M2 CyberSecurity
Threat and Risk Analysis, IT Security Audit and Norms

Security Assessment of Information System
Standards, Methods and Tools

Florent Autréau - florent.autreau@imag.fr
2016 /2017

Outline

- *Introduction*
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
  - Nessus, nmap, wireshark, ntop, ...
- Hand-on Labs

Standard : what's the (f***) purpose ?

Cartography of InfoSec

- Set of documentation, questionnaires and knowledge bases.
- Allow to measure existing practices and to compare to a reference guide of « good practices ».
- Identify important processes within organization and propose metrics in order to calculate impacts of potential losses (Risk Analysis).

Purpose of InfoSec Standards

- Protection of informational assets
- Sign (if not Proof) of Trust
- Potential Differentiatior (from Competition)
- Profitability
- Respect of Legislation and Rules
- Public Image

Legislation

- Sarbanes-Oxley (USA)
- HIPAA – Heath Information Protection Assurance Act (USA)
- FOIA – Freedom Of Information Act (USA)
- Access to Information and Privacy Acts (Canada)
- Bale2 (EU)
- LCEN (FR)

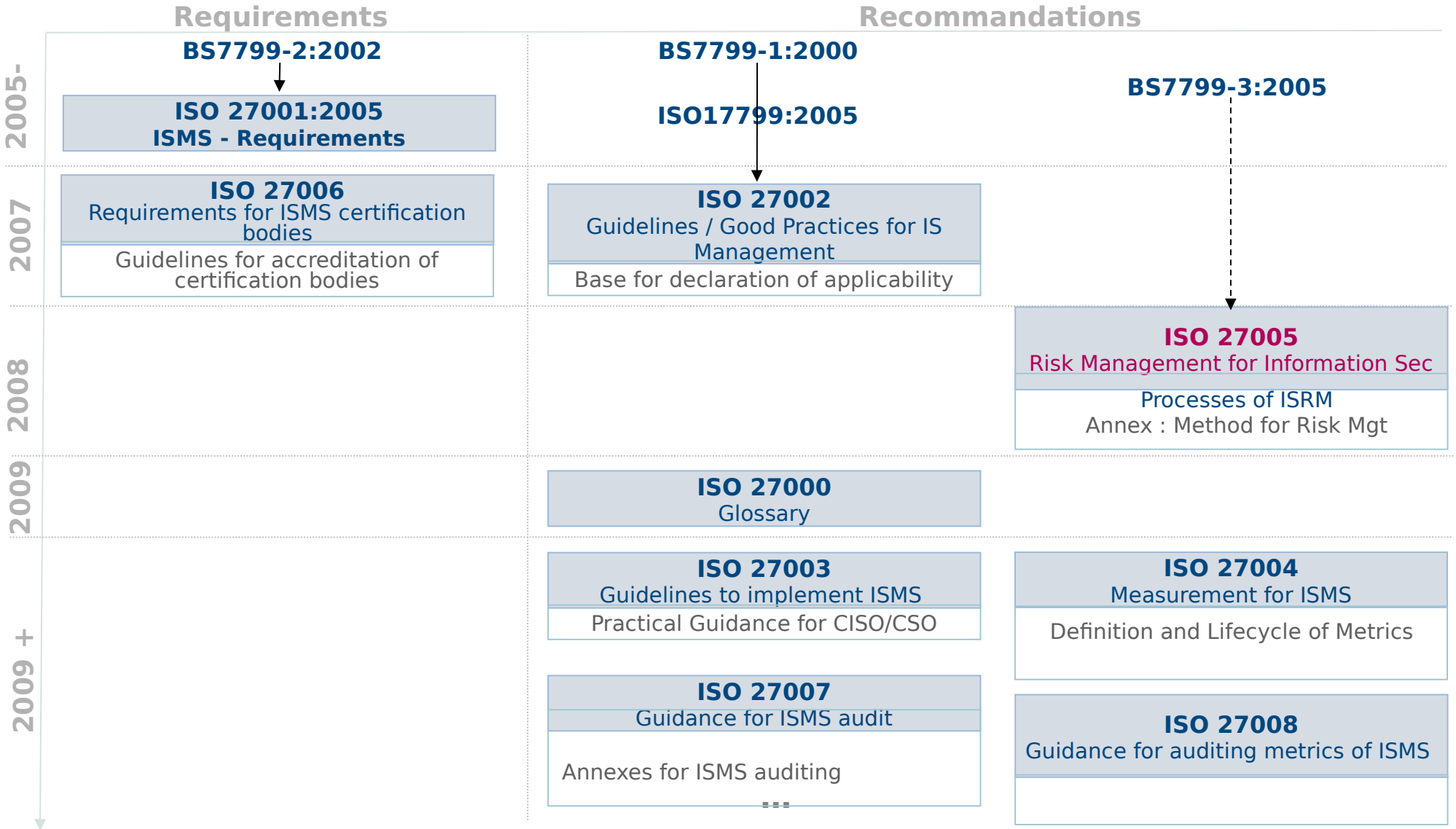
Standards : Guide of Good Practices

- Define a set of **good pratices** for Information Security, used as reference and able to insure third party with an acceptable and recognized level of security.
- Specify **requirements** for
  - Implementation
  - Operation
  - Improvement of documented ISMS (Information Security Management System)
- Specify **requirements** to implement security measures that are :
  - Adapted to the needs of the enterprise or organisation
  - Appropriate
  - Well Suited / Commensurate

