EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONTACT

AUTHORS

Sławomir Górniak

LEGAL NOTICE

COPYRIGHT NOTICE

1.1 THE PURPOSE OF THIS DOCUMENT

Risk Management is all about identifying and protecting the valuable assets of an organisation. Risk management procedures are fundamental processes to prepare organisations for a future cybersecurity attack, to evaluate products and services for their resistance to potential attacks before placing them on the market, and to prevent supply chain fraud.

*"ENISA shall facilitate the establishment and take-up of European and international standards for **risk management** and for the security of ICT products, ICT services and ICT processes".*

1.2 EU LEGAL REQUIREMENTS

risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems

Table 1: References on risk management in the NIS directive

Article	Point	Text

	a risk assessment plan to identify risks.

Table 2: References on risk management in the CSA

CSA items	**Cybersecurity Act Regulation - Regulation (EU) 2019/881**
Risk management as a tool for cybersecurity vulnerability management and remediation	**In many cases, identifying and documenting such dependencies enables end users of mans.12 fooCd 0 -1s a(v)13.3 (i)2 (c.3 (s)-1 Tw 5.12 030 TdT0.0)0.7 (o)0.39 ((i)7( )13.4 (o)1 (n)0.7 (g)s.6**

Regulation (EU) No 910/2014
Regulation (EU) 2016/679
Directive (EU) 2015/2366
Directive (EU) 2015/849
Directive 2014/53/EU (RED)

Table 4: non-exhaustive list of proposed EU legislative acts containing risk management

1.3 ENISA WORK ON RISK MANAGEMENT

Table 5: Non-exhaustive list of relevant ENISA publications

Editor	Publication name

2.1 SCOPE OF THE ANALYSIS

ENISA shall facilitate the establishment and take-up of European and international standards for risk management

2.2 NEEDS OF STAKEHOLDERS IN RELATION TO RISK MANAGEMENT

2.3 DEFINITIONS

2.3.1 Risk management

Risk

Table 6: Comparison of risk definitions in ISO standards and directives

Effect of uncertainty on objectives	Effect on uncertainty

Risk management

Risk assessment

Risk treatment

2.3.2 Standards and methodologies

standard

methodology

relation

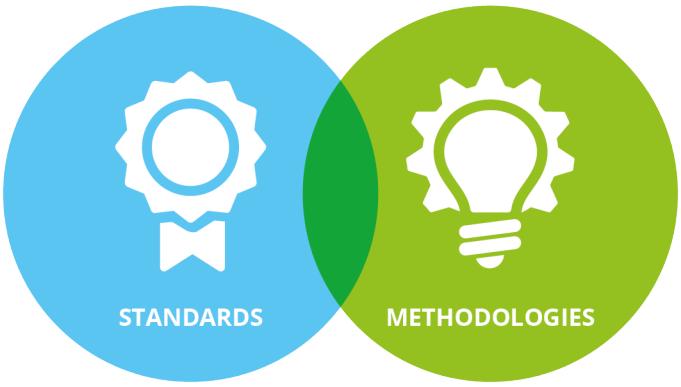


Table 7: Examples of methodologies, which are published as standards

2.4 ROLE OF RISK MANAGEMENT STANDARDS IN CERTIFICATION SCHEMES

2.4.1 Introduction

2.4.2 ICT Products certification

ICT product *means an element or a group of elements of a network or information system.*

