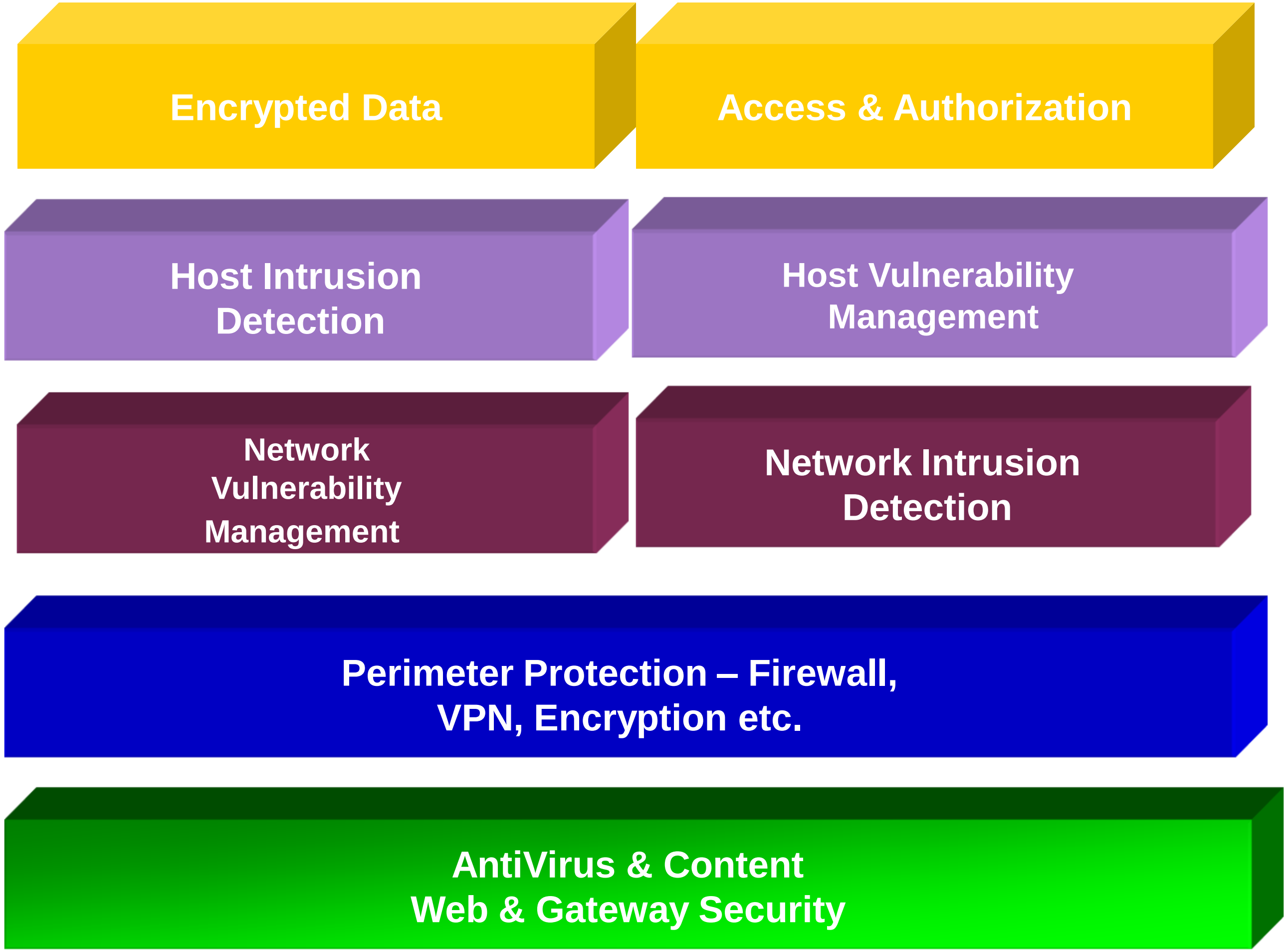
Threat: "a potential cause of an unwanted incident, which may result in harm to a system or organization."

Vulnerability: "a weakness of an asset or group of assets that can be exploited by one or more threats."

Asset: "anything of value to an organization".

All definitions from ISO 27002: 2005

Barriers seem to be the answer



Encrypted Data

Access & Authorization

Host Intrusion Detection

Host Vulnerability Management

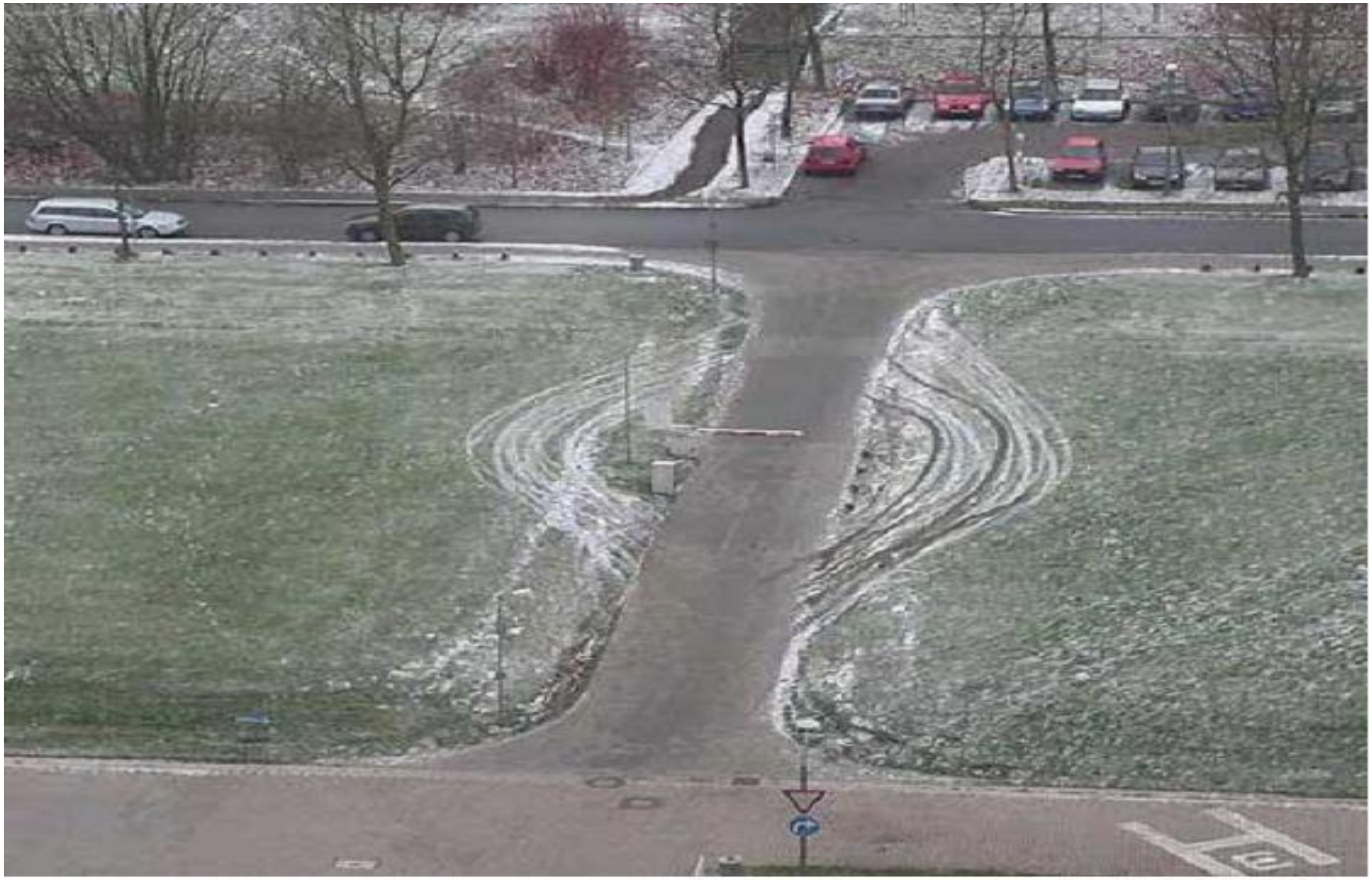
Network Vulnerability Management

Network Intrusion Detection

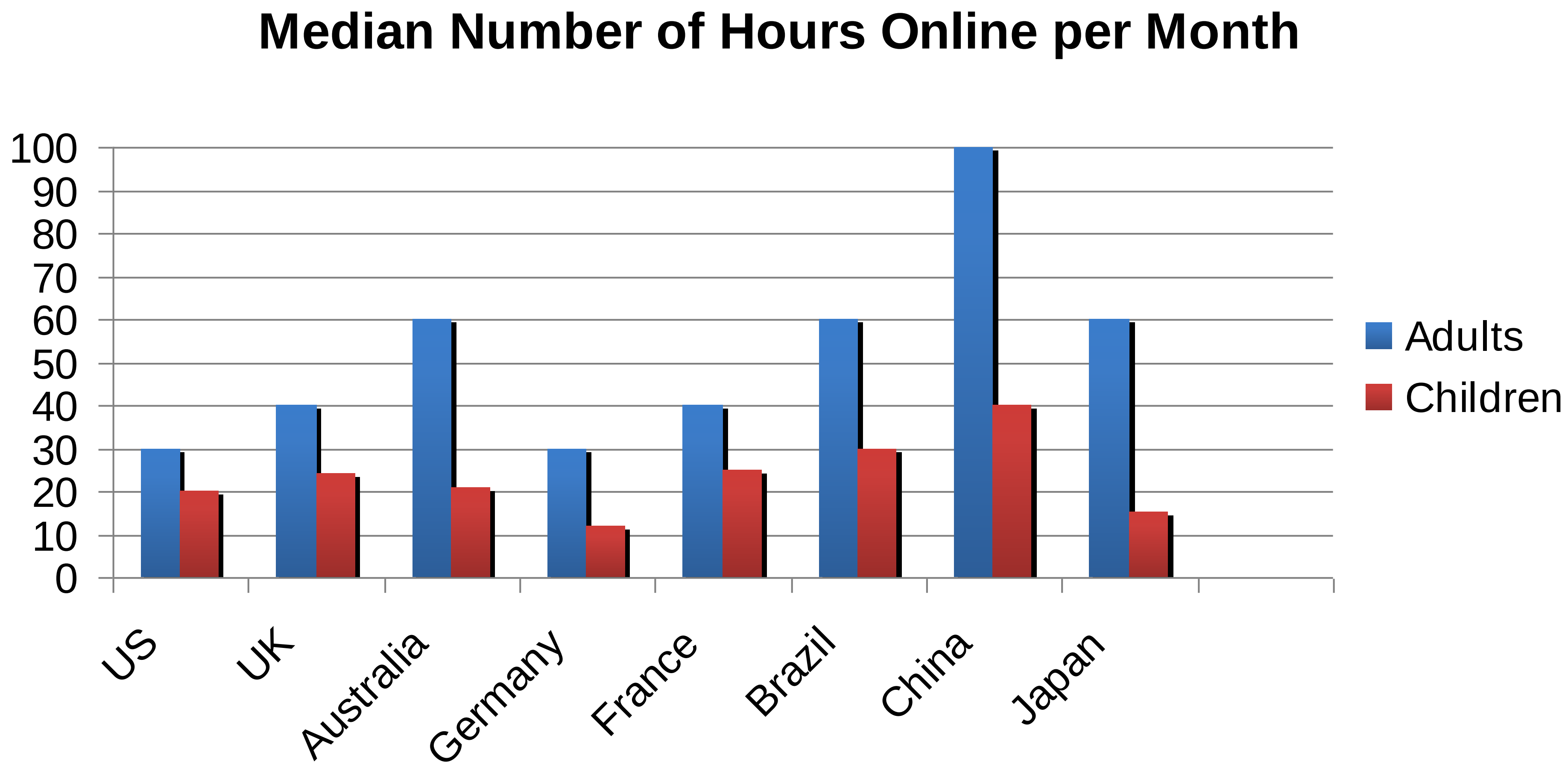
Perimeter Protection – Firewall, VPN, Encryption etc.