Identification	Désignation	Source
EBIOS	Méthode	ANSSI
MEHARI	Méthode	CLUSIF
OCTAVE	Méthode	CERT
PSSI	Guide Méthodologique	ANSSI
TDBSSI	Guide Méthodologique	ANSSI
RMF	Guide Méthodologique	NIST
SP800-60	Guide Méthodologique	NIST
ITIL	Guide de bonnes pratiques	OGC – BSI
COBIT	Guide de bonnes pratiques	ISACA
ITSEC	Norme d'exigences	UE – ANSSI
ISO 15408	Norme d'exigences	ISO
NF Z 42-013	Norme d'exigences	AFNOR
ISO 2700x	Norme de bonnes pratiques	ISO
PP nc / 0XX	Guide Technique	ANSSI
SP800-45	Guide Technique	NIST

- ANSSI :
  - www.ssi.gouv.fr
- CERT :
  - www.cert.org
- NIST :
  - csrc.nist.gov
- CNRS :
  - www.sg.cnrs.fr/fsd
- ISACA :
  - www.isaca.org
- ITIL :
  - www.itil.co.uk
- ISF :
  - www.securityforum.fr

Standards for ISMS
(Information Security Management System)



Antoine Rojat / Florent Autréau

ISO 27000 Standards

Covers :

- Risk Assessment
- Security policy - management direction
- Organization / Governance of InfoSec
- Asset management
- Human resources security
- Physical and environmental security

ISO 27000 Standards (cont.)

- Communications and operations management - management of technical security controls in systems and networks
- Access control
- Information systems acquisition, development and maintenance - building security into applications
- InfoSec incident management

ISO 27000 Standards (cont.)

- Business continuity management
- Compliance/conformance with policies, standards, laws and regulations

ISO 27000 Series

- ISO 27000
  - Glossary
- ISO 27001 (2005)
  - ISMS – Information Security Management System
  - certification standard against which organizations' ISMS may be certified
  - good practices in IT Security .
  - 2nd part of BS7799.

ISO 27000 Series (2)

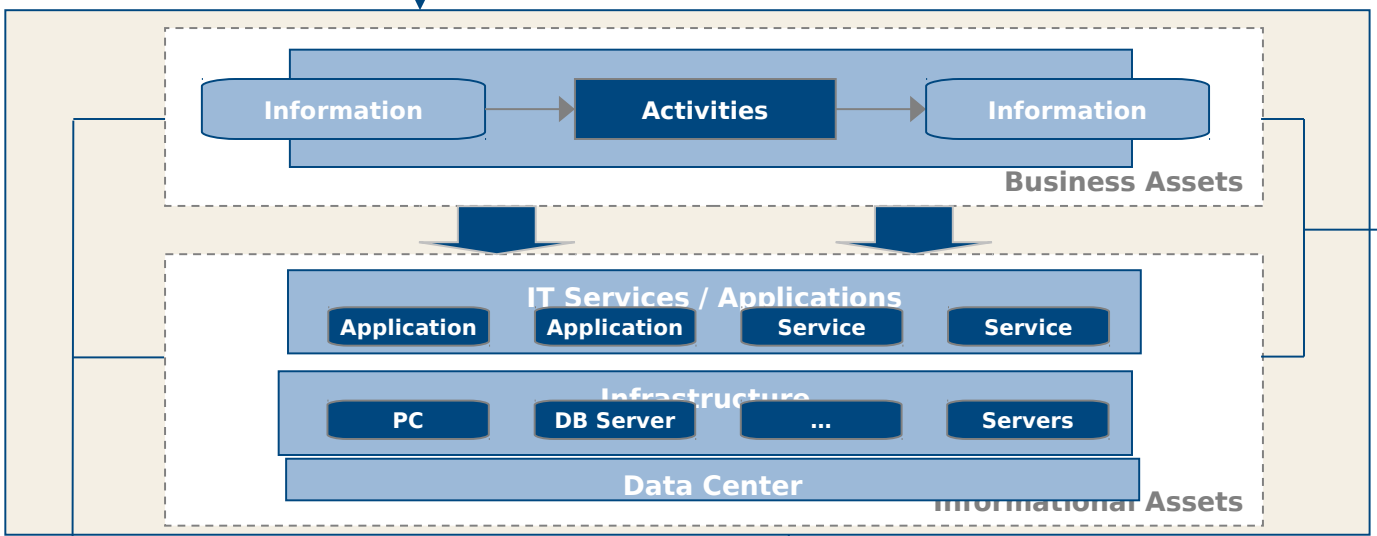
- ISO 27002 (ex-17799)
  - Code of practice
  - Security Measures
  - 1st part of BS7799.
- ISO 27003
  - Implementation Guide
- ISO 27004 (2007 ou2008)
  - Measurement and metrics

ISO 27000 Series (3)

- ISO 27005 (2007)
  - Risk management / Risk analysis
  - 3rd part of BS7799
- ISO 27006 (2007)
  - Guideline for Auditing and Certification of ISMS
- ISO 27007
  - Continuity and Contingency Plan

ISO 27005 – Risk Analysis

- Definition of ***evaluation criteria***
- Definition of ***acceptance criteria***