Common Criteria for Information Technology Security Evaluation

2.4.3 Management system certification

ICT service *means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.*

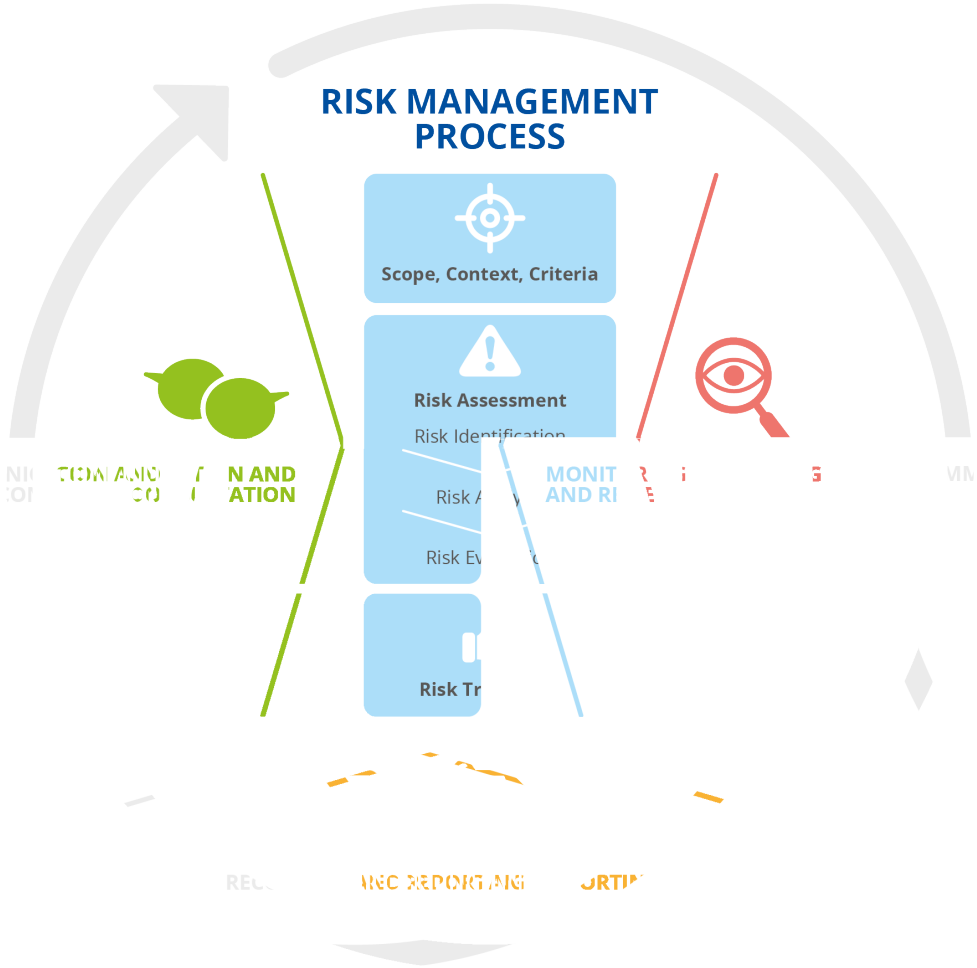
ICT process *means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.*

-

-
-
-
-
-
-
-
-
-
-
-
-
-
-

3.1 OBJECTIVES OF RISK MANAGEMENT

3.2 RISK MANAGEMENT PROCESSES



Scope, Context, Criteria

-
-
-
-
-
-

-
-

Risk treatment

-
-
-
-
-
-
-

3.3 USE OF STANDARDS IN RISK MANAGEMENT

4.1 RISK ASSESSMENT STANDARDS

-
-
-

4.1.1 European SDOs (ESOs) and European Standards

-
-
-
-

-
-

4.1.2 International SDOs and Standards

-
-
-
-

4.1.3 National standardisation bodies and specialised agencies

-

-
-

4.1.4 Industrial bodies

4.1.5 The Risk Management Standards Inventory

-
-
-
-

-
-
-
-

4.1.6 Risk management methodologies and tools

Option 1: Methodology is used to achieve conformance to a standard (referencing in part or in whole to a certain standard and its requirements).

Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) Risk Manager

-
  -
  -
    -
    -
    -
  -
  -
  -

-
-

Method for the Harmonised Analysis of Risk (MAGERIT)

Option 2: Methodology is given as a standard and can be used to achieve conformance to a standard and its requirements.

NIST 800-30 Methodology

Option 3: Methodology is a set of good practices but not related to any standard and not used to achieve conformance.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method

CCTA Risk Assessment and Management Methodology (CRAMM)

IT-Grundschutz

MEHARI

Information Security Assessment and Monitoring Method (ISAMM)

4.2 OTHER SYSTEMS AND TOOLS SUPPORTING RM

Baldrige Cybersecurity Excellence Builder (BCEB)

Common Vulnerabilities and Exposures (CVE)

Common Vulnerability Scoring System (CVSS)

Security Content Automation Protocol (SCAP)