AntiVirus & Content Web & Gateway Security

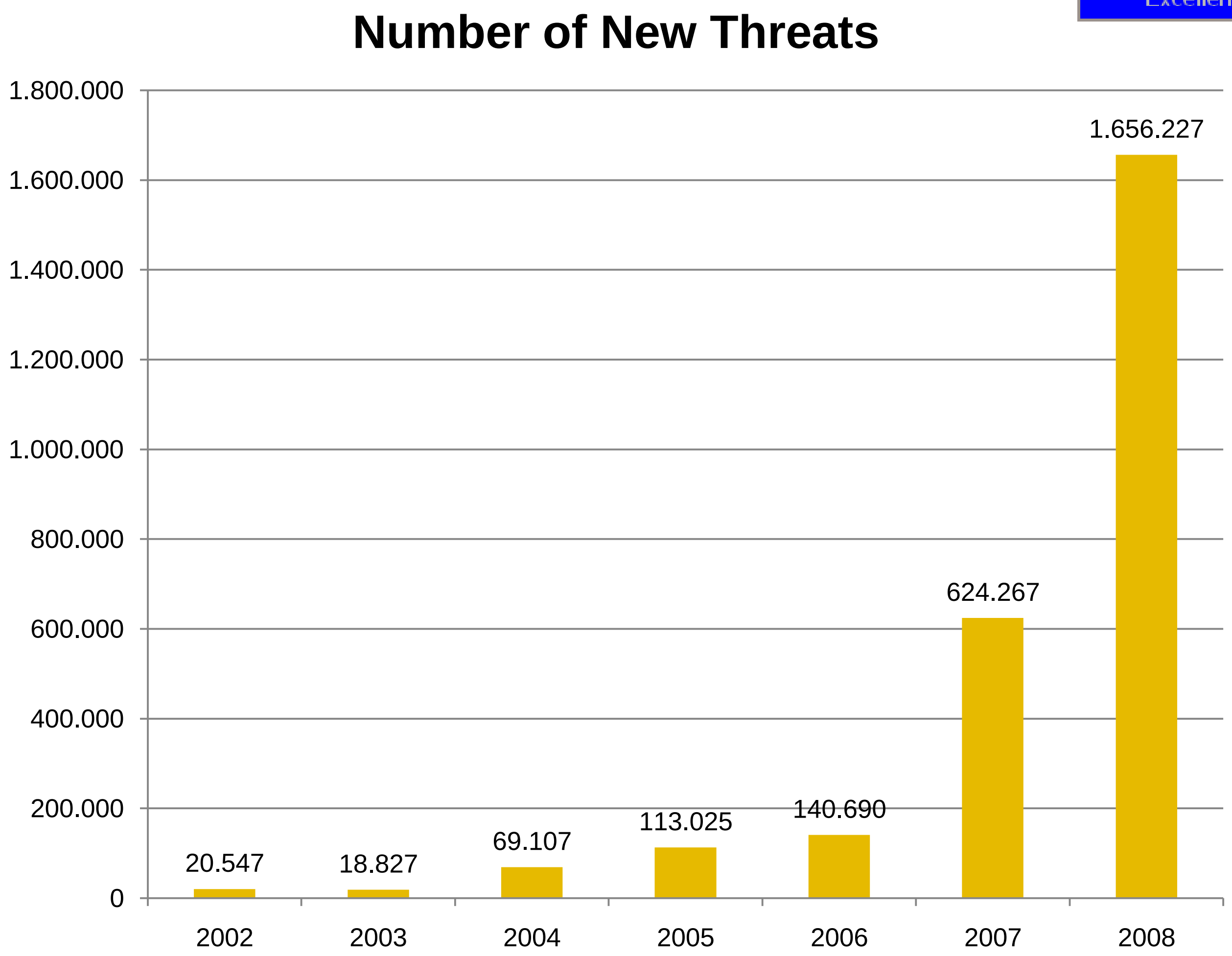
But they don't always work!



Users are the online security risk



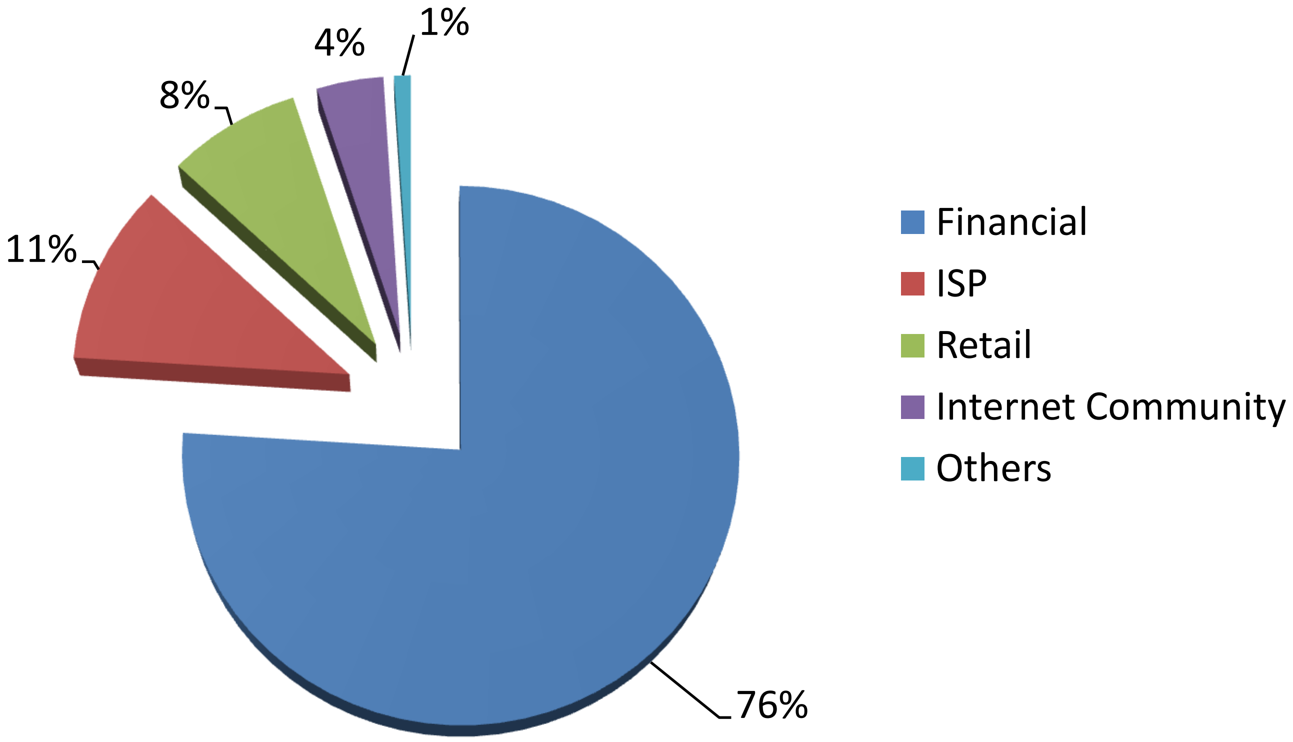
Malware threats continue to increase



Growth indicates customised production of new types of specialised items, for example to enable phishing.