- Identification of ***Threats***
- Mapping of ***existing measures***
- Identification of ***Vulnerabilities***

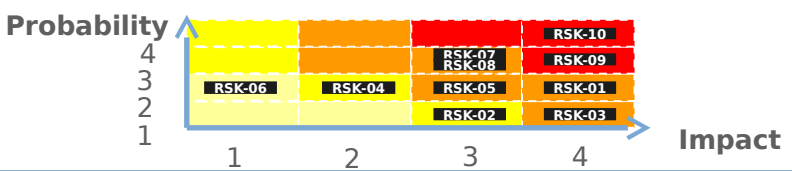
- Classification of Security Issues

D	I	C	P
3	4	2	1

- Identification of ***risk scenarios***

- ***Classification of risk scenarios (Impact, Potentiality)***

- ***Evaluation*** of risk scenarios



ISO 27005

Step 1 : Context Study

Goal : Definition of perimeter and evaluation criteria for the risk analysis

- The **context study** defines the criteria and metrics to quantify :
  - Impact (categories/level)
  - Potentiality of scenarios
  - Criteria for Acceptance.

⚠️ Insure coherence of metrics/scale over the perimeter

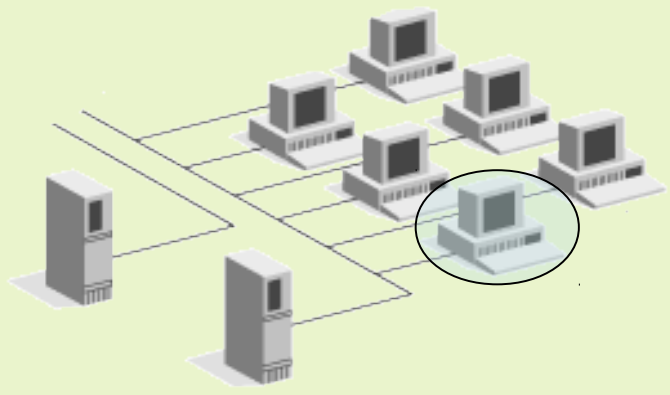
« End-user workstation used for accounting and finance »

ISO 27005

Step 2 : Identify Assets

Goal: mapping of valuables / discovery of perimeter

- Identification of assets to insure :
  - That no asset has been ignored or forgotten ;
  - That the perimeter of risk analysis is clearly defined.



- The **workstation** itself ;
- **Information hosted by or transiting** on the workstation.

⚠️ **Better define** the perimeter and **identify** people to be involved

ISO 27005

Step 3 : List Threats and existing Countermeasures

Goal : Identify Threats, Vulnerabilities and Countermeasures.

- Based on the Context Study :
  - Identify threats against assets ;
  - Identify countermeasures ;
  - Identify existing vulnerabilities.

- Threat :
  Phishing ;
- Countermeasure :
  Mail filtering ;
- Vulnerability :
  Lack of user awareness to social engineering tricks.

⚠ Define threats that **only** apply to perimeter

ISO 27005
Step 4 : Estimate Security Issue

Goals : Evaluate security needs for perimeter

- Based on interviews of stakeholders, quantify needs/requirements for the security of assets.

Workstation	A	I	C	P
User	4	4	1	?
Company	1 / 2	1 / 2	4	4

⚠️ Getting accurate estimation from stakeholders

ISO 27005
Step 5 : Define Risk Scenarios

Goal : Define the risk scenarios

- Risk Scenario : exploitation, by a threat of existing vulnerability on given asset.

- Menace : Phishing ;
- Vulnerability : uneducated user ;
- Asset : information owned or manipulated by user.

Scenario 10 : *User clicks on link that drives to malicious code*

- **Rigourous and Systemic**

ISO 27005
Step 6 : Estimation of Risk Scenarios

Goal : Estimate impact and likelihood of scenarios

- From the list of scenarios and used scales :
  - Quantify impact;
  - Quantify likelihood

Scenario 10 : *User clicks on link that drives to malicious code*

- Impact :
  4 ➔compromise of confidential data ;
- Likelihood :
  2 ➔ moderated by mail filtering solution

⚠️

- What is **likelihood** ?

ISO 27005
Step 7 : Classify Risk Scenarios

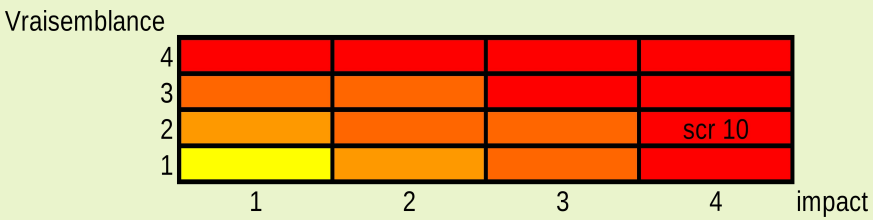
Goal : Evaluate and Classify the Risk Scenarios

- Evaluate criticality of scenarios :

Criticality = Likelihood x Impact

- Classify scenarios to identify remaining risks.

Scenario 10 : *User clicks on link that drives to malicious code*



No major difficulties

Methods and ad-hoc standards

- Complexity of methods for risk analysis
- Hence ad-hoc methods and standards for specific environment
- As an example, Comité Français d'Organisation et de Normalisation Bancaire defined a profile of minimum set of protection to cover precise needs of banking sector.