OWASP threat modelling tool

Factors Analysis in Information Risk (FAIR Privacy

SRAQ Online Risk Calculator

Vulnerability registers and databases

CYSM

MEDUSA

MITIGATE

Cyberwatching Cyber Risk Temperature Tool

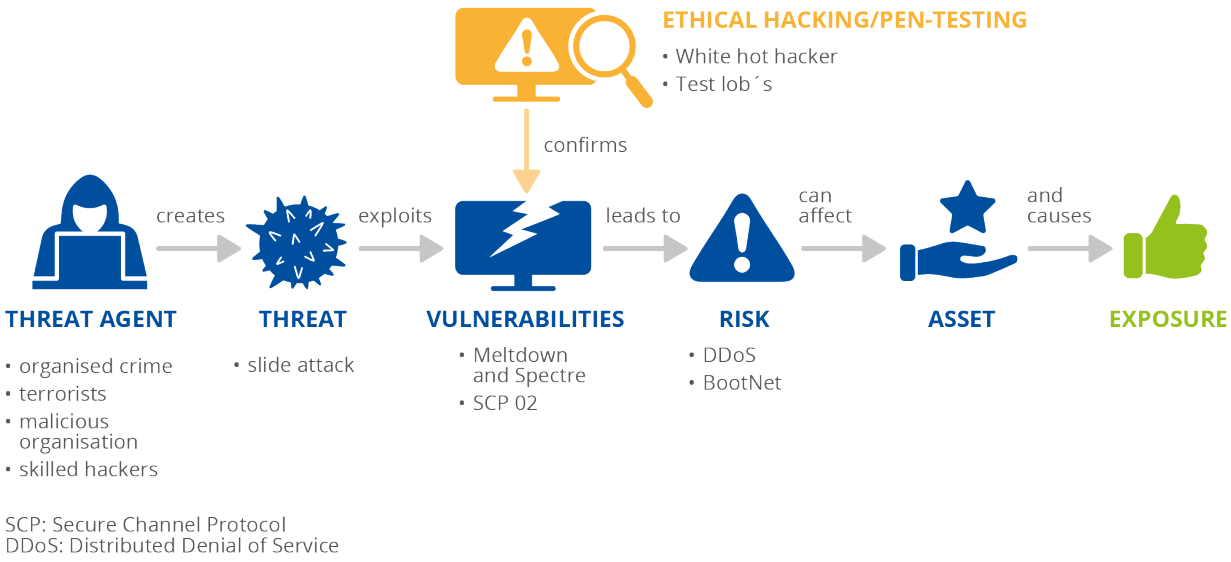
RESISTO

FINSEC

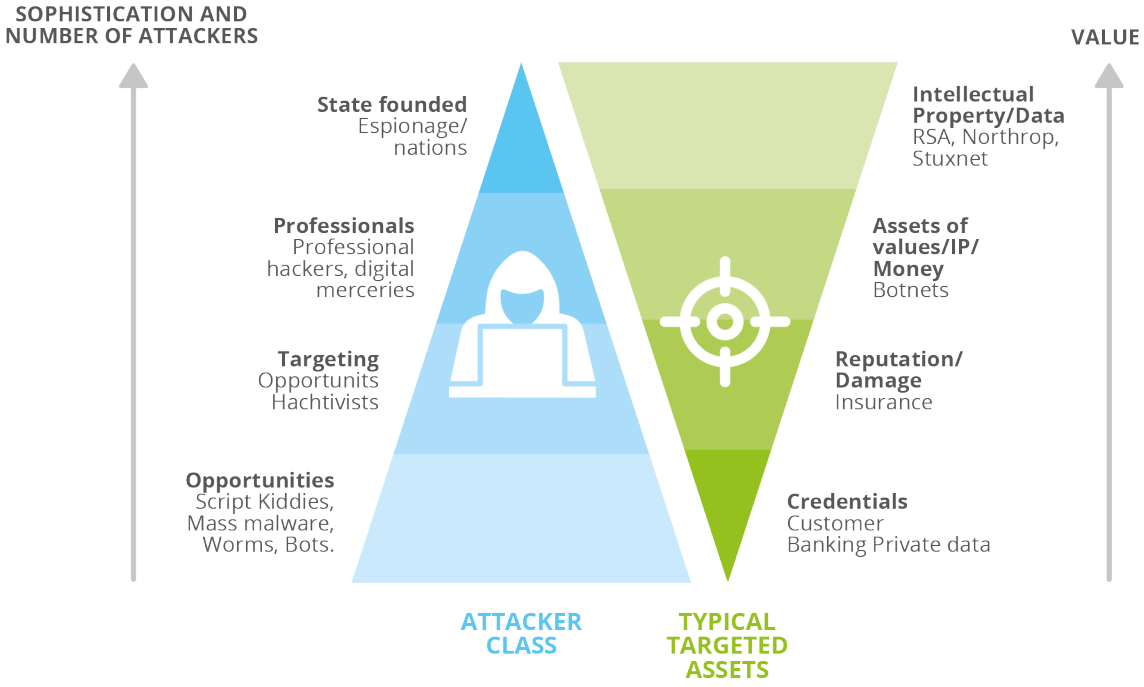
4.3 PRACTICAL USE OF STANDARDS AND METHODOLOGIES