Phishing

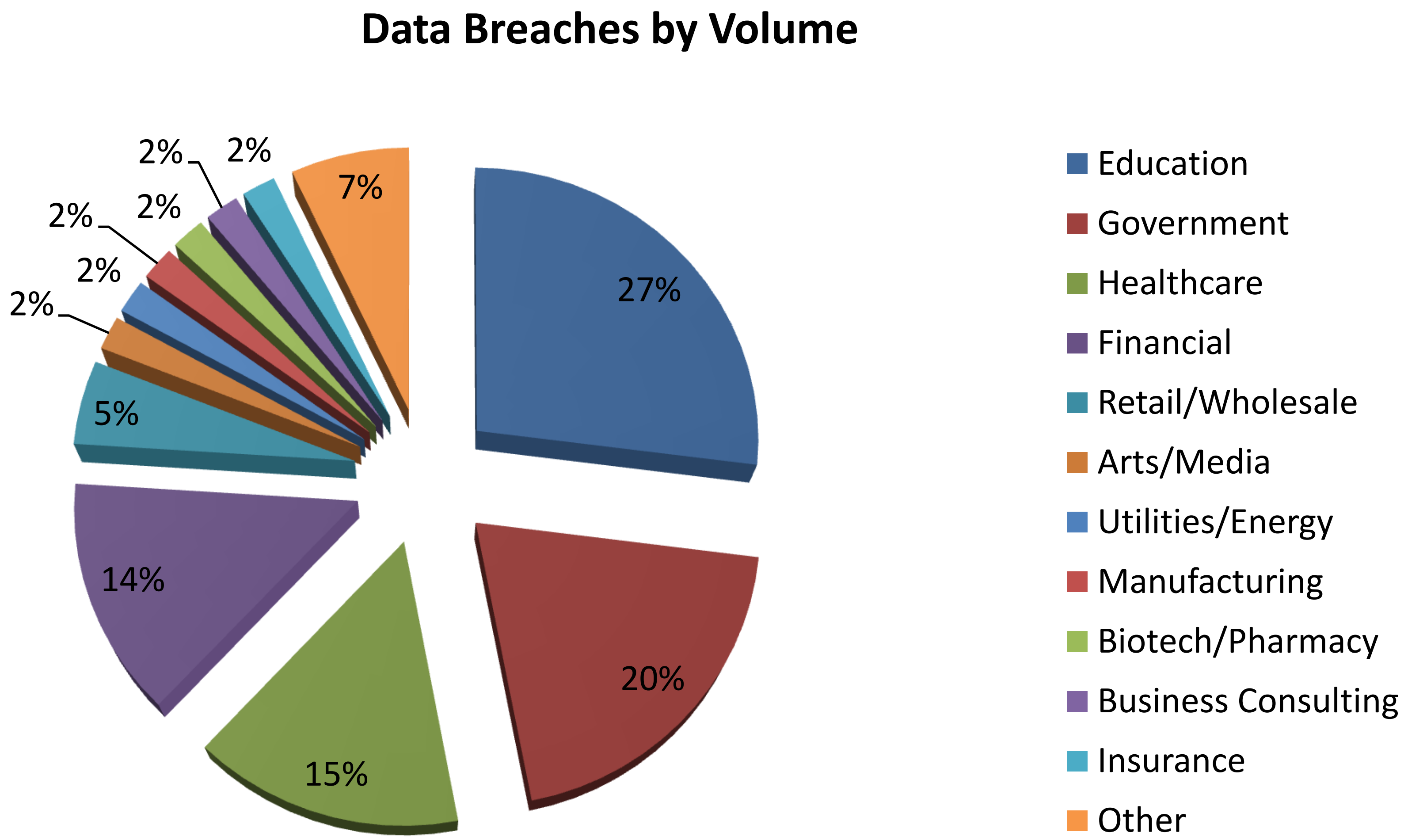
Phishing Volume by Sector



Data Losses by Sector

ExecIA LLP

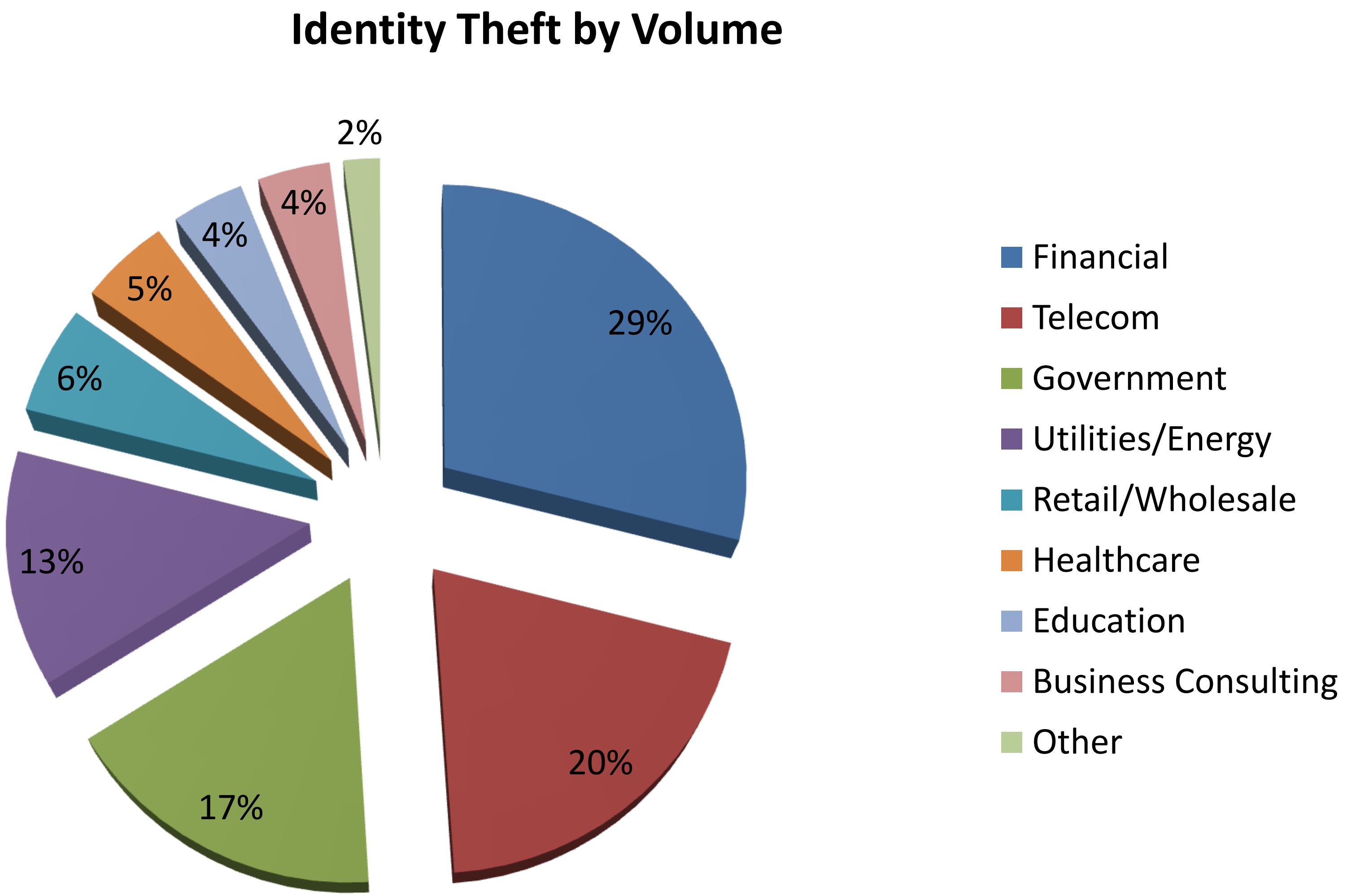
Excellence in Information Assurance



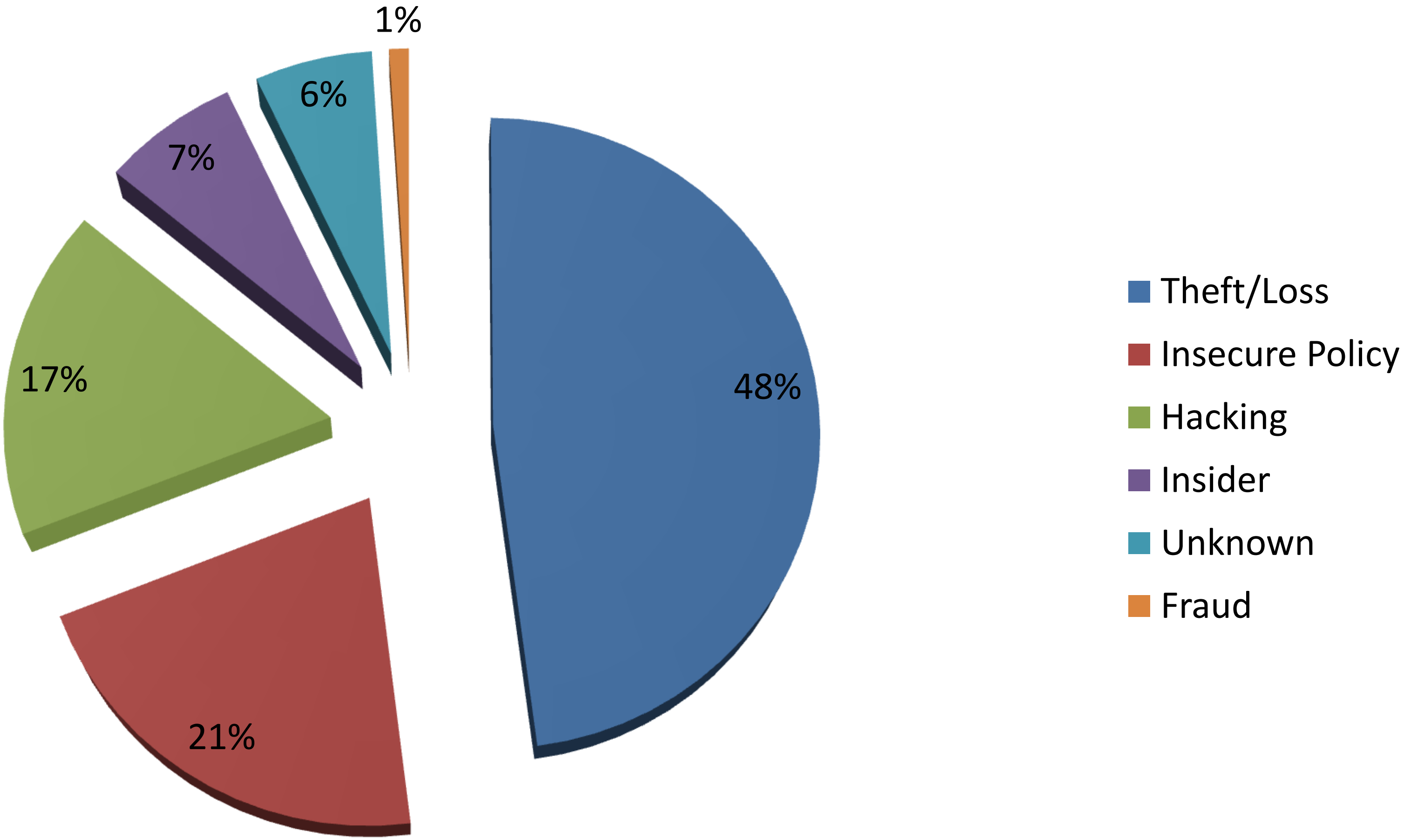
Identity Theft by Sector

ExecIA LLP

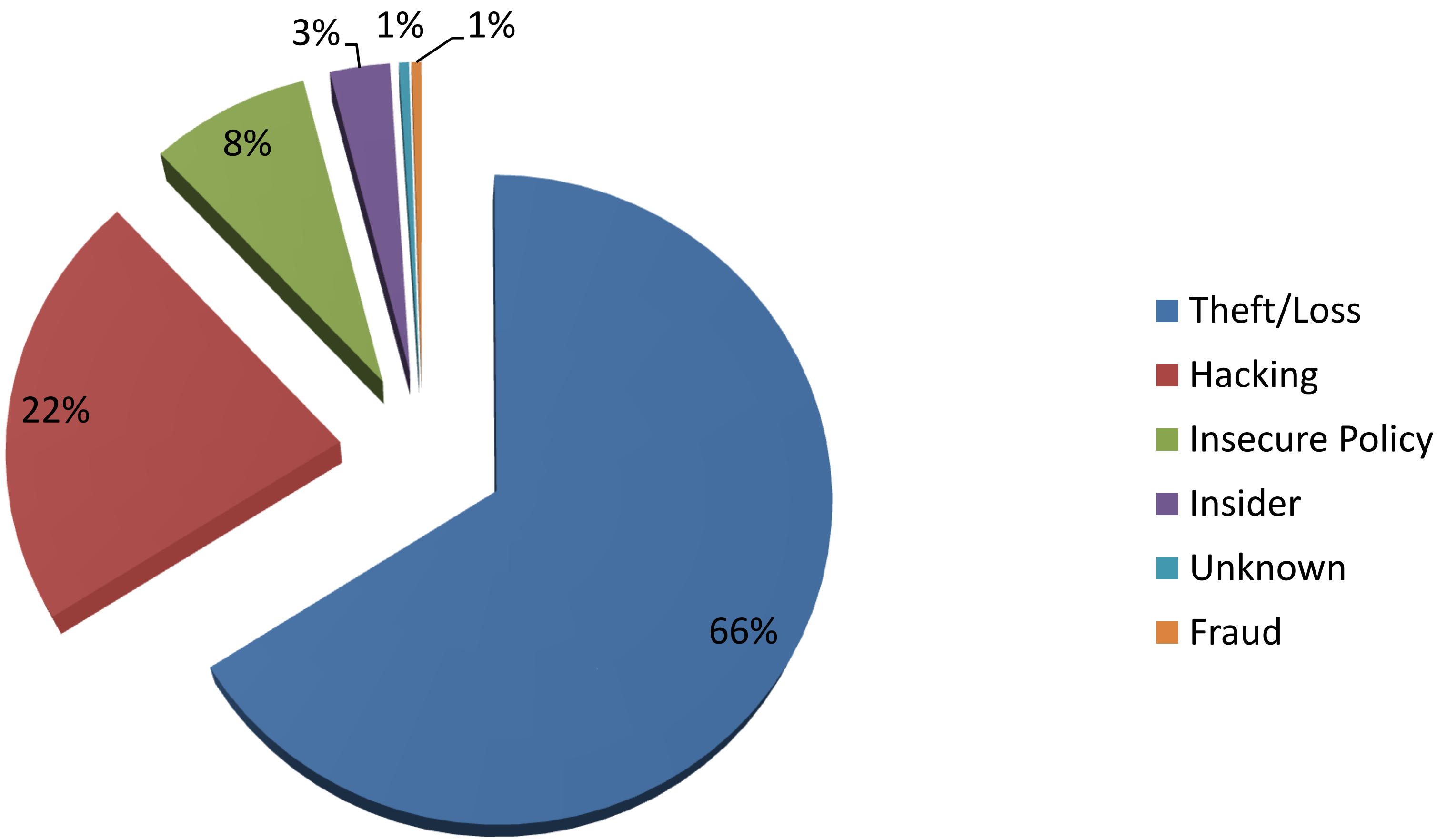
Excellence in Information Assurance



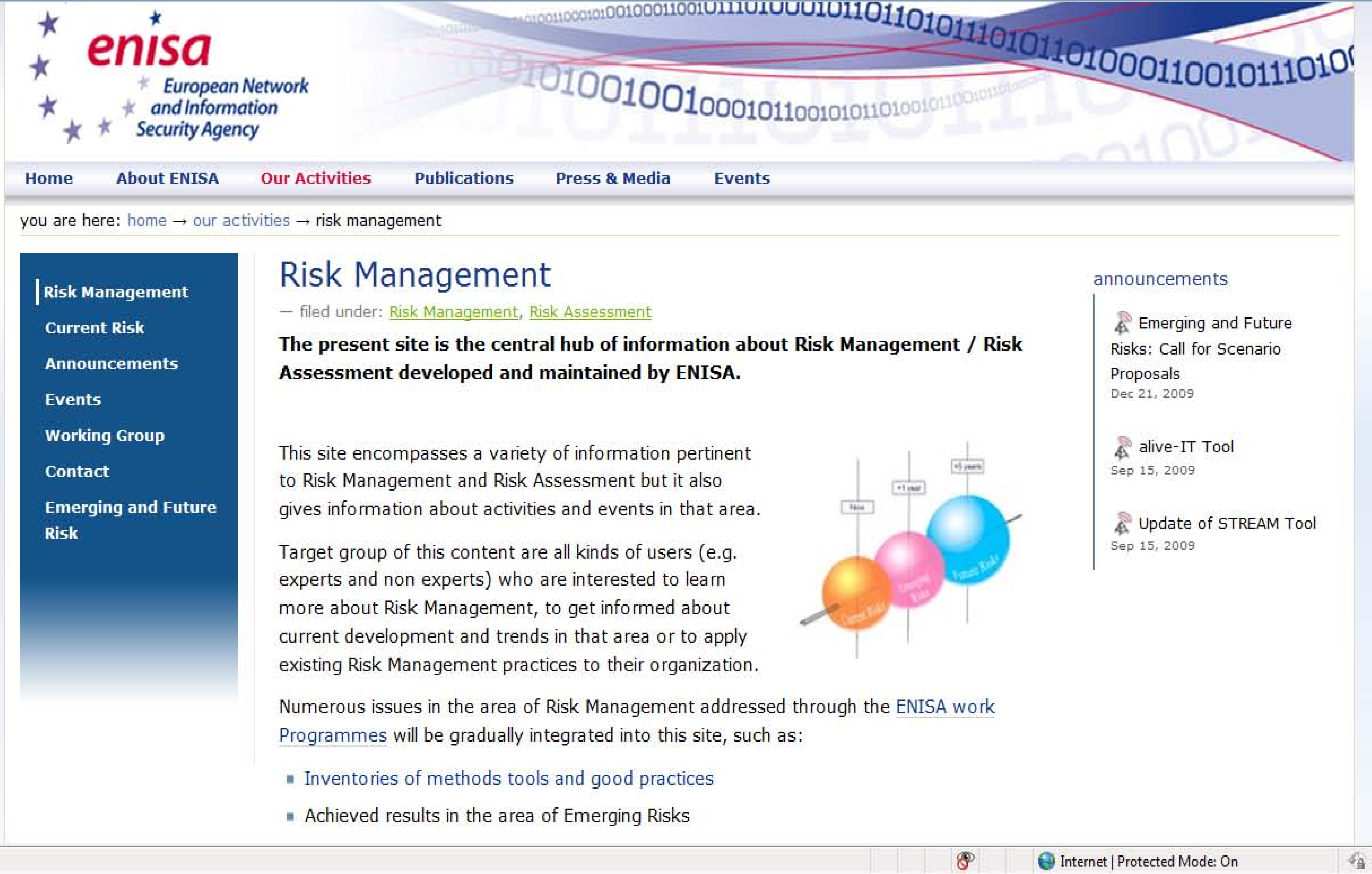
Causes of Data Loss



Causes of Identity Loss



ENISA Risk Management Website



you are here: home → our activities → risk management

Risk Management

— filed under: Risk Management, Risk Assessment

The present site is the central hub of information about Risk Management / Risk Assessment developed and maintained by ENISA.

This site encompasses a variety of information pertinent to Risk Management and Risk Assessment but it also gives information about activities and events in that area.

Target group of this content are all kinds of users (e.g. experts and non experts) who are interested to learn more about Risk Management, to get informed about current development and trends in that area or to apply existing Risk Management practices to their organization.

Numerous issues in the area of Risk Management addressed through the ENISA work Programmes will be gradually integrated into this site, such as:

- Inventories of methods tools and good practices
- Achieved results in the area of Emerging Risks

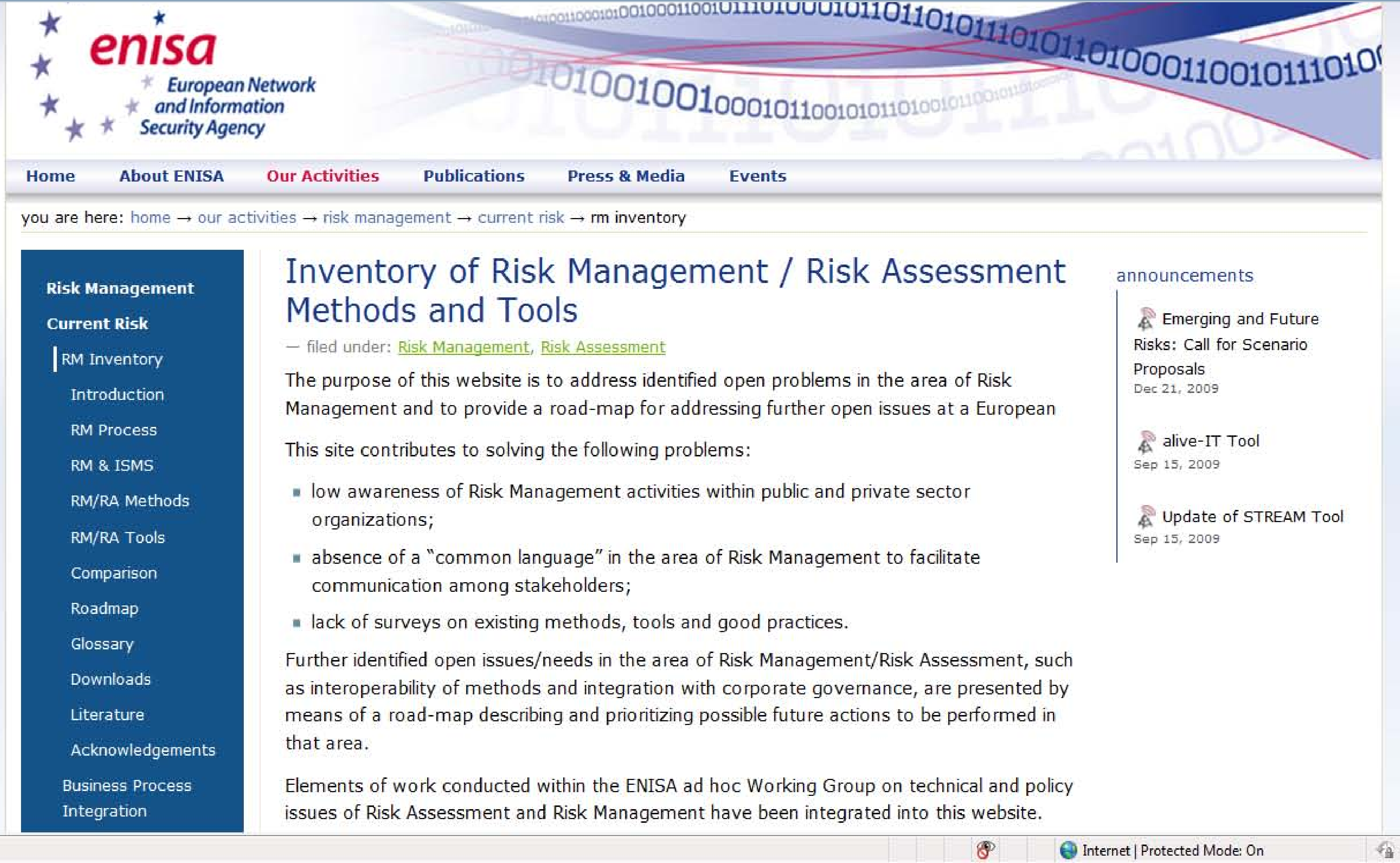
announcements

Emerging and Future Risks: Call for Scenario Proposals
Dec 21, 2009

alive-IT Tool
Sep 15, 2009

Update of STREAM Tool
Sep 15, 2009

ENISA Risk Management Methods



you are here: home → our activities → risk management → current risk → rm inventory

Inventory of Risk Management / Risk Assessment Methods and Tools

— filed under: Risk Management, Risk Assessment

The purpose of this website is to address identified open problems in the area of Risk Management and to provide a road-map for addressing further open issues at a European

This site contributes to solving the following problems:

- low awareness of Risk Management activities within public and private sector organizations;
- absence of a "common language" in the area of Risk Management to facilitate communication among stakeholders;
- lack of surveys on existing methods, tools and good practices.

Further identified open issues/needs in the area of Risk Management/Risk Assessment, such as interoperability of methods and integration with corporate governance, are presented by means of a road-map describing and prioritizing possible future actions to be performed in that area.

Elements of work conducted within the ENISA ad hoc Working Group on technical and policy issues of Risk Assessment and Risk Management have been integrated into this website.

announcements

Emerging and Future Risks: Call for Scenario Proposals
Dec 21, 2009

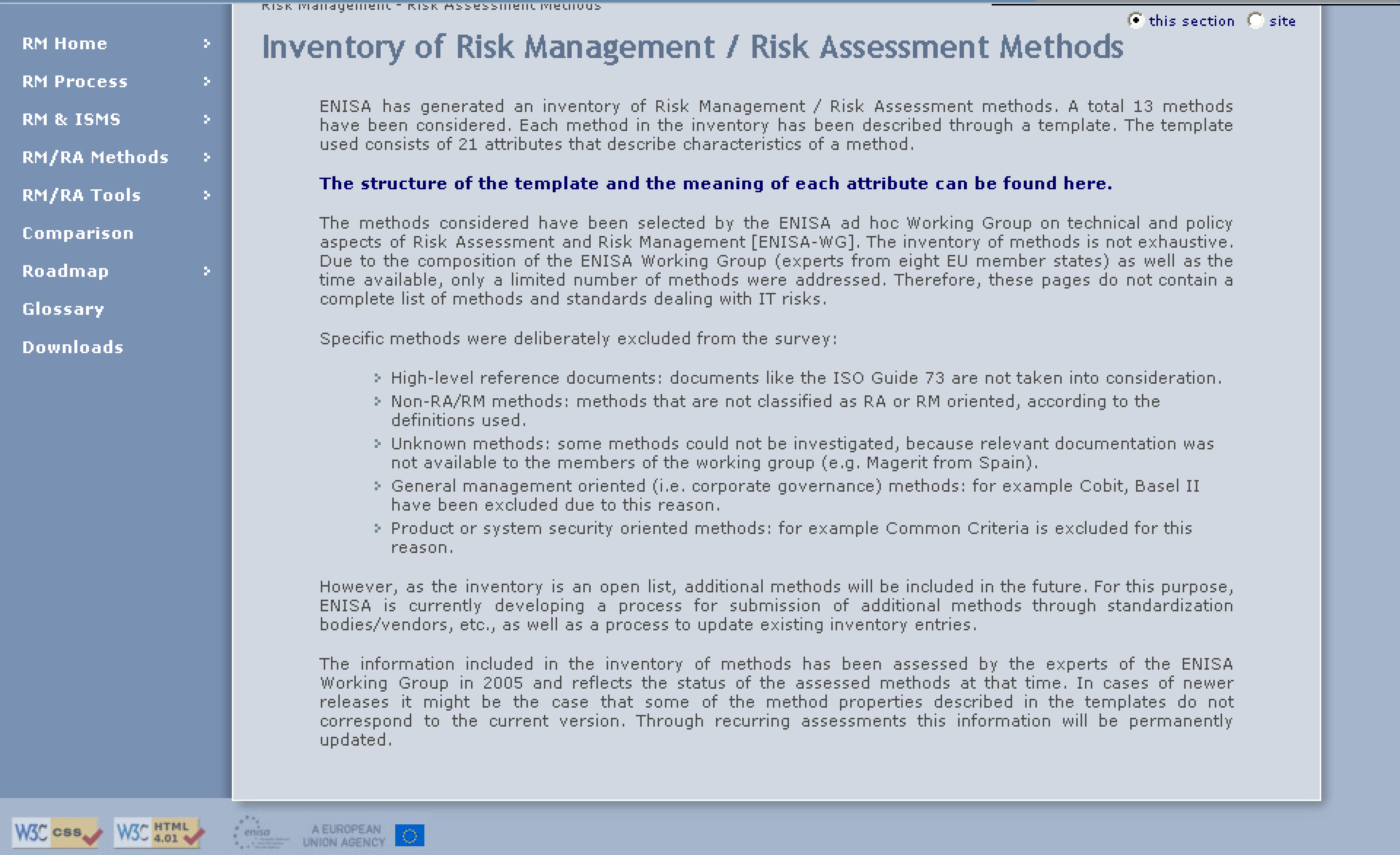
alive-IT Tool
Sep 15, 2009

Update of STREAM Tool
Sep 15, 2009

ENISA Risk Management

ExecIA LLP

Excellence in Information Assurance



Risk Management - Risk Assessment Methods

● this section ○ site

Inventory of Risk Management / Risk Assessment Methods

ENISA has generated an inventory of Risk Management / Risk Assessment methods. A total 13 methods have been considered. Each method in the inventory has been described through a template. The template used consists of 21 attributes that describe characteristics of a method.

The structure of the template and the meaning of each attribute can be found here.

The methods considered have been selected by the ENISA ad hoc Working Group on technical and policy aspects of Risk Assessment and Risk Management [ENISA-WG]. The inventory of methods is not exhaustive. Due to the composition of the ENISA Working Group (experts from eight EU member states) as well as the time available, only a limited number of methods were addressed. Therefore, these pages do not contain a complete list of methods and standards dealing with IT risks.

Specific methods were deliberately excluded from the survey:

- High-level reference documents: documents like the ISO Guide 73 are not taken into consideration.
- Non-RA/RM methods: methods that are not classified as RA or RM oriented, according to the definitions used.
- Unknown methods: some methods could not be investigated, because relevant documentation was not available to the members of the working group (e.g. Magerit from Spain).
- General management oriented (i.e. corporate governance) methods: for example Cobit, Basel II have been excluded due to this reason.
- Product or system security oriented methods: for example Common Criteria is excluded for this reason.

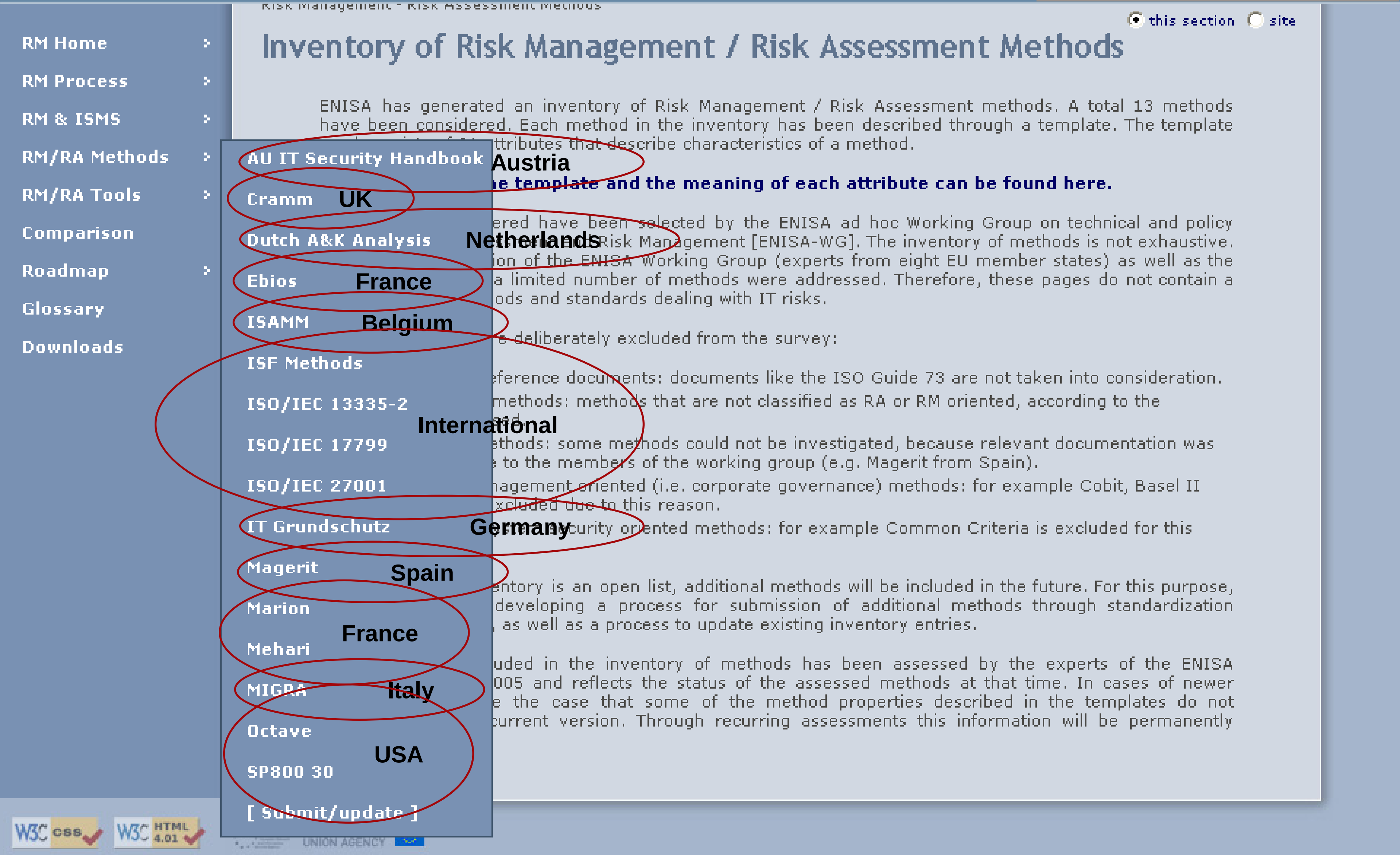
However, as the inventory is an open list, additional methods will be included in the future. For this purpose, ENISA is currently developing a process for submission of additional methods through standardization bodies/vendors, etc., as well as a process to update existing inventory entries.

The information included in the inventory of methods has been assessed by the experts of the ENISA Working Group in 2005 and reflects the status of the assessed methods at that time. In cases of newer releases it might be the case that some of the method properties described in the templates do not correspond to the current version. Through recurring assessments this information will be permanently updated.

ENISA Risk Management Methods

ExecIA LLP

Excellence in Information Assurance



Risk Management - Risk Assessment Methods

● this section ○ site

Inventory of Risk Management / Risk Assessment Methods

- RM Home
- RM Process
- RM & ISMS
- RM/RA Methods
- RM/RA Tools
- Comparison
- Roadmap
- Glossary
- Downloads

- AU IT Security Handbook
- Cramm
- Dutch A&K Analysis
- Ebios
- ISAMM
- ISF Methods
- ISO/IEC 13335-2
- ISO/IEC 17799
- ISO/IEC 27001
- IT Grundschutz
- Magerit
- Marion
- Mehari
- MIGRA
- Octave
- SP800 30
- [Submit/update]

ENISA has generated an inventory of Risk Management / Risk Assessment methods. A total 13 methods have been considered. Each method in the inventory has been described through a template. The template ttributes that describe characteristics of a method.

e template and the meaning of each attribute can be found here.

ered have been selected by the ENISA ad hoc Working Group on technical and policy Risk Management [ENISA-WG]. The inventory of methods is not exhaustive. ion of the ENISA Working Group (experts from eight EU member states) as well as the a limited number of methods were addressed. Therefore, these pages do not contain a ods and standards dealing with IT risks.

e deliberately excluded from the survey:

eference documents: documents like the ISO Guide 73 are not taken into consideration.

methods: methods that are not classified as RA or RM oriented, according to the

ethods: some methods could not be investigated, because relevant documentation was e to the members of the working group (e.g. Magerit from Spain).

nagement oriented (i.e. corporate governance) methods: for example Cobit, Basel II xcluded due to this reason.

ecurity oriented methods: for example Common Criteria is excluded for this

entory is an open list, additional methods will be included in the future. For this purpose, developing a process for submission of additional methods through standardization as well as a process to update existing inventory entries.

uded in the inventory of methods has been assessed by the experts of the ENISA 005 and reflects the status of the assessed methods at that time. In cases of newer e the case that some of the method properties described in the templates do not current version. Through recurring assessments this information will be permanently

UNION AGENCY

W3C CSS ✓ W3C HTML 4.01 ✓

ENISA Risk Management Method Descriptions

R.A. Method phases supported

- Risk identification : The handbook contains a generic description of RA, but does not specify a special method
- Risk analysis
- Risk evaluation

R.M. Method phases supported

- Risk assessment: Part 1, chapter 4
- Risk treatment : Part 1, chapter 5.1, part 2
- Risk acceptance : Part 1, chapter 5.2
- Risk communication : Part1, chapters 5.5 and 6.2

Brief description of the product

- The Austrian IT Security Handbook consists of 2 parts. Part 1 gives a detailed description of the IT security management process, including development of security policies, risk analysis, design of security concepts, implementation of the security plan and follow-up activities. Part 2 is a collection of 230 baseline security measures. A tool supporting the implementation is available as a prototype. The Austrian IT Security Handbook was originally developed for government organizations, and is now available for all types of business. The handbook is compliant with ISO/IEC IS 13335, the German IT-Grundschutzhandbuch and partly with ISO/IEC IS 17799.

Lifecycle

Date of the first edition, date and number of actual version

Date of first release : 1998
Date and identification of the last version : Version 2.2, November 2004

Useful links

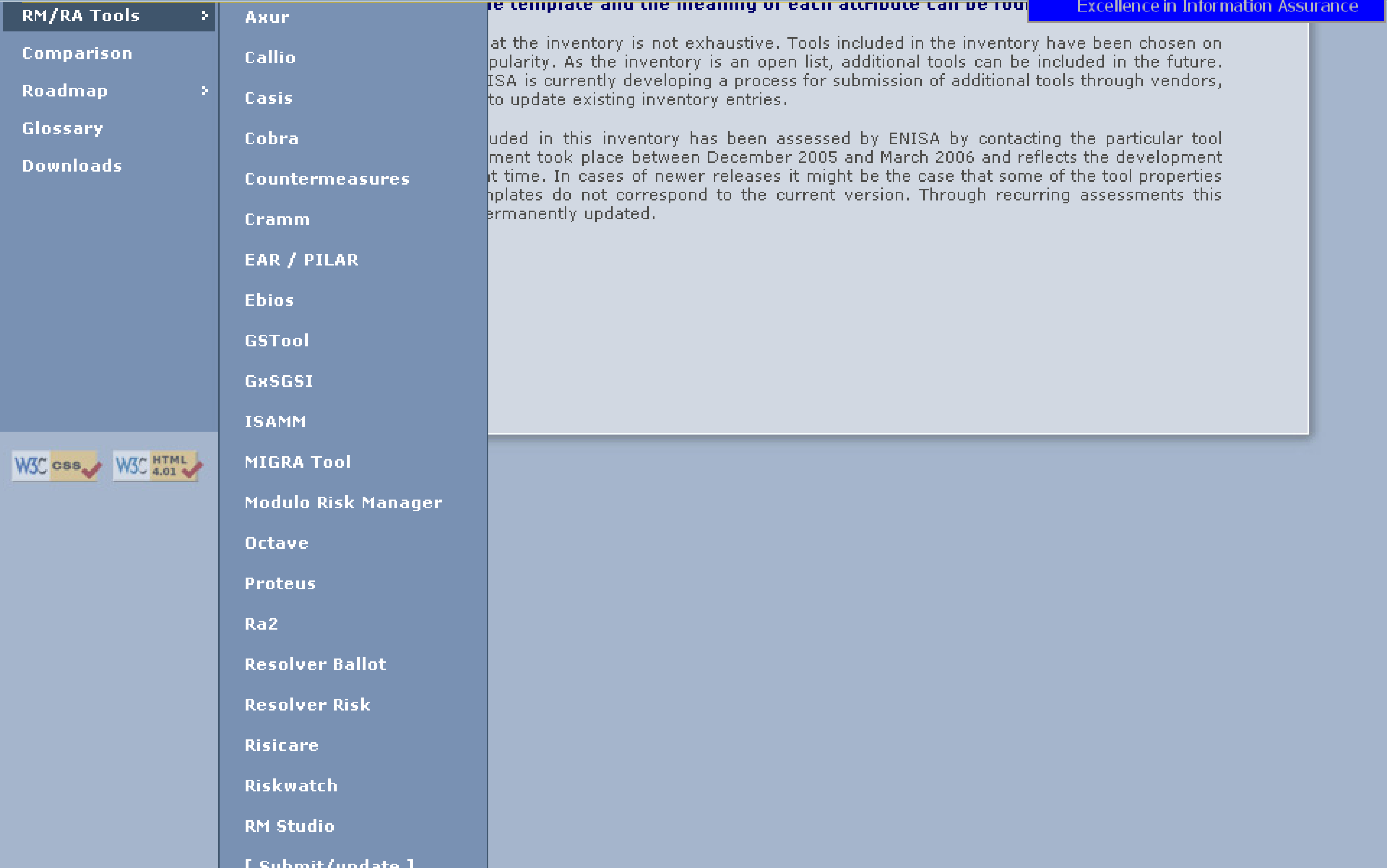
Link for further information

Official web site : http://www.cio.gv.at/securenetworks/sihb/
User group web site : N/A
Relevant web site : N/A

ENISA Risk Management Tools

ExecIA LLP

Excellence in Information Assurance



e template and the meaning of each attribute can be fou

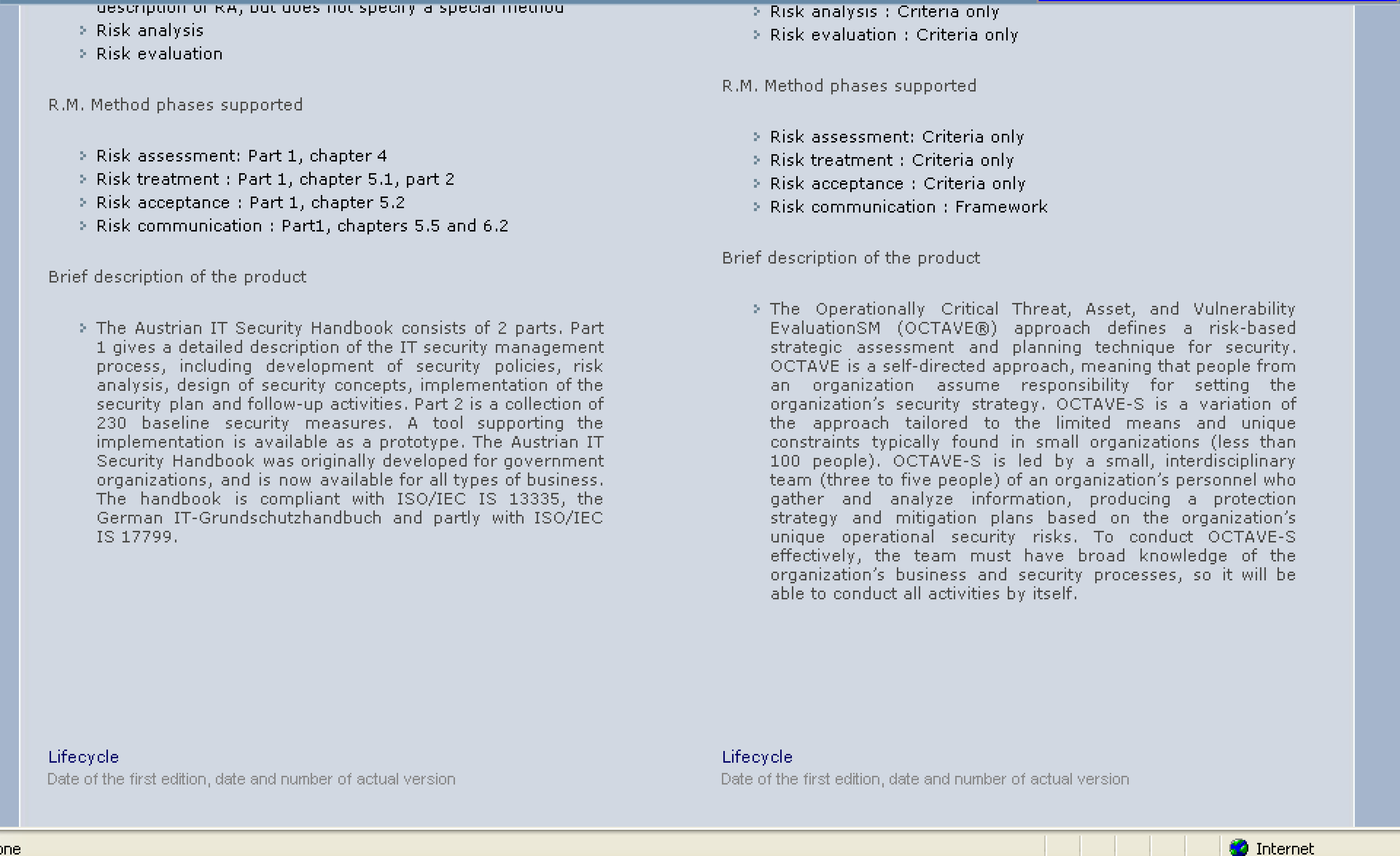
at the inventory is not exhaustive. Tools included in the inventory have been chosen on pularity. As the inventory is an open list, additional tools can be included in the future. ISA is currently developing a process for submission of additional tools through vendors, to update existing inventory entries.

uded in this inventory has been assessed by ENISA by contacting the particular tool ment took place between December 2005 and March 2006 and reflects the development it time. In cases of newer releases it might be the case that some of the tool properties nplates do not correspond to the current version. Through recurring assessments this ermanently updated.

ENISA Risk Management Method Comparison

ExecIA LLP

Excellence in Information Assurance



description of RA, but does not specify a special method

- Risk analysis
- Risk evaluation

R.M. Method phases supported

- Risk assessment: Part 1, chapter 4
- Risk treatment : Part 1, chapter 5.1, part 2
- Risk acceptance : Part 1, chapter 5.2
- Risk communication : Part1, chapters 5.5 and 6.2

Brief description of the product

- The Austrian IT Security Handbook consists of 2 parts. Part 1 gives a detailed description of the IT security management process, including development of security policies, risk analysis, design of security concepts, implementation of the security plan and follow-up activities. Part 2 is a collection of 230 baseline security measures. A tool supporting the implementation is available as a prototype. The Austrian IT Security Handbook was originally developed for government organizations, and is now available for all types of business. The handbook is compliant with ISO/IEC IS 13335, the German IT-Grundschutzhandbuch and partly with ISO/IEC IS 17799.

Lifecycle

Date of the first edition, date and number of actual version

- Risk analysis : Criteria only
- Risk evaluation : Criteria only

R.M. Method phases supported

- Risk assessment: Criteria only
- Risk treatment : Criteria only
- Risk acceptance : Criteria only
- Risk communication : Framework

Brief description of the product

- The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

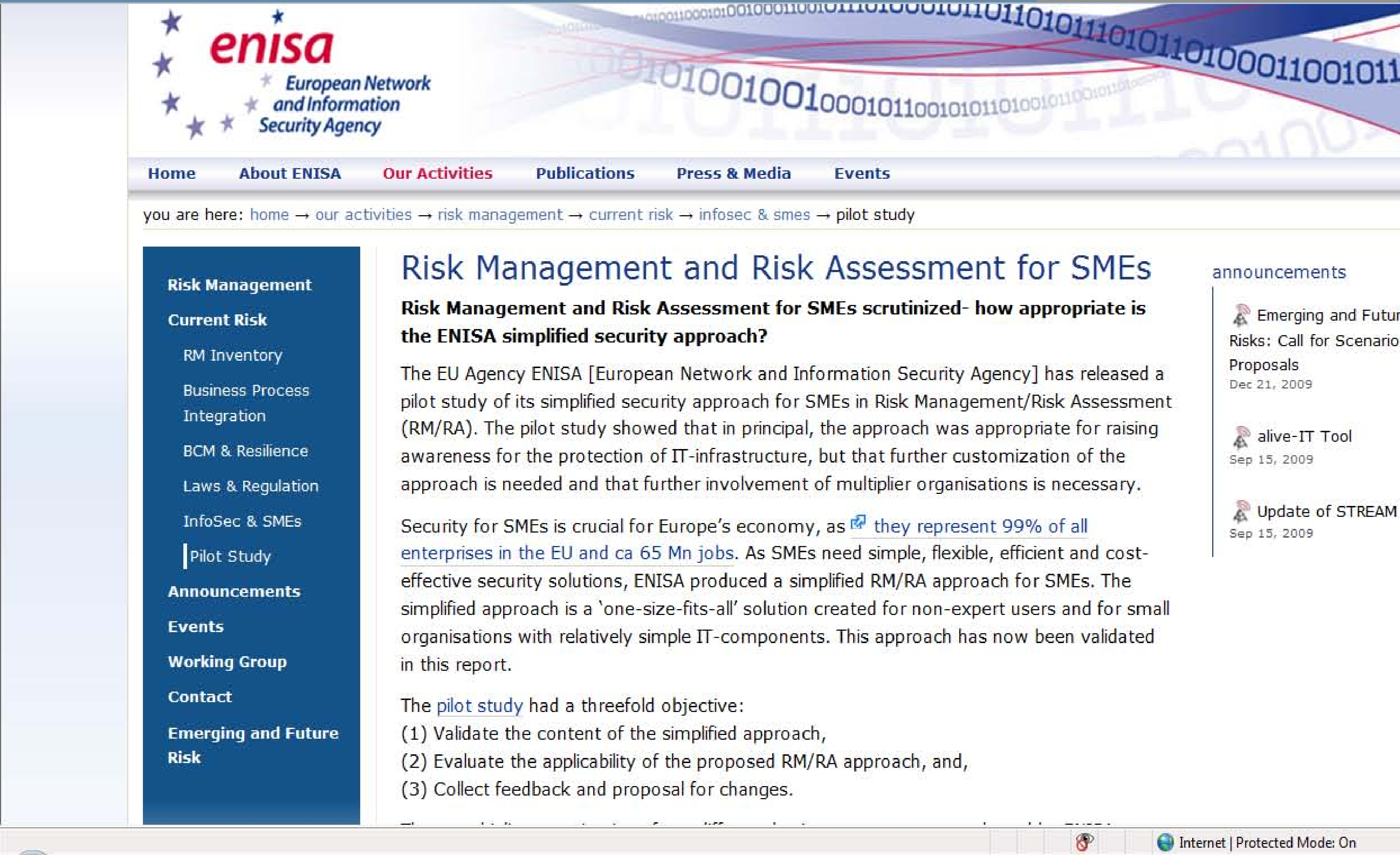
Lifecycle

Date of the first edition, date and number of actual version

ENISA Risk Management for SMEs

ExecIA LLP

Excellence in Information Assurance



you are here: home → our activities → risk management → current risk → infosec & smes → pilot study

Risk Management and Risk Assessment for SMEs

Risk Management and Risk Assessment for SMEs scrutinized- how appropriate is the ENISA simplified security approach?

The EU Agency ENISA [European Network and Information Security Agency] has released a pilot study of its simplified security approach for SMEs in Risk Management/Risk Assessment (RM/RA). The pilot study showed that in principal, the approach was appropriate for raising awareness for the protection of IT-infrastructure, but that further customization of the approach is needed and that further involvement of multiplier organisations is necessary.

Security for SMEs is crucial for Europe's economy, as they represent 99% of all enterprises in the EU and ca 65 Mn jobs. As SMEs need simple, flexible, efficient and cost-effective security solutions, ENISA produced a simplified RM/RA approach for SMEs. The simplified approach is a 'one-size-fits-all' solution created for non-expert users and for small organisations with relatively simple IT-components. This approach has now been validated in this report.

The pilot study had a threefold objective:
(1) Validate the content of the simplified approach,
(2) Evaluate the applicability of the proposed RM/RA approach, and,
(3) Collect feedback and proposal for changes.

announcements

Emerging and Futur Risks: Call for Scenario Proposals
Dec 21, 2009

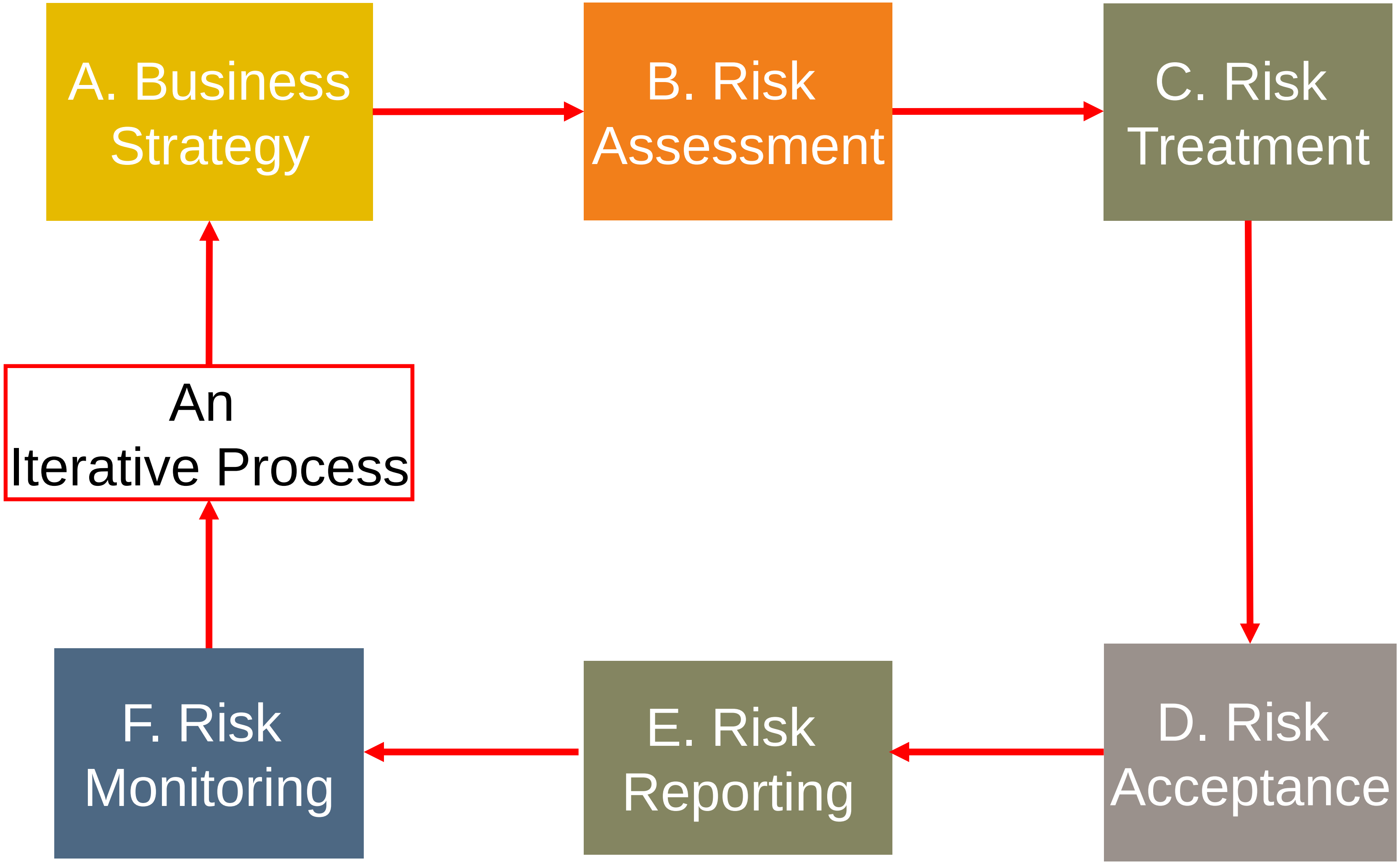
alive-IT Tool
Sep 15, 2009

Update of STREAM
Sep 15, 2009

Basic Risk Management

ExecIA LLP

Excellence in Information Assurance



A. Business Strategy

B. Risk Assessment

C. Risk Treatment

D. Risk Acceptance

E. Risk Reporting

F. Risk Monitoring

An Iterative Process

System consists of 15 Processes

- Stage A: Business strategy:
  - P.1 Definition of external environment
  - P.2 Definition of internal environment
  - P.3 Generation of risk management context
  - P.4 Formulation of impact limit criteria
- Stage B: Risk assessment:
  - P.5 Identification of risks
  - P.6 Analysis of relevant risks
  - P.7 Evaluation of risks
- Stage C: Risk treatment:
  - P.8 Identification of options
  - P.9 Development of action plan
  - P.10 Approval of action plan
  - P.11 Implementation of action plan
  - P.12 Identification of residual risks
- Stage D: Risk acceptance:
  - P.13 Risk acceptance
- Stage E: Risk reporting and monitoring:
  - P.14 Risk monitoring and reporting
  - P.15 Risk communication, awareness and consulting

Each Process has an Input and an Output

Example input

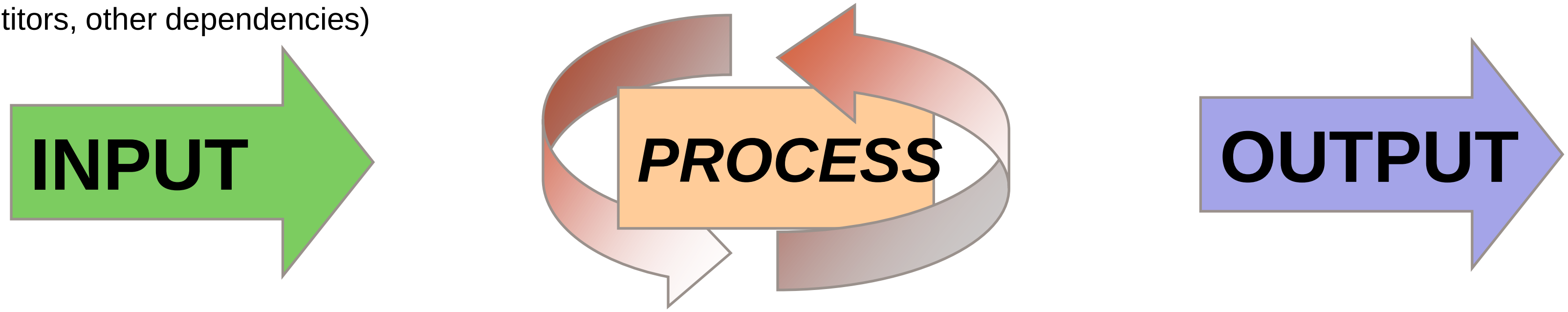
- Market information (market indicators, competitive information, etc.)
- Financial & political information
- Relevant legal and regulatory information
- Information about geographical, social and cultural conditions
- Information about external stakeholders (values and perception) (Note: partners, competitors, other dependencies)

Example process

Definition of external environment

Example output

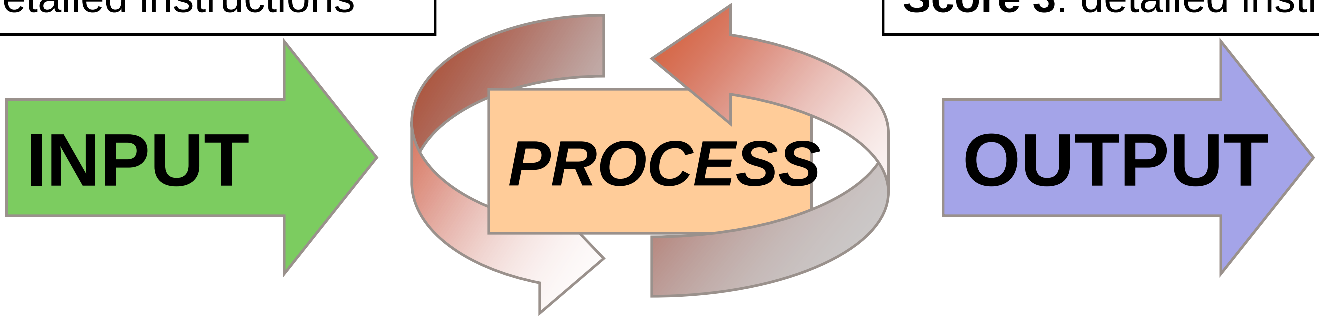
- All records of the external environment of the organization
- List of relevant obligatory laws and regulations (with respect to obligations)
- Various lists with applicable rules (social, cultural, values etc.)



Characterising the Methods

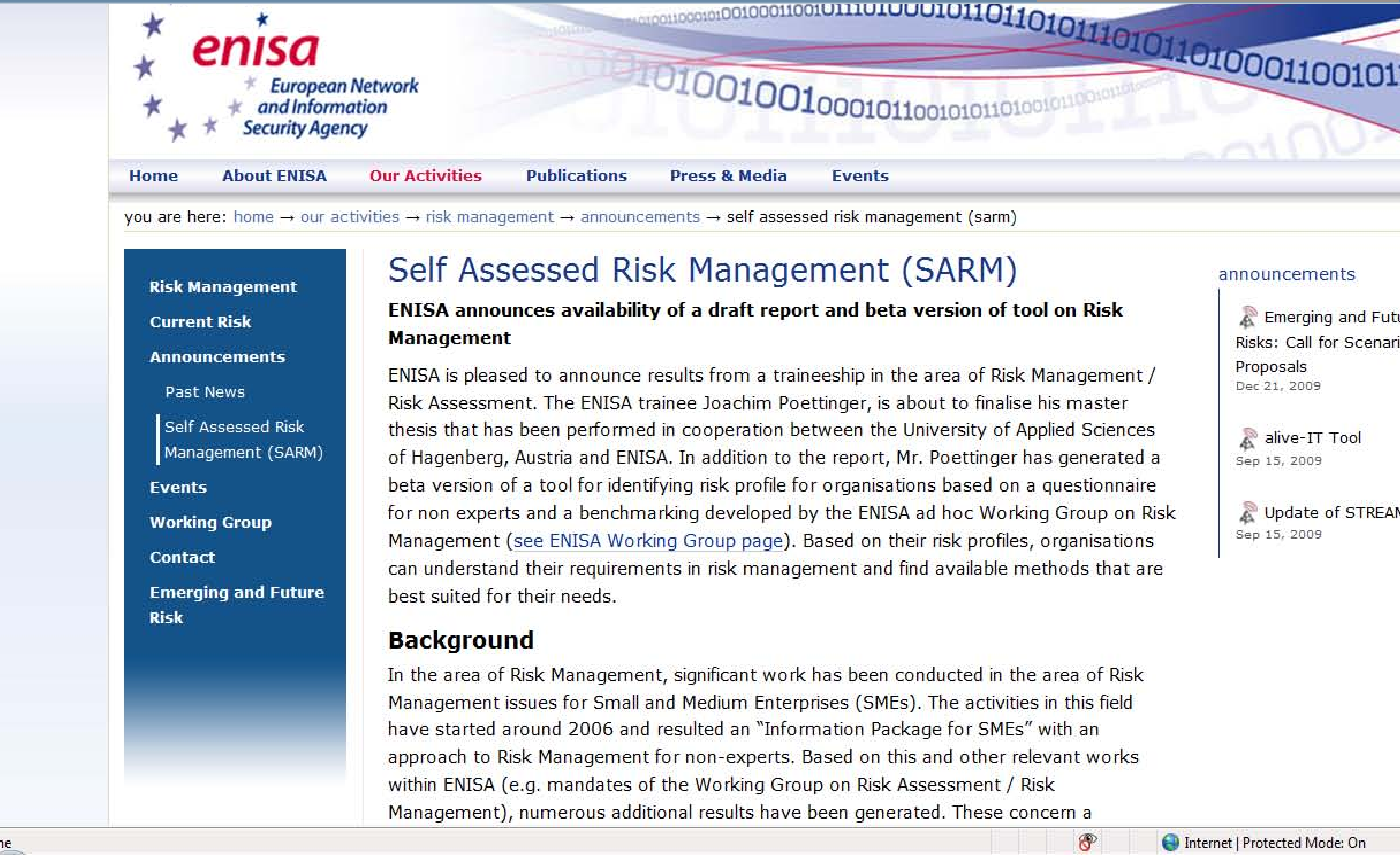
Input Score:
Score 0: not mentioned
Score 1: external reference only
Score 2: simple description only
Score 3: detailed instructions

Output Score:
Score 0: not mentioned
Score 1: external reference only
Score 2: simple description only
Score 3: detailed instructions



Process Score =
Sum of Input Score +
Output Score

ENISA Risk Profiler



Self Assessed Risk Management (SARM)

ENISA announces availability of a draft report and beta version of tool on Risk Management

ENISA is pleased to announce results from a traineeship in the area of Risk Management / Risk Assessment. The ENISA trainee Joachim Poettinger, is about to finalise his master thesis that has been performed in cooperation between the University of Applied Sciences of Hagenberg, Austria and ENISA. In addition to the report, Mr. Poettinger has generated a beta version of a tool for identifying risk profile for organisations based on a questionnaire for non experts and a benchmarking developed by the ENISA ad hoc Working Group on Risk Management (see ENISA Working Group page). Based on their risk profiles, organisations can understand their requirements in risk management and find available methods that are best suited for their needs.

Background

In the area of Risk Management, significant work has been conducted in the area of Risk Management issues for Small and Medium Enterprises (SMEs). The activities in this field have started around 2006 and resulted an "Information Package for SMEs" with an approach to Risk Management for non-experts. Based on this and other relevant works within ENISA (e.g. mandates of the Working Group on Risk Assessment / Risk Management), numerous additional results have been generated. These concern a

Assessing Exposure to Threats and Vulnerabilities

- Business exposure:
  - Size and complexity of the business
  - Attitude to change.
- Exposure to problems:
  - Likelihood of technical problems
  - Likelihood of problems caused by people
  - Likelihood that people have the knowledge & means to cause problems.
- Use of IT:
  - Complexity of IT systems
  - Importance of Internet to the business
  - Partner access to your network
  - Home and remote access to your network.

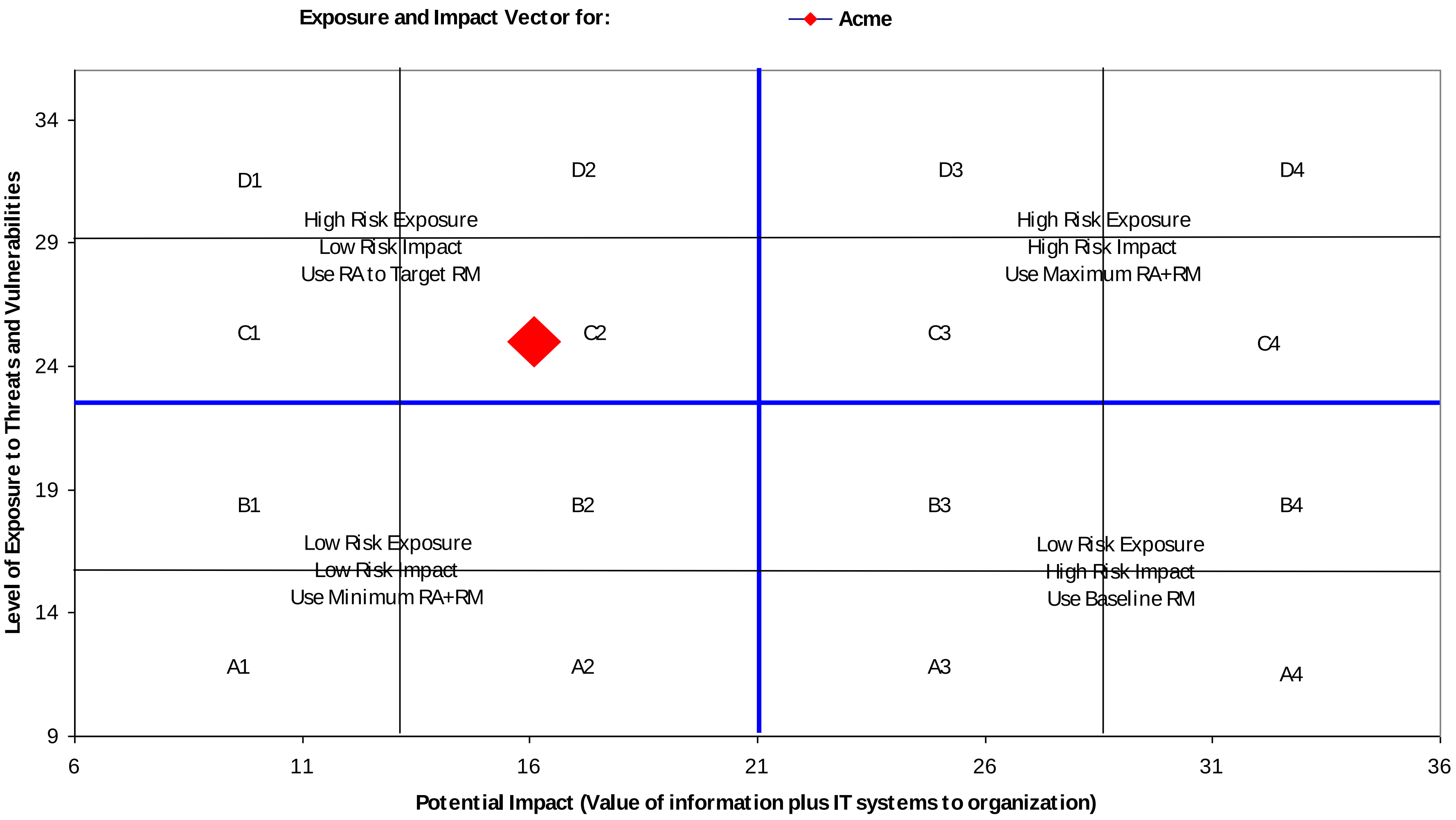
Assessing Potential Impact

- Importance of legal and regulatory requirements to your business.
- Value of information to your business:
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality.
- Value of IT systems to your business:
  - Importance in enabling you to achieve objectives
  - Importance of your systems to your business partners.

Which method do you need?

ExecIA LLP

Excellence in Information Assurance



Example Approach (Level 2)

- General Information:
  - Basic understanding of risks and some investment in resources.
- Degree of Action:
  - Basic concern with a few processes, focusing on risk treatment.
- Requirements:
  - Understanding information assets.
  - Understanding stakeholders and organization.
  - Understanding risk acceptability and strategy for managing this.
  - Identifying business strategies relevant to risk management.
  - Understanding basic threats and impacts and having a simple plan to deal with these.

Example Recommendations (Level 2)

- Use basic guides to good practice and keep simple checklists.
- Coordinate and cost the actions to be taken.
- Prioritize actions to be taken.
- Assign responsibility for carrying out actions.
- Produce basic reports about the actions carried out.

ExecIA LLP

Excellence in Information Assurance

Thank You!

Jeremy Ward

Jeremy.ward@execia.com

+44 7768 287 026