Methods

- MEHARI
  - Method for Risk Analysis based on ISO 2700x series. www.clusif.asso.fr
  - Derived from MARION and MELISSA
- EBIOS/PSSI
  - Methods and plans provided by the French government www.ssi.gouv.fr/fr/confiance/methodes.html

MEHARI

- MEthode Harmonisée d'Analyse de RIsques (MEHARI) - Commission Méthodes du CLUSIF (Club de la Sécurité des Systèmes d'Information Français)
- 6 factors for risks :
  - 3 for potentiality and 3 for impact ;
- 6 types of security measures:
  - structural, dissuasive, prevent/protection, palliative and recovery.

MEHARI – Domains (1)

- Organization of ISMS
- Security Awareness and Education
- Physical Security of Sites
- Access Control to Sensitive Areas
- Protection against usual risks (fire, flooding, etc.)
- Network Architecture (Access Control, Filtering, containment, reliability)
- Confidentiality and integrity of communication

MEHARI – Domains (2)

- Access Control to Logical level (systems, apps and data)
- Data Security
- Operational Procedures
- Management of Information Support
- Rescue Plan
- Backup and Recovery Planning
- Maintenance
- Security of projects and development
- Incident Management

MEHARI


Stakes & asset analysis– Classification
Security services audit
Identification of critical risks
Risk situation analysis
Action plans based on the vulnerability audit
Action plans based on risk analysis
Project-based risk management
Action plans based on stakes analysis

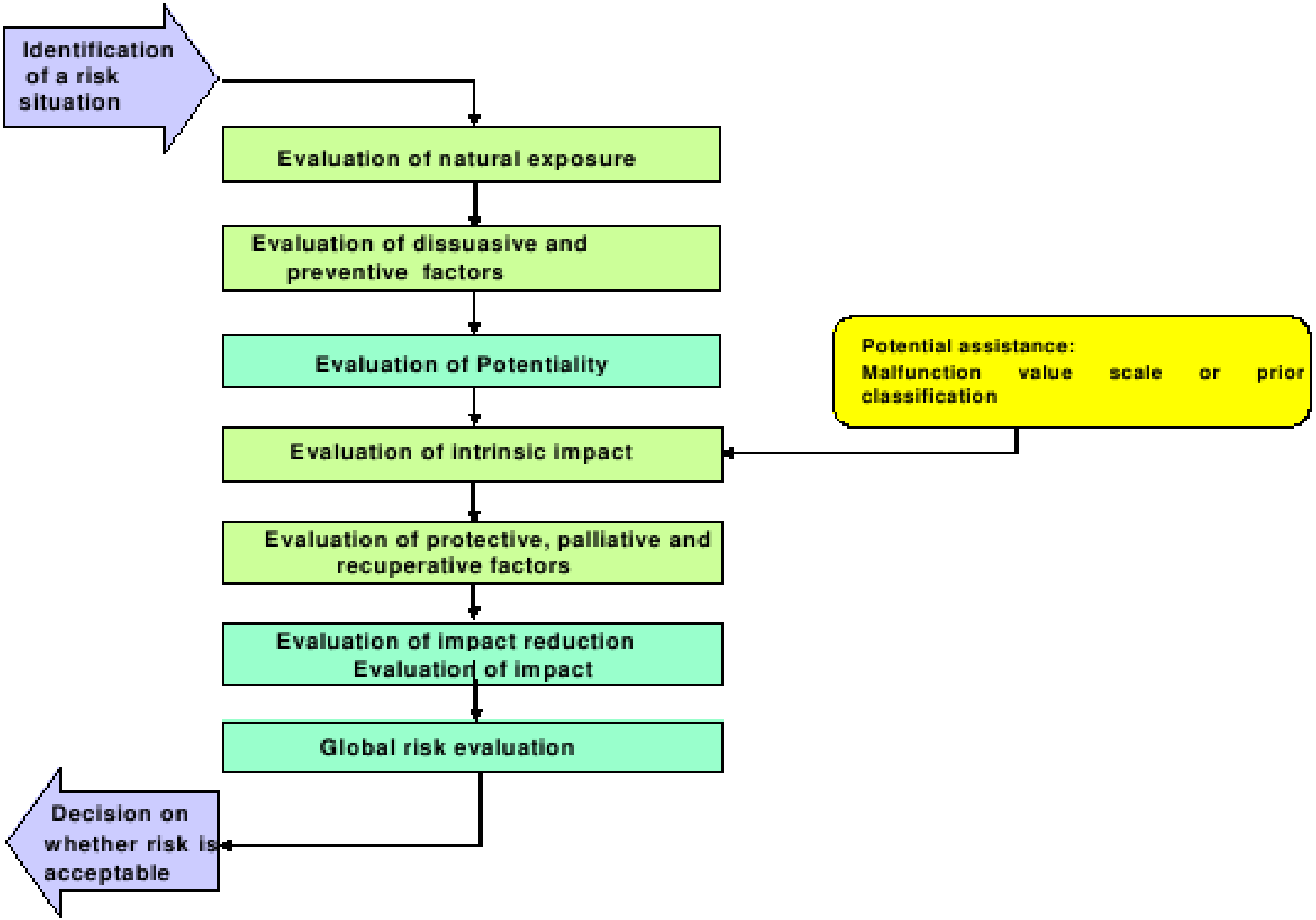
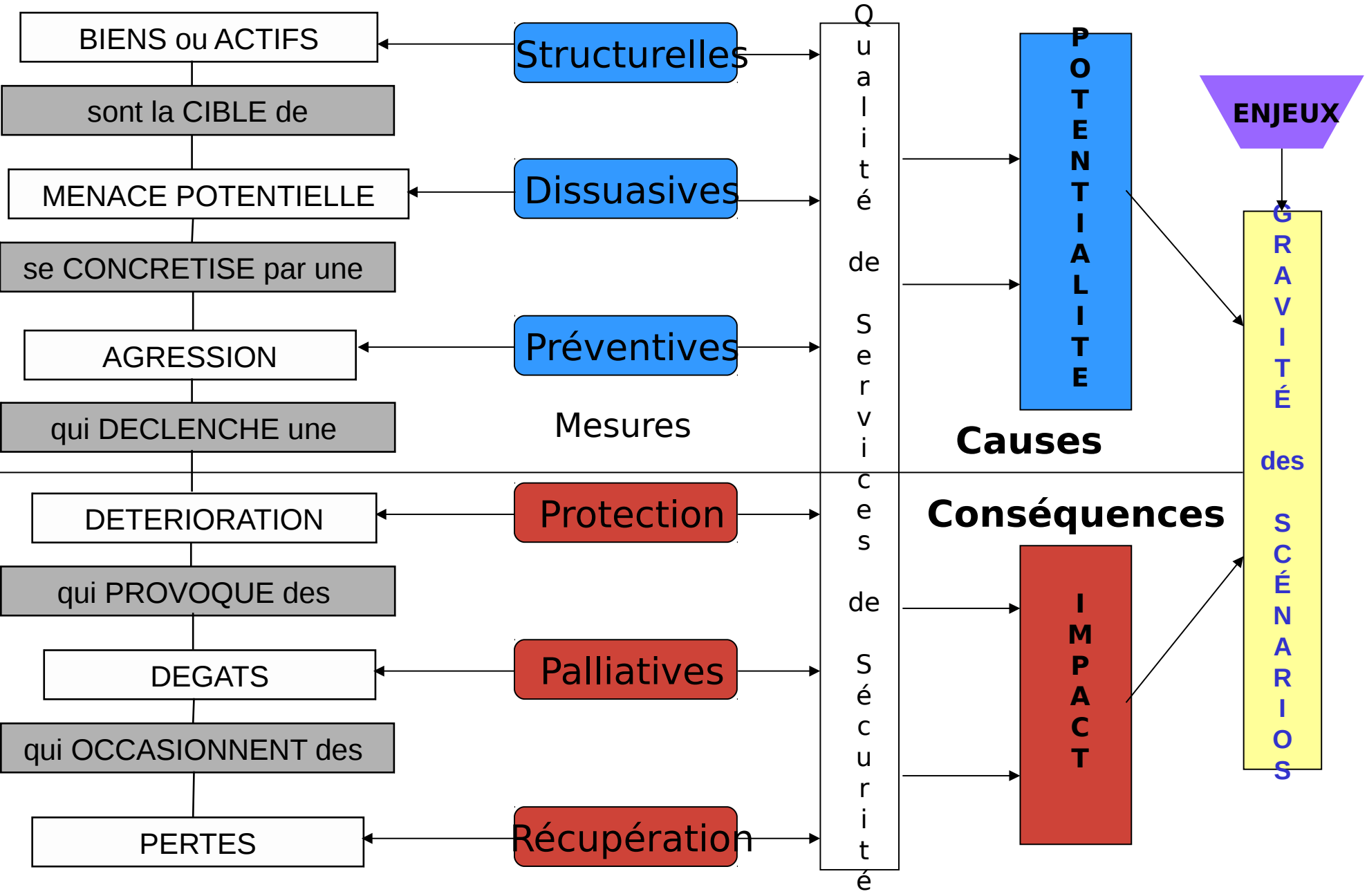
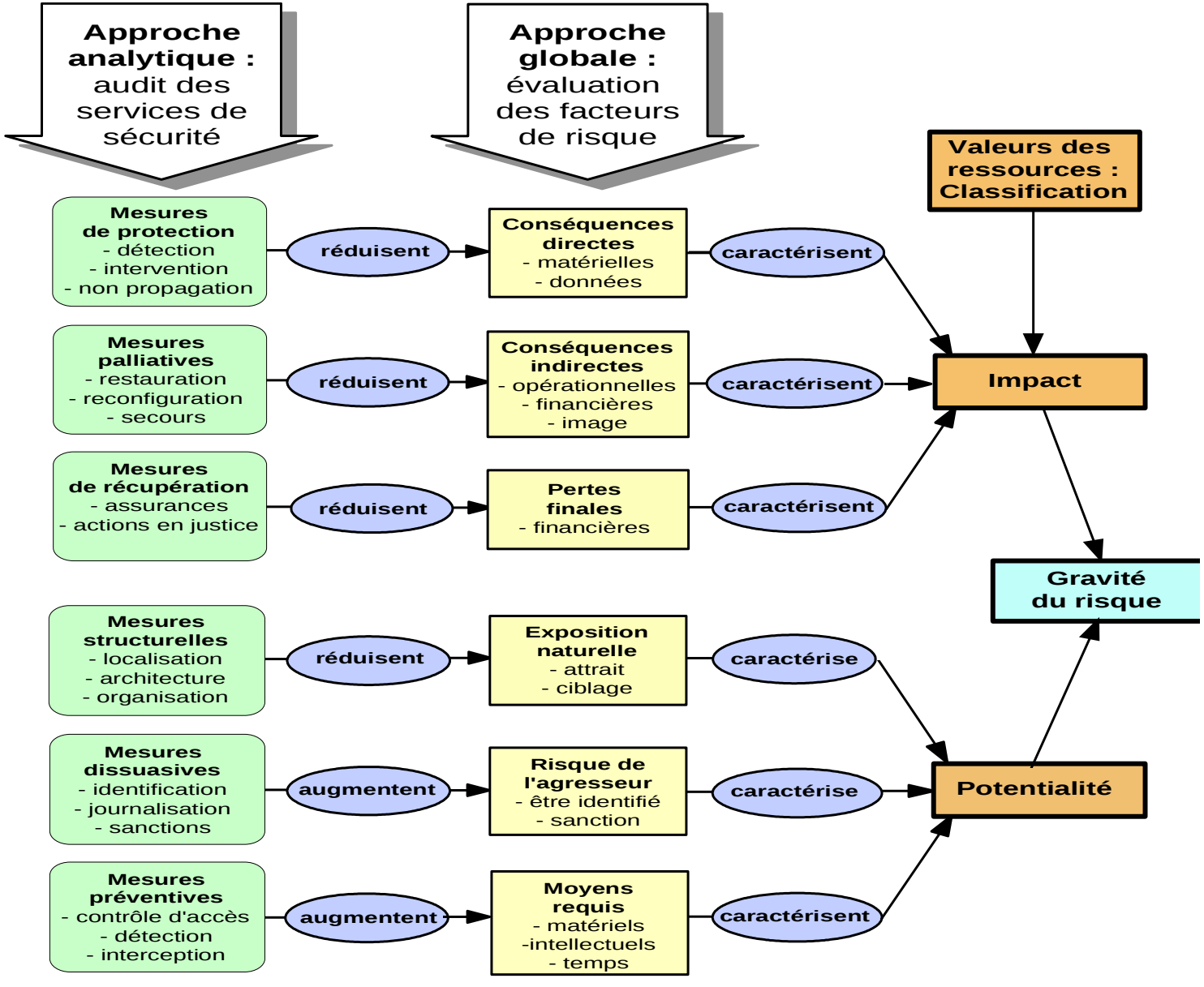


Figure 5: Risk situation analysis


BIENS ou ACTIFS
sont la CIBLE de
MENACE POTENTIELLE
se CONCRETISE par une
AGRESSION
qui DECLENCHE une
DETERIORATION
qui PROVOQUE des
DEGATS
qui OCCASIONNENT des
PERTES
Structurelles
Dissuasives
Préventives
Mesures
Protection
Palliatives
Récupération
Qualité de Services de Sécurité
POTENTIALITE
Causes
IMPACT
Conséquences
ENJEUX
GRAVITÉ des SCÉNARIOS


Approche analytique : audit des services de sécurité
Approche globale : évaluation des facteurs de risque
Valeurs des ressources : Classification
Mesures de protection
- détection
- intervention
- non propagation
réduisent
Conséquences directes
- matérielles
- données
caractérisent
Mesures palliatives
- restauration
- reconfiguration
- secours
réduisent
Conséquences indirectes
- opérationnelles
- financières
- image
caractérisent
Impact
Mesures de récupération
- assurances
- actions en justice
réduisent
Pertes finales
- financières
caractérisent
Gravité du risque
Mesures structurelles
- localisation
- architecture
- organisation
réduisent
Exposition naturelle
- attrait
- ciblage
caractérise
Mesures dissuasives
- identification
- journalisation
- sanctions
augmentent
Risque de l'agresseur
- être identifié
- sanction
caractérise
Potentialité
Mesures préventives
- contrôle d'accès
- détection
- interception
augmentent
Moyens requis
- matériels
-intellectuels
- temps
caractérisent

EBIOS

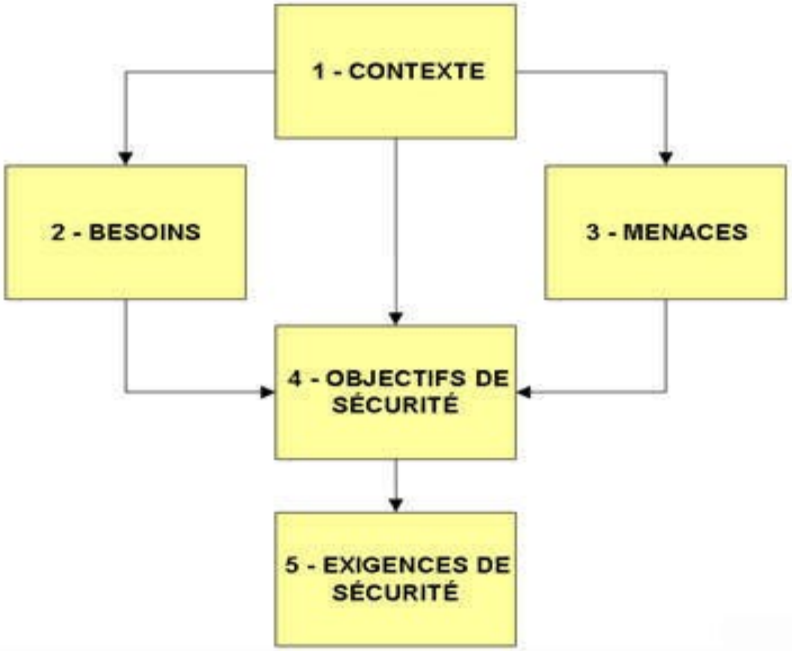
- Expression des Besoins et Identification des Objectifs de Sécurité : Méthode de gestion des risques de l'ANSSI.

http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/

EBIOS

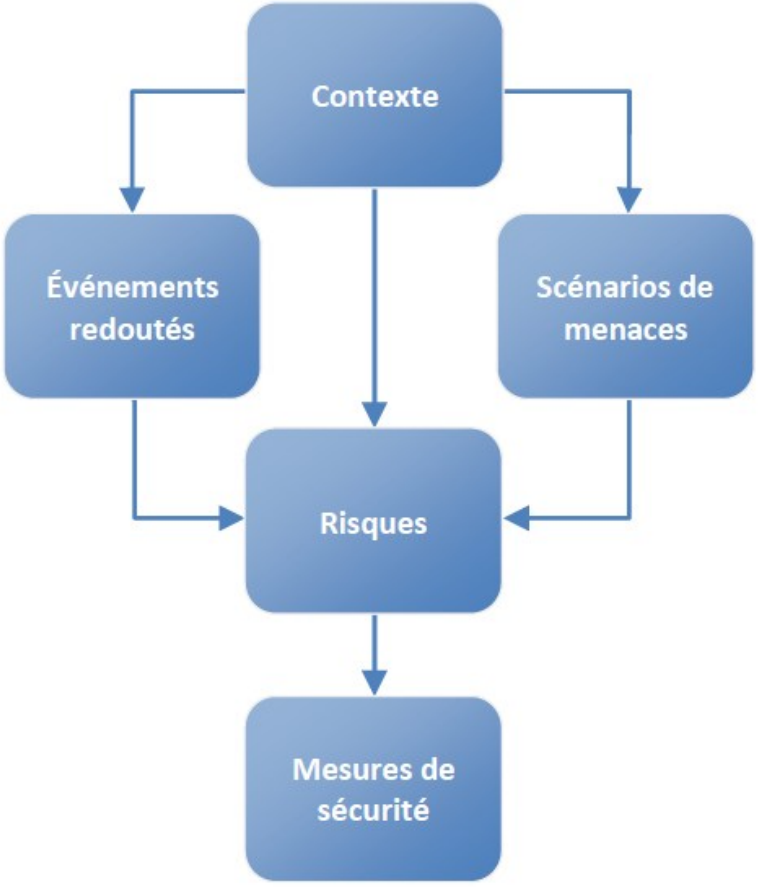
Risk Analysis

- ANSSI
- Version 3 (2010)
- 5 modules
- ISO 27001
- *French*



EBIOS

Les 10 questions essentielles pour gérer les risques



Contexte	•Pourquoi et comment va-t-on gérer les risques ? •Quel est le sujet de l'étude ?
Evénements redoutés	•Quels sont tous les événements craints ? •Quels seraient les plus graves ?
Scénarios de menaces	•Quels sont tous les scénarios possibles ? •Quels sont les plus vraisemblables ?
Risques	•Quelle est la cartographie des risques ? •Comment choisit-on de les traiter ?
Mesures de sécurité	•Quelles mesures devrait-on appliquer ? •Les risques résiduels sont-ils acceptables ?

OCTAVE

- From CERT http://www.CERT.org/octave/osig.html
- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®)
- self-directed approach
- Required broad knowledge of business and security processes

OSSTMM

- OSSTMM - Open Source Security Testing Methodology Manual
    - http://www.isecom.org/osstmm/


OSSTMM
Discovery:
Obtaining and analysis of the existing system documentation
Enumeration Verification:
Testing of the operating systems, the configuration and services in comparion with the system documentation
Vulnerability Research & Verification:
Vulnerability research and analysis by penetration tests
Integrity Testing:
Integrity testing of all results
Security Mapping:
Mapping of the measured security. Mapping of the results on systems and services.
Risk Assesment Value:
Calculation of the RAV and risk classification of the weaknesses found.
Reporting:
Mapping of the results and giving of recommendations

PCI -DSS – Set of standards for those who work with and are associated with payment cards. This includes: merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

Requirement 1.0

Install and maintain a firewall configuration to protect cardholder data.

Requirement 2.0

Do not use defaults for passwords and other security parameters.

Requirement 3.0

Protect stored data.

Requirement 4.0

Encrypt cardholder data and information across public networks.

Requirement 5.0

Use and regularly update antivirus software.

Requirement 6.0

Develop and maintain secure systems and applications.

Requirement 7.0

Restrict access to data by business need-to-know.

Requirement 8.0

Assign a unique ID to each person with computer access.

Requirement 9.0

Restrict physical access to cardholder data.

Requirement 10.0

Track and monitor all access to network resources and cardholder data.

Requirement 11.0

Regularly test security systems and processes.

Requirement 12.0

Maintain a policy that addresses information security.

Certifications

- INFORMATION SECURITY CERTIFICATIONS
- APPLICATION SECURITY AND SOFTWARE SECURITY CERTIFICATIONS
- AUDIT CERTIFICATIONS
- PHYSICAL SECURITY CERTIFICATIONS
- FRAUD, INVESTIGATION AND FORENSICS CERTIFICATIONS
- PRIVACY CERTIFICATIONS
- BUSINESS CONTINUITY CERTIFICATIONS

Information Security

- Certified Information Systems Professional, CISSP - Information Systems Security Certification Consortium (ISC)2 - www.isc2.org/cissp/default.aspx
- Systems Security Certification Practitioner (SSCP)- (ISC)2 - www.isc2.org
- Global Information Assurance Certification (GIAC)- SANS Institute - www.giac.org
- CompTIA Security+ Certification – CompTIA – certification.comptia.org/security/default.aspx
- Professional in Critical Infrastructure Protection (PCIP) (formerly CCISP)- Critical Infrastructure Insitute- www.ci-institute.org

Information Security (cont.)

- Certified Ethical Hacker (CEH) - EC Council - www.eccouncil.org/CEH.htm
- EC-Council Certified Security Analyst (ECSA) – EC Council -www.eccouncil.org
- Licensed Penetration Tester (LPT) – EC Council - www.eccouncil.org/lpt/Licensed_Penetration_Tester.htm
- Anti-Hacking Certification - Security University - www.securityuniversity.net
- Advanced Information Security Certification (AIS) - Security University- www.securityuniversity.net

Application / Software Security

- GIAC Secure Software Programmer (GSSP) - SANS Institute - www.giac.org/certifications/software
- Certified Secure Software Lifecycle Professional (CSSLP) – ISC2 - www.isc2.org/csslp-certification.aspx
- Software Security Engineering Certification - www.securityuniversity.net

Audit Certifications

- Certified Information Systems Auditor (CISA)- Institute of Internal Auditors - www.isaca.org
- Certified Information Security Manager (CISM)- Institute of Internal Auditors - www.isaca.org
- Certification in Control Self-Assessment (CCSA) - Institute of Internal Auditors - www.theiia.org
- Certified Internal Auditor (CIA)- Institute of Internal Auditors - www.theiia.org
- Certification in Control Self-Assessment (CCSA) - Institute of Internal Auditors
- PASSI – Prestataire d'Audit de SSI - ANSSI

Fraud, Investigation, Forensics

- Certified Fraud Examiner (CFE) - Association of Certified Fraud Examiners - www.cfenet.com
- Certified Identity Theft Risk Management Specialist (CITRMS) - Institute of Consumer Financial Education - www.icfe.org
- Professional Certified Investigator (PCI) - ASIS International
- Computer Hacking Forensic Investigator Certification (CHFI) -: EC Council

Physical Security

- Certified Protection Professional (CPP) - ASIS International
- Physical Security Professional (PSP) - ASIS International

Business Continuity

- Associate Business Continuity Planner (ABCP) - DRI International
- Certified Business Continuity Professional (CBCP) - DRI International
- Master Business Continuity Professional (MBCP) - DRI International
- Business Continuity Certified Planner (BCCP) - BCM Institute

Privacy

- Certified Information Privacy Professional (CIPP) - International Association of Privacy Professionals, IAPP

FIPS 140-1

- Security Requirements for Security Modules
- Standard from US Department of Industry
- Mainly used to evaluate security equipment from anglo-saxon countries
- Barely used for software

FIPS 140-1 (Levels)

- **Level 1** : Minimum Level with basic security requirements
- **Level 2** : Includes constraints to resist to attack by using integrity checking and authentication for operators
- **Level 3** : Includes physicals requirements (detection of physical intrusion).
- **Level 4** : Adds stricter stronger requirements (armoured shelter, detection variation of pressure, d…).

ITSEC

- Relatively Old Standard (1991)
- Derived from the Orange Book (DOD)
- Define level of trust as well as methods to evaluate
- Interpretated differently from one country to another
- Most of the products have been evaluated in UK
- European Standard

Common Criteria

- Following ITSEC.
- Attempt to correct ITSEC weaknesses (discrepancy in evaluations)
- LARGE amount of documentation
- International recognition (not EU only)
- define classes of insurance (development, tests, vulnerabilities...).
- Global level is obtained by minimal level in each class.

Common Criteria (levels)

- EAL 1 : functionnally tested
- EAL 2 : structurally tested
- EAL 3 : methodically tested and evaluated
- EAL 4 : methodically designed, tested and evaluated
- EAL 5 : designed with semi-formal methods and tested
- EAL 6 : design validated with semi-formal methods and tested
- EAL 7 : design verified with semi-formal methods and tested

Maintenance of evaluation

- Evolution of products
  - Technical evolution,
  - Functional evolution,
  - corrections.
- Need to update evaluation peridiocally.

Tutoring

Exercise 5

- Identify, quantify and classify the risks for the following scenarios (preparation for lab):
  - As a student in M2 CySec, conduct a risk analysis for your personal informational assets in your usage of IT resources.
  - Idem acting as a sysadmin working for the university, when providing and managing shared facilities such as in F103 room.

Exercise 6

- Cheating – Fake Exam
  - Exam situation : write down the 100 first digits of PI
  - Describe the strategies used for cheating and the potential countermeasures