-
-
-

threat agent and the asset

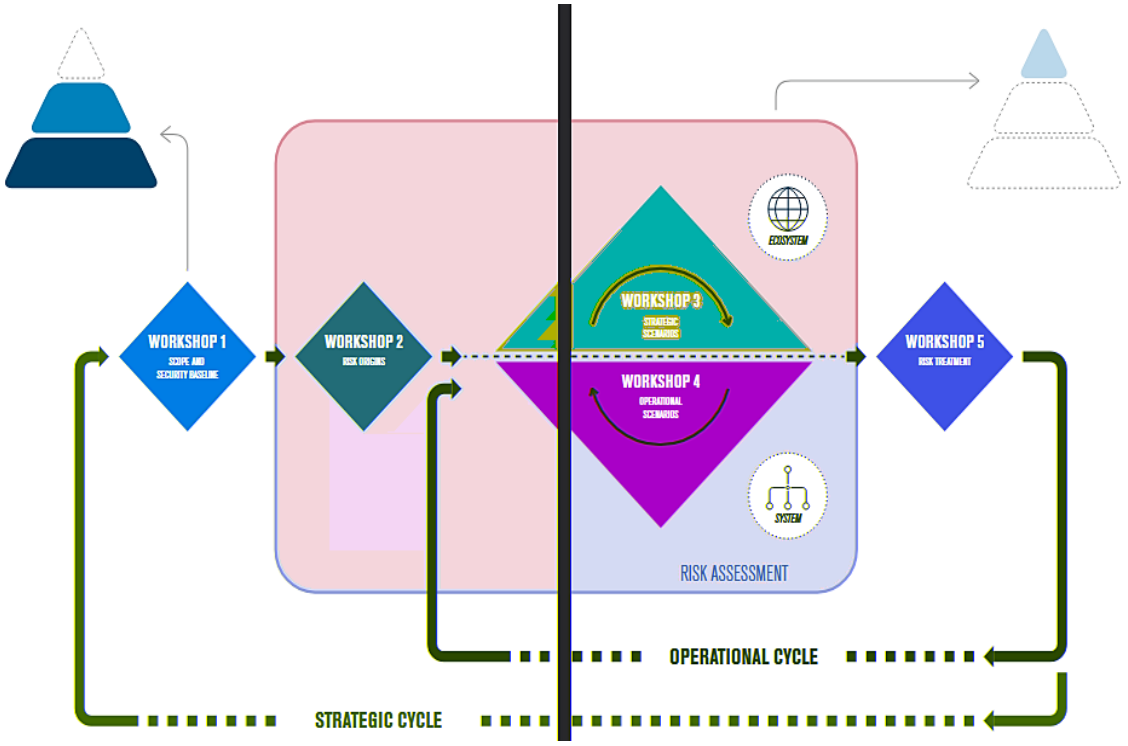


SCP: Secure Channel Protocol
DDoS: Distributed Denial of Service


SOPHISTICATION AND NUMBER OF ATTACKERS
VALUE
State founded
Espionage/ nations
Professionals
Professional hackers, digital merceries
Targeting
Opportunits Hachtivists
Opportunities
Script Kiddies, Mass malware, Worms, Bots.
Intellectual Property/Data
RSA, Northrop, Stuxnet
Assets of values/IP/ Money
Botnets
Reputation/ Damage
Insurance
Credentials
Customer Banking Private data
ATTACKER CLASS
TYPICAL TARGETED ASSETS

-
-
-
-
-
-

Figure 1 — An iterative approach in five workshops - Source ANSSI



WORKSHOP 1
Scope and security baseline

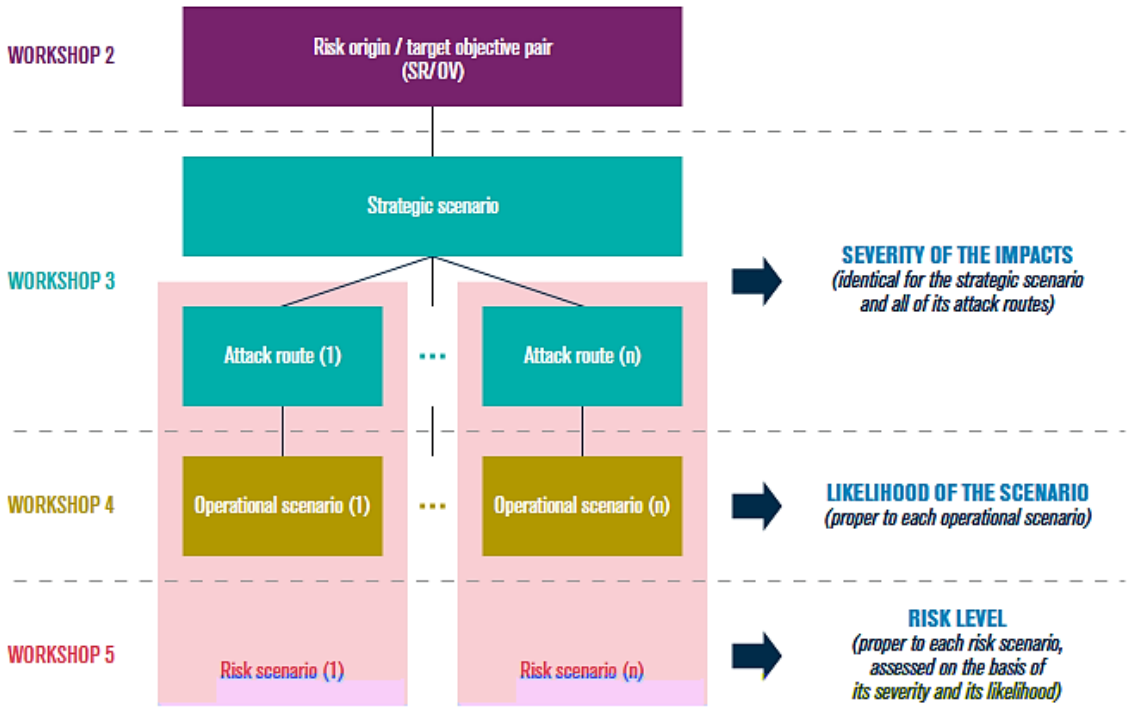
WORKSHOP 2
Risk origins

WORKSHOP 3
Strategic scenarios

WORKSHOP 4
Operational scenarios

WORKSHOP 5
Risk mitigation

Figure 2: Link between the various workshop – source EBIOS RM - ANSSI



-
-
-
-
-

-
-
-
-
-
-
-

Concepts, terms and definitions

Risk Criteria

Areas of application

ICT

Level of application

European vs international technical specifications

EU legislation versus standards

6.1 EU POLICY MAKERS

Recommendation 1:

Recommendation 2:

Recommendation 3:

Recommendation 4:

Recommendation 5:

Recommendation 6:

6.2 EUROPEAN SDOS

Recommendation 7:

Recommendation 8:

Recommendation 9:

-
-
-

Recommendation 10:

6.3 ENISA

Recommendation 11:

Recommendation 12:

Recommendation 13:

Recommendation 14:

Recommendation 15:

Name	Document reference	Document type	Document scope	Name of the publishing Organisation	Short description


enisa

eIDAS items	Electronic Identification and Trust Services for Electronic Transactions - Regulation (EU) No 910/2014		Means
Identification schemes – Mutual recognition	**appropriate to the degree of risk**	**security**	
Trust Service Providers	**activities**	**the risks related to their**	
Data protection handle by electronic registered delivery service	**or any unauthorised alterations.**	**the risk of loss, theft, damage**	
Liability of all trust service providers – assessment of financial risk			
	assurance level low		

assurance level substantial

Security requirements applicable to trust service providers

Requirements for qualified trust service providers

ABOUT ENISA

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu