Security Audit

Patrick Lacharme

ENSICAEN

2010

Plan

Information Security

Information security (*sécurité de l'information*).

Preservation of confidentiality, integrity and availability of information (ISO 27002).

Confidentiality (*confidentialité*).

Property of essential elements making them only accessible to authorized users.

Integrity (*intégrité*).

Property defining the accuracy and completeness of the essential elements.

Availability (*disponibilité*).

Property of essential elements that allows authorized users to access them at the required time.

Information Security Management Systems (ISMS)

Information Security Management Systems (*Système de gestion de la sécurité de l'information*).

Organizes the various information security controls in an organisation (ISO 27000).

Information systems security policy (*politique de sécurité des systèmes d'information (PSSI)*).

Set of strategic informations, directives and technical rules formalised in an applicable document whose objective is to protect the organisation's information systems.

Information Systems Security (ISS)

Any organisation using means of information and communication technology is directly concerned by ISS.

Assessement and management of risks are an essential part of information system security.

Objects of the ISS approach are :

- The information (essential element).
- The processes, functions or applications (essential element).
- The technology (equipment and OS) (entity).
- The physical environment (entity).
- The human factor (entity).

Standardised approaches

A general ISMS is described in ISO/IEC 27001 and related standards in **ISO/IEC 27000 series**.

Information technology security evaluation is described in **Common Criteria**, also called ISO 15408.

In France, **EBIOS** is a method for assessing and treating information systems security risks. EBIOS is compatible with ISO 27000 suite and Common Criteria.

MEHARI (*MÉthode Harmonisée d'Analyse de RIsques*) for IS risk management (2010), created by the **CLUSIF** in 1995.

Other methods on IS risk management : Marion (clusif, 1983), Melisa (DGA), Octave (1999),...

General security concepts and relationships

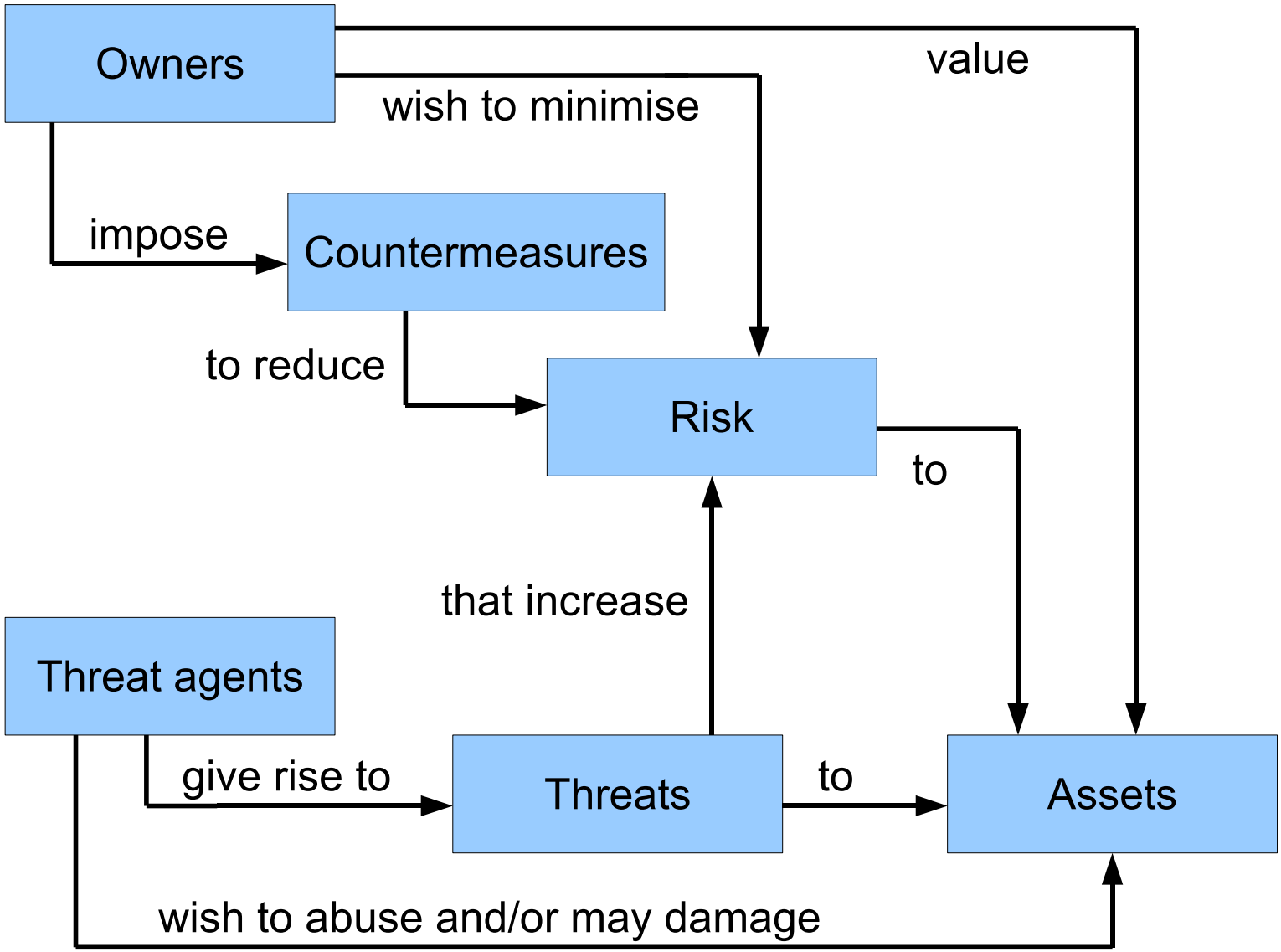

FIGURE: General security concepts and relationships (CC)

Assets and threats

Asset (*bien*).

Any resource of value to the organization and necessary for achieving its objectives (essential element or entities).

Threat (*menace*).

Possible attack of a threat agent on assets.

Threat agent (*élément menaçant*).

Human action, natural or environmental element that has potentially negative consequences on the system.

Threat agent can be characterized by its **type** (human, environmental) and by its **cause** (accidental or deliberate).

Risk and countermeasures

Owner are (held) responsible for assets. They decide or not to accept the risk to expose the assets to the threats.

Risk (*risque*).

Combination of a threat and the losses it can cause, ie : of the opportunity for a threat agent using an attack method, to exploit one or more vulnerabilities of one or more entities and the impact on the essential elements and on the organization.

Countermeasures (*contre-mesures*).

A measure designed to reduce the risk on the assets. Countermeasures are IT measures such as firewall or non-IT measures such as guards.

ISO/IEC 27000 series

The **ISO/IEC 27000 series** (or ISO2700k) is a family of international standards published by ISO and IEC.

ISO = International Organization of Standards.
IEC = International Electrotechnical Commission.

This serie provides recommendations and certifications on Information Security Management Systems.

More details on the web pages :
`http://www.27000.org/`
`http://www.iso27001security.com/.`

Content of ISO/IEC 27000 serie

ISO/IEC 27000 : *Information technology - Security techniques - ISMS - Fundamentals and vocabulary* (2009).

ISO/IEC 27001 : *Information technology - Security techniques - Specification for ISMS* (2005).

ISO/IEC 27002 : *Information technology - Security techniques - Code of practice for information security* (2005).

ISO/IEC 27003 : *Information technology - Security techniques. ISMS implementation guidance* (january 2010).

ISO/IEC 27004 : *Information technology - Security techniques - IS management - Measurement* (dec. 2009).

ISO/IEC 27005 : *Information technology - Security techniques - IS risk management* (june 2008).

ISO/IEC 27001 standard

Title of ISO/IEC 27001 : *Information technology - Security techniques - Specification for ISMS*.

Proposed in 2005 and **based on BS 7799** (part 2), created by the British Standard Institute (BSI) in 1995.
More details on BS 7799 on web site :
`http://www.induction.to/bs7799/`.

Formal set of **specifications and requirements for ISMS**.
Certification of ISMS organization, compliant with this standard.

Process of ISO 27001 uses a Deming cycle, similar to ISO 9001 and ISO 14001 (ISO 9001 : quality management system and ISO 14001 : environmental management)

Approach : Plan-Do-Check-Act (PDCA) cycles

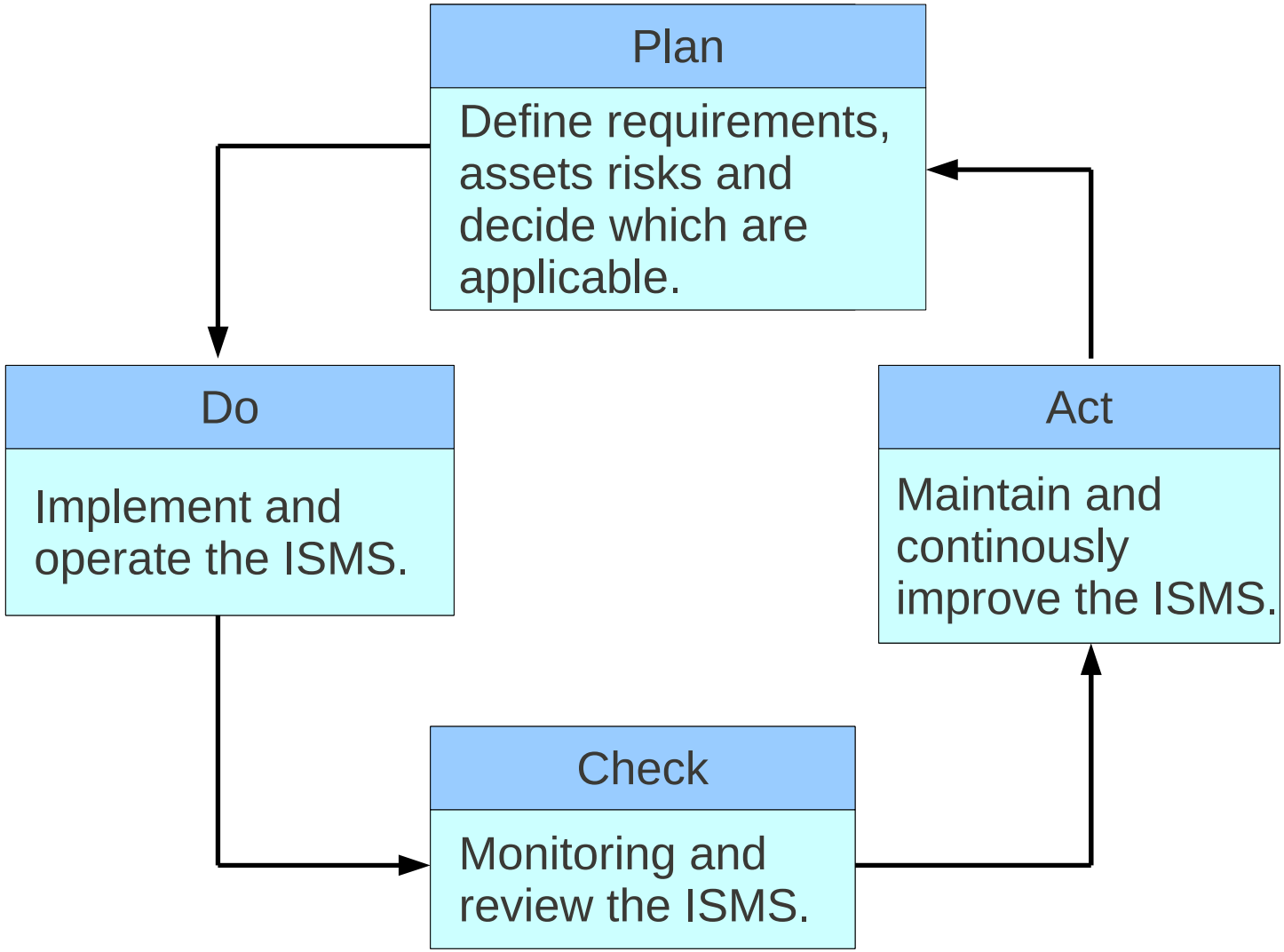

FIGURE: Description of ISO/IEC 27001 approach

ISO/IEC 27002 standard

Title of ISO/IEC 27002 :
Information technology - Security techniques - Code of practice for information security.

Created in 2005 and **replacing in 2007 ISO/IEC 17799** (created in 2000 and based on BS 7799) :
`http://www.induction.to/bs7799/`

Standard of good practices and recommendations for IS. Used for the establishment of a ISMS (identification of security measures), in order to obtain a certification ISO/IEC 27001.

Description of 39 controls objectives. Also used as *generic functional security requirement* by EBIOS (part. 5, section 3).

Security requirements of ISO 27002

- **Security policy (BPS)** : *politique de sécurité*.
- **Organisational security (BOS)** : *organisation de la sécurité*.
- **Asset classification and control (BCM)** : *classification et contrôle des actifs*.
- **Personnel security (BSP)** : *sécurité du personnel*.
- **Physical and environmental security (BPE)** : *sécurité physique et sécurité de l'environnement*.
- **Communications and operations management (BGC)** : *gestion des comunications et des opérations*.
- **Access control (BMA)** : *contrôle des accès*.
- **Business continuity management (BCA)** : *gestion de la continuité des activités de l'organisme*.
- **Compliance (BCC)** : *conformité*.

Security policy and organisational security

Information security policy (BPS_PSI).
(*politique de sécurité de l'information*).

Elaboration, communication and review of the security policy.

Information security infrastructure (BOS_ISI).
(*infrastructure de la sécurité de l'information*).

Establishment of a security management. Responsibilities for the protection of individual assets and information must be clearly defined (internal organisation).

Security of third party access (BOS_SAT) and outsourcing (BOS_SOT).
(*sécurité des accès par des tiers et sous-traitance*).

Asset classification and control

Accountability for assets (BCM_RLC).
(*responsabilités liées aux actifs*).

Global inventory of assets and services allowing to identify sensitive and essential elements with associated responsability.

Information classification (BCM_CLI).
(*classification de l'information*).

Classification and associated controls, taking into account company needs.

A set of procedures are defined for information labelling.
Example : public, sensitive, restricted, confidential, secret.

Personnel security

Security in job definition and resourcing (BSP_SPR).
(*sécurité dans la définition des postes et des resources*).

Responsability for information security, non-disclosure agreement.

User training (BSP_FOU).
(*formation des utilisateurs*).

Responding to security incidents and malfunctions (BSP_RIS).
(*réaction aux incidents de sécurité et aux défauts de fonctionnement*).

Establishment of procedures for reporting malfunctions.

Physical and environmental security

Secure areas (BPE_ZOS).
(*zone de sécurité*).

Use of security perimeters to protect zones containing information processing facilities, with a related access control.

Equipment security (BPE_SEM).
(*sécurité du matériel*).

Protection and reduction of risks from environmental threats.

General controls (BPE_MMG).
(*mesures de contrôles générales*).

Policy of clear desk and a clear screen,...

Communications and operations management

System planning and acceptance (BGC_PRS).
(*planification et recette des systèmes*).

Acceptance criteria for new information systems.

Protection against malicious software (PGC_PLM).
(*protection contre les logiciels malveillants*).

Network management (BGC_GER).
(*gestion des réseaux*).

Media handling and security (BGC_MSS).
(*manipulation et sécurité des supports*).

...

Access control

Business requirement for access control (BMA_EMA).
(*exigences de l'entreprise concernant le contrôle des accès*).

User access management (BMA_GAU).
(*gestion des accès utilisateurs*).

User responsabilities (BMA_REU).
(*responsabilités des utilisateurs*).

Selection and use of passwords,...

Network access control (BMA_MAR).
(*contrôle de l'accès aux réseaux*).

...

System development and maintenance

Security requirements of systems (BDM_ESS).
(*exigences de sécurité des systèmes*).

Business requirements for new systems, or enhancements to existing systems.

Cryptographic controls (BDM_COC).
(*mesures cryptographiques*).

Encryption of sensitive or critical information. Use of digital signature and non-repudiation services,...

Security of system files (BDM_SFS).
(*sécurité des fichiers*).

...

Business continuity management

Aspect of business continuity management (BCA_AGC). (*aspects de la gestion de la continuité des activtés de l'organisme*).

Management process for developing and maintening business continuity throughout the organization.

The development of a strategy plan must be based on an appropriate risk assessement.

Business continuity plan must be tested regulary and maintened by regular review.

Compliance

Compliance with legal requirements (BCO_CEL).
(*conformité aux exigences légales*).

Appropriate procedures must be implemented to ensure compliance with legal restrictions.

Reviews of security policy and technical compliance (BCO_RPS).
(*examens de la politique de sécurité et de la conformité technique*).

Regular reviews for compliance with security policies and standards.

System audit considerations (BCO_CAS).
(*considérations sur les audits des systèmes*).

Audits on operational systems must be carrefully planned and access to system audit tools must be protected.

Plan

ISO/IEC 27005

Title of ISO/IEC 27005 :
Information technology - Security techniques - Information security risk management.

Created in june 2008.
Revision of the standard ISO/IEC 13335
(ISO 13335 is composed of four documents (1998-2004)).

Global approach for providing guidelines for **information security risk management** (64 pages), in relation with ISO 31000 (risk management, not necessary on information security, 2009).

ISO/IEC 27005 : Outline

- Glossary
- Risk management process
- Context establishment
- Risk assessement (*appréciation du risque*) :
  - Risk analysis : Risk identification
  - Risk analysis : Risk estimation
  - Risk evaluation
- Risk treatment
- Risk acceptance
- Risk communication
- Risk monitoring and review (*surveillance et réexamen du risque*)
- Conclusion

Risk management : glossary 1/2

Risk assessment (*appréciation du risque*). The complete process combining *risk analysis* and *risk evaluation*.

Risk analysis (*analyse du risque*). Systematic use of data to identify the sources of and estimate the risk (includes *risk identification* and *risk estimation*).

Risk identification (*identification du risque*). Identification of threats and sources of attacks.

Risk estimation (*estimation du risque*). Process used to assign values to the opportunity and losses that a risk could create.

Risk evaluation (*évaluation des risques*). Process of comparing the estimated risk with the given risk criteria to determine the size of a risk.

Risk management : glossary 2/2

Risk treatment (*traitement du risque*).

Risk criteria. Reference terms allowing the importance of risks to be assessed. Sometimes called risk acceptance criteria.

Risk acceptance. (*acceptation du risque*) Decision to accept a risk treated according to the risk criteria.

Risk communication. (*communication du risque*). Exchange or sharing of information concerning the risk between the decision-maker and other parties involved.

Risk monitoring and review. (*surveillance et réexamen du risque*).

Risk management process : PDCA system

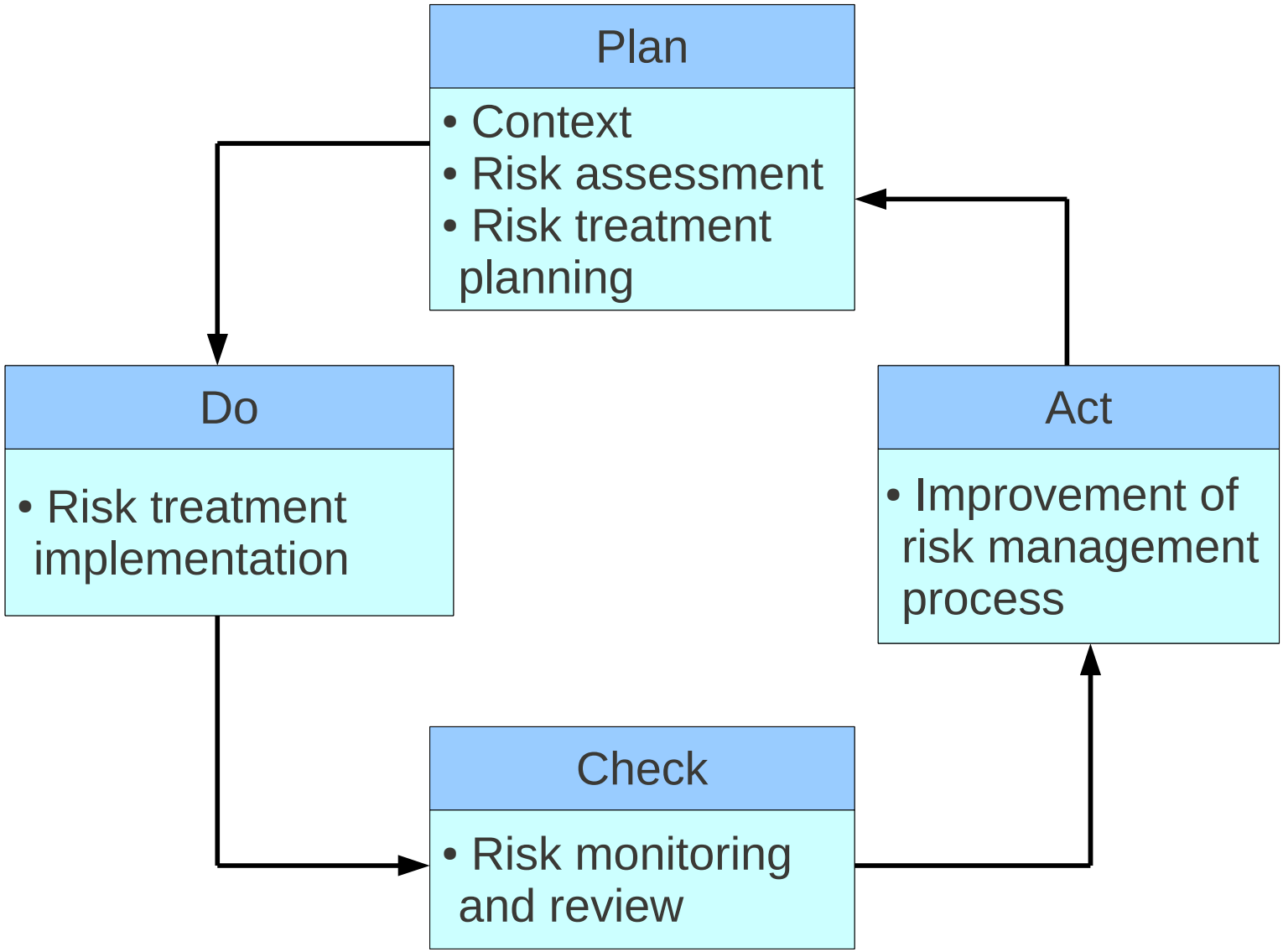

FIGURE: Information security risk management process

Risk management : approach of ISO 27005

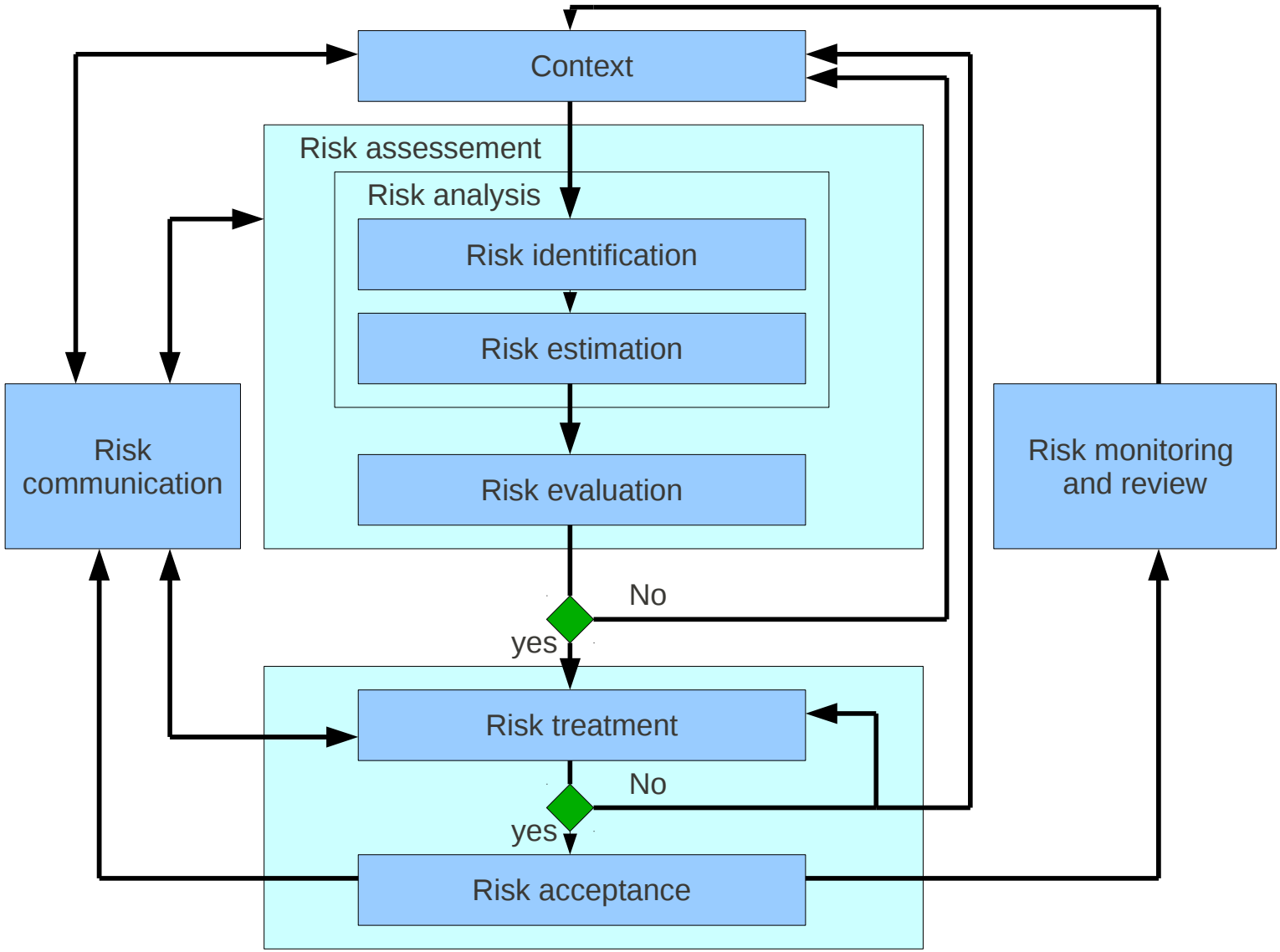

FIGURE: Risk management process : global approach

Context establishment

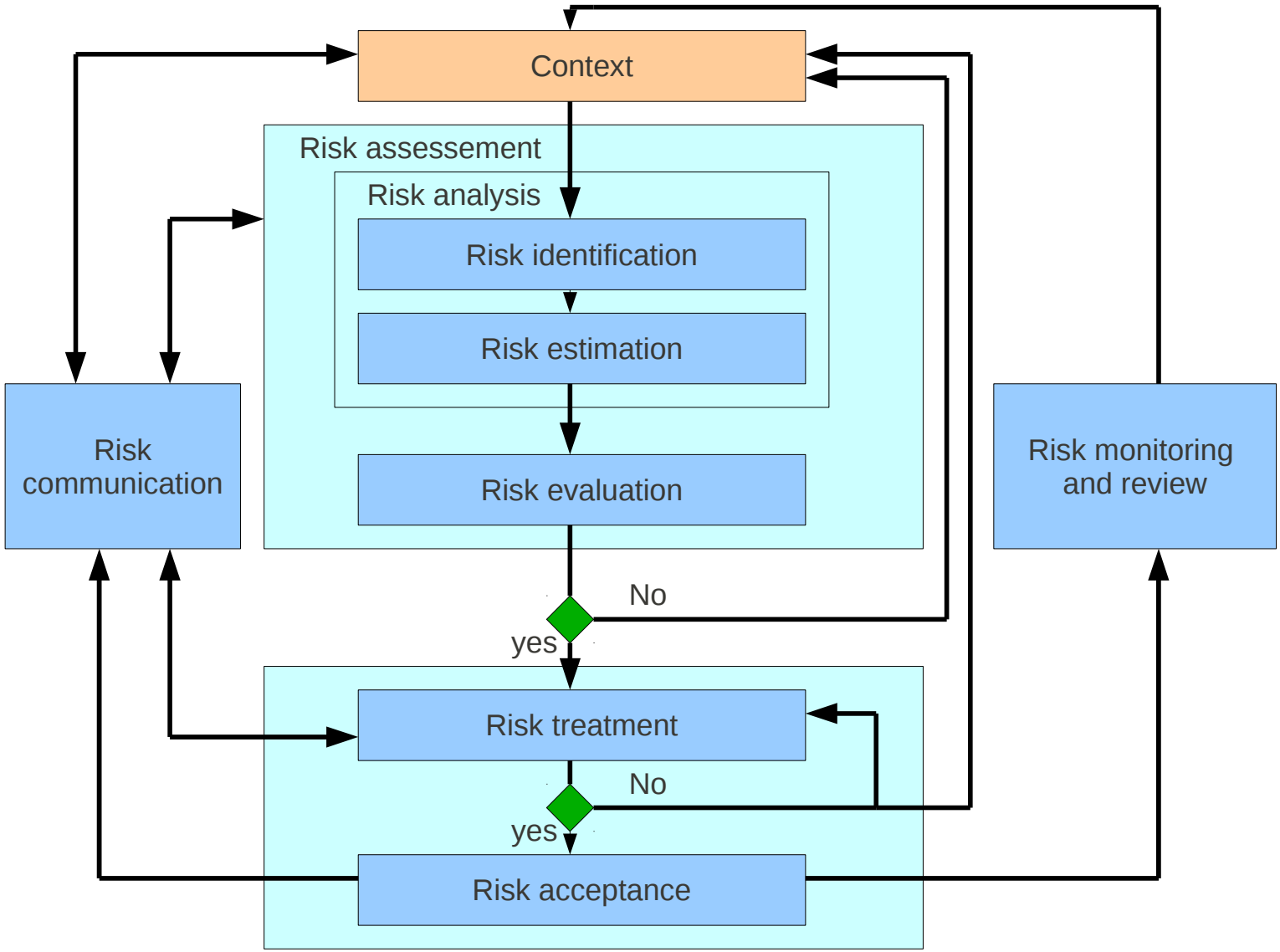

FIGURE: Risk management : Context

Scope of risk management process

Scope and boundaries are include in ISMS
(*champs et limites du processus de gestion du risque*).

Environment of risk management process
(presentation of organization, security policy, constraints of organization,...).

Target of evaluation of the risk management process
(presentation, functional description, constraints,...).

Organization of risk management process
(involved parties, responsabilities,...).

Global Approach : Risk assessement

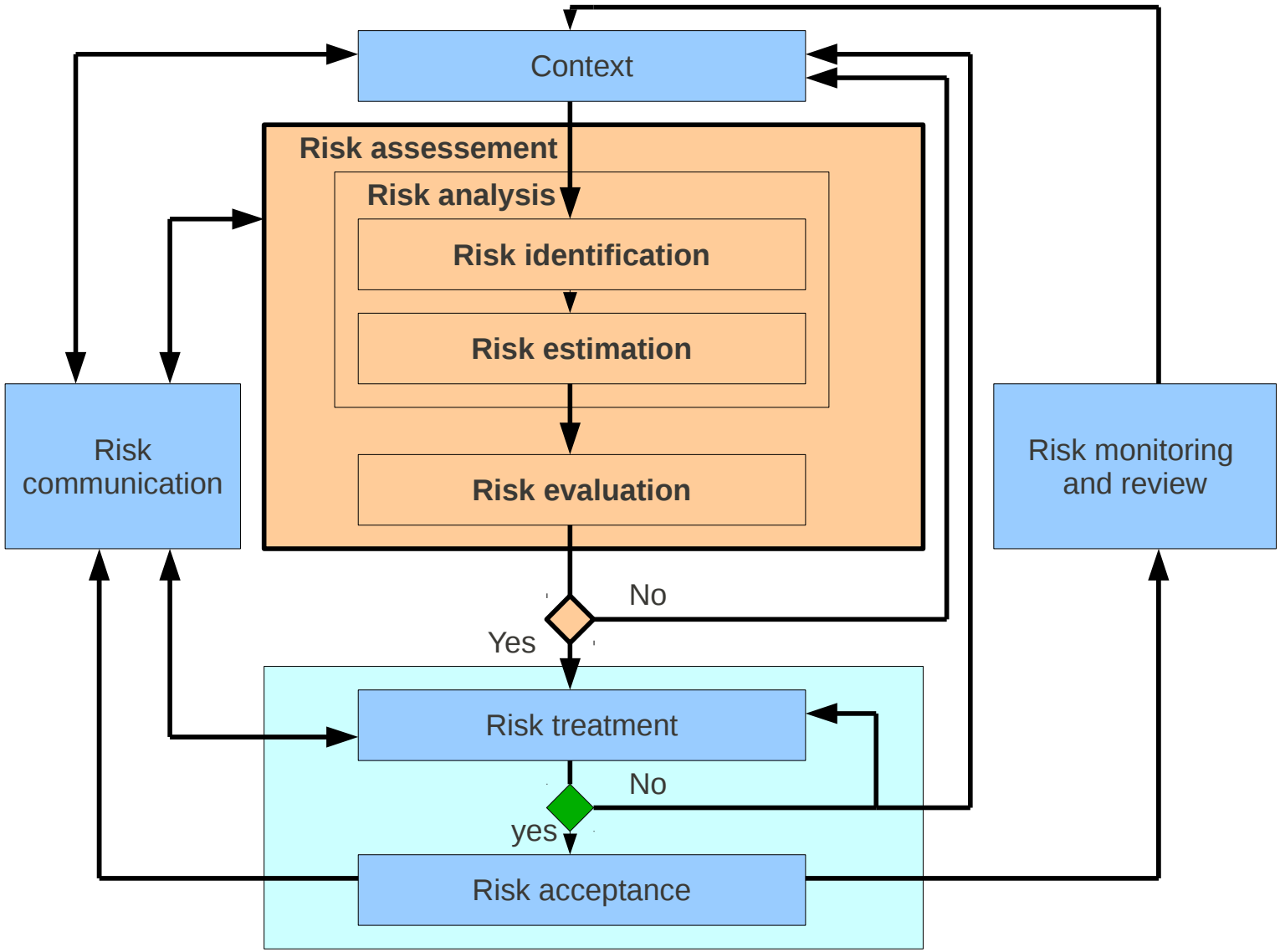

FIGURE: Risk management : risk assessement

Approach of risk assessement

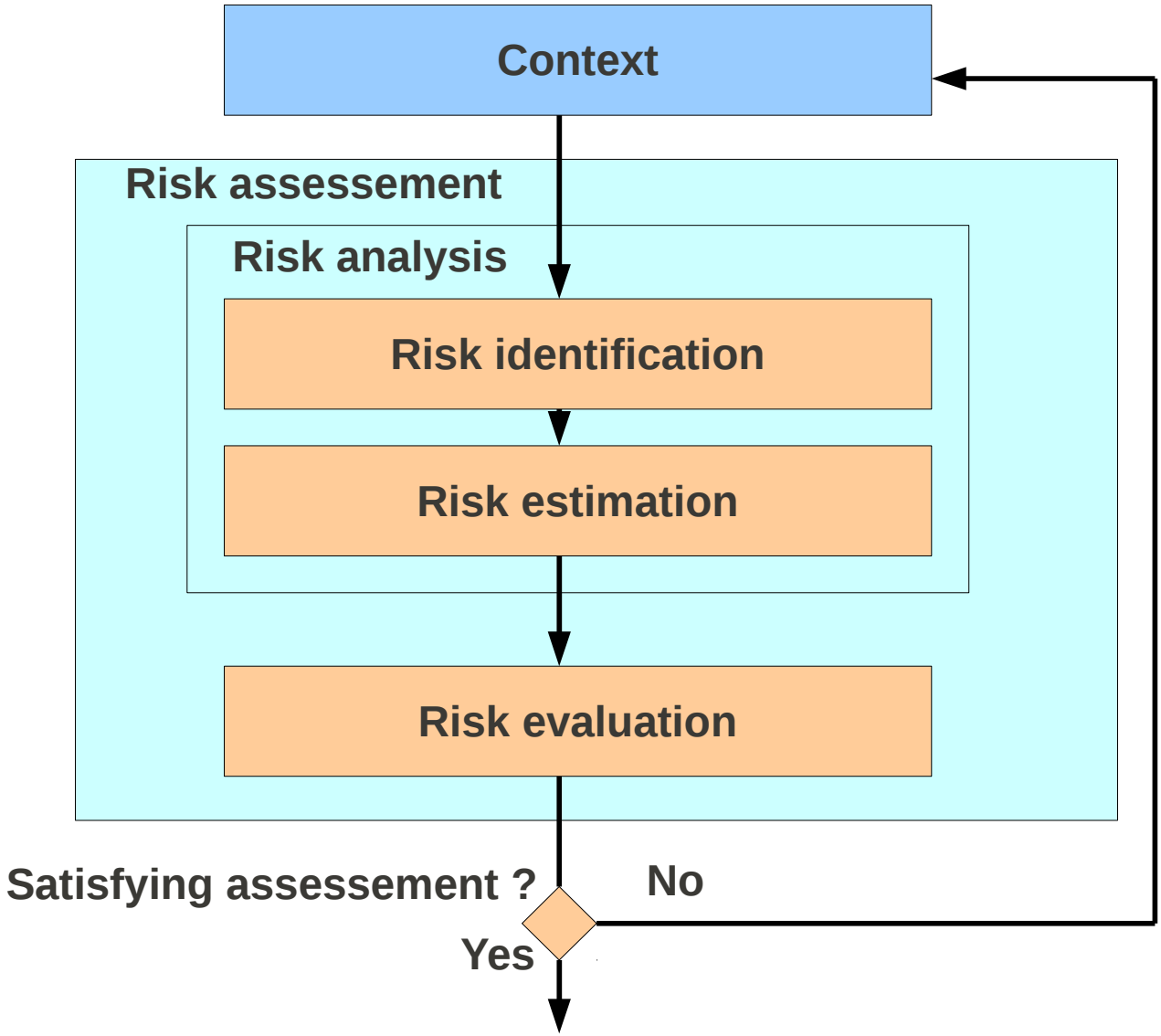

FIGURE: Approach of risk assessement

Risk identification 1/2 (risk analysis)

Asset evaluation :

Identification of any ressources of values in a list (use context), with location, functionality and responsible.

Evaluation of assets, with justification, definition of a scale and evaluation criteria.

Identification of threats :

Interview of asset responsibles and governemental authorities for a general list of threats.

Identification of type (human, environmental,..), cause (accidental, deliberate), threat agents and target system.

Risk identification 2/2 (risk analysis)

Identification of vulnerabilities :

Use the list of threats and the evaluation of assets.

Determination of active vulnerabilities (with threats) or passive vulnerabilities (without threats for now).

Identification of consequences :

Identification of type of consequences and impact from evaluation of assets (possibility of impacts of several asset).

Example : financial, human consequences,...

Evaluation of existing solutions :

Review of existing risk management process.

Risk estimation 1/2 (risk analysis)

Methods for risk evaluation :

Qualitative approach (use low, average or high for evaluation : easy to understand, but subjective).

Quantitative approach (use a precise scale of value).

Evaluation of threat likelihood of occurence :

Use threat likelihood of occurence (*Probabilité d'occurence de la menace*), depending to the type and the cause, with motivation, resources and potential of the threat agent.

Risk estimation : 2/2 (risk analysis)

Evaluation of consequences :

Use the list of consequences and impact criteria.

Analysis of vulnerabilities :

Use the list of threats, a list of vulnerabilities and existing security measures.

Estimation of risk level :

Use the estimation of consequences, the estimation of threats likelihood of occurence and the analysis of vulnerabilities.

Provides a list of risk with level.

Example of matrix of risk level (1)

Matrix of risk level with qualitative evaluation and predefined values (four level of risks) :

- Five levels for consequences (1-5).
- Five levels for likehood of ocurence of threat (1-5).

Likelihood	Consequences				
	1	2	3	4	5
1	L	L	L	M	M
2	L	L	M	M	H
3	M	M	H	H	X
4	H	H	H	X	X
5	H	X	X	X	X

L = Low ; M = Moderate ; H = High and X = Extreme

Example of matrix of risk level (2)

Matrix of risk level with qualitative evaluation and predefined values (seven level of risks) :

- Consequences based on asset value (L-M-H).
- likehood of ocurence of threat (L-M-H).
- Ease of exploitation : level of vulnerabilities (L-M-H).

Likelihood of ocurence -threat		Low			Medium			High		
Ease of exploitation		L	M	H	L	M	H	L	M	H
Asset value	L	0	1	2	1	2	3	2	3	4
	M	1	2	3	2	3	4	3	4	5
	H	2	3	4	3	4	5	4	5	6

Threat ranking depending to risk level

Example of threat ranking, where measure of risk = consequence value x likelihood of threat occurence :

Threat descriptor	Consequence	Likelihood of threat	Measure of risk	Threat ranking
Threat A	3	2	6	1
Threat B	2	1	2	3
Threat C	2	3	6	1
Threat D	2	2	4	2

Risk evaluation

Compare the estimated risk with the given risk criteria, taking account security rules, constraints and **prioritise risks**.

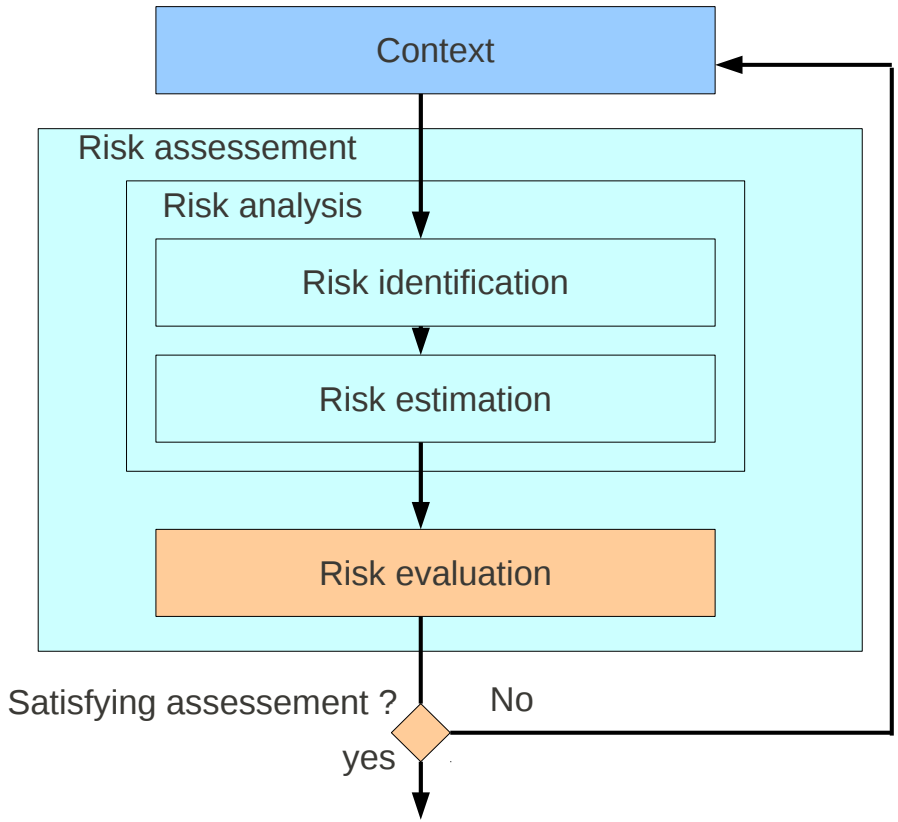

FIGURE: Risk evaluation

Risk treatment

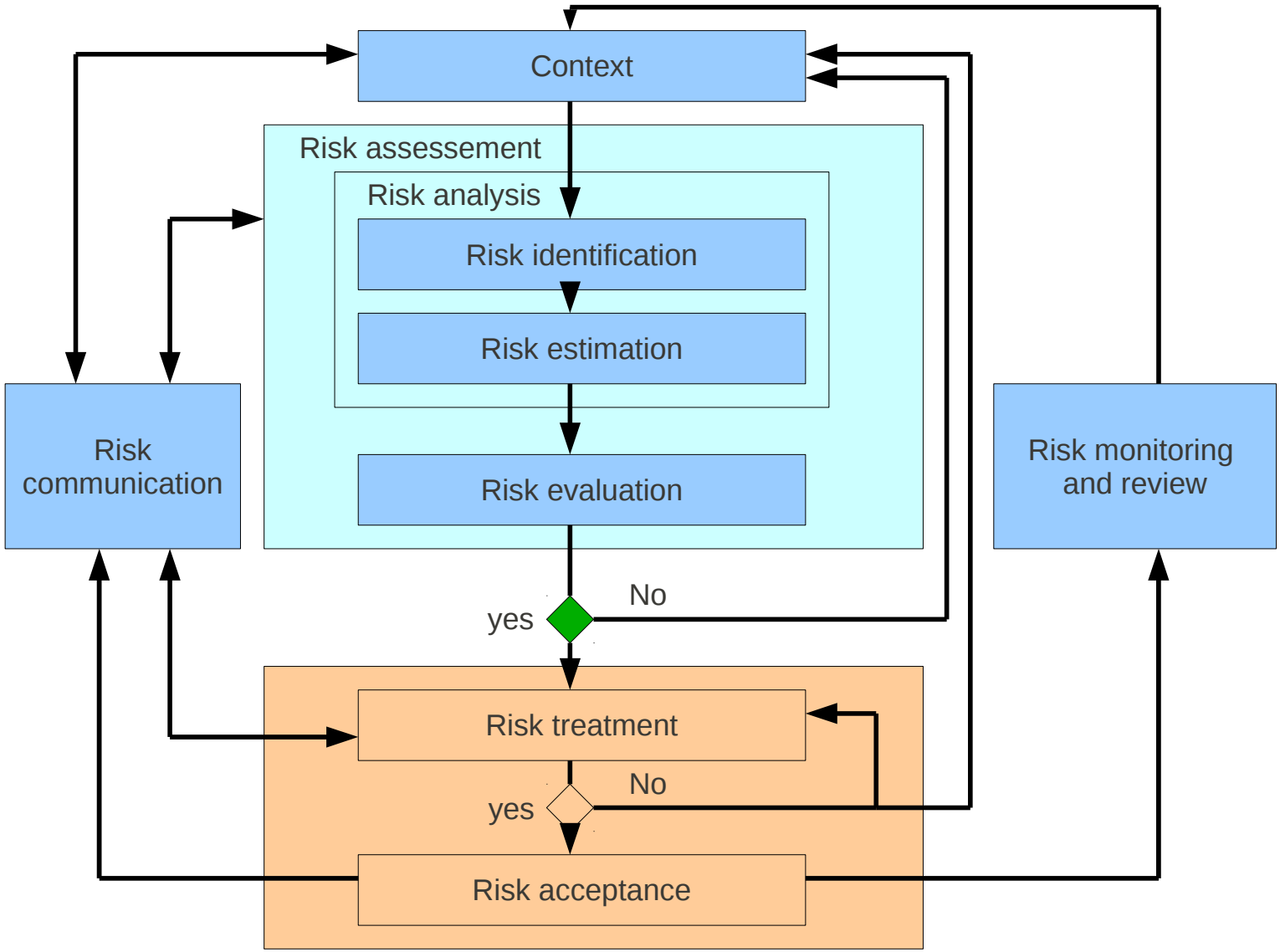

FIGURE: Risk treatment

Risk treatment

Risk avoidance (*évitement du risque*). The risk is considered as too high.

Risk transfer (*transfert du risque*). Sharing with another party the possible loss associated with a particular risk.

Risk reduction (*réduction du risque*). Process aiming to minimise the negative consequences and opportunities of a threat. Called sometimes risk mitigation (*atténuation du risque*).

Risk retention (*prise de risque*). Acceptance of the possible loss associated with a particular risk. Used when risk level is lower than risk acceptance criteria.

Risk Communication

Exchange or sharing of information concerning the risk between the decision-maker and other parties involved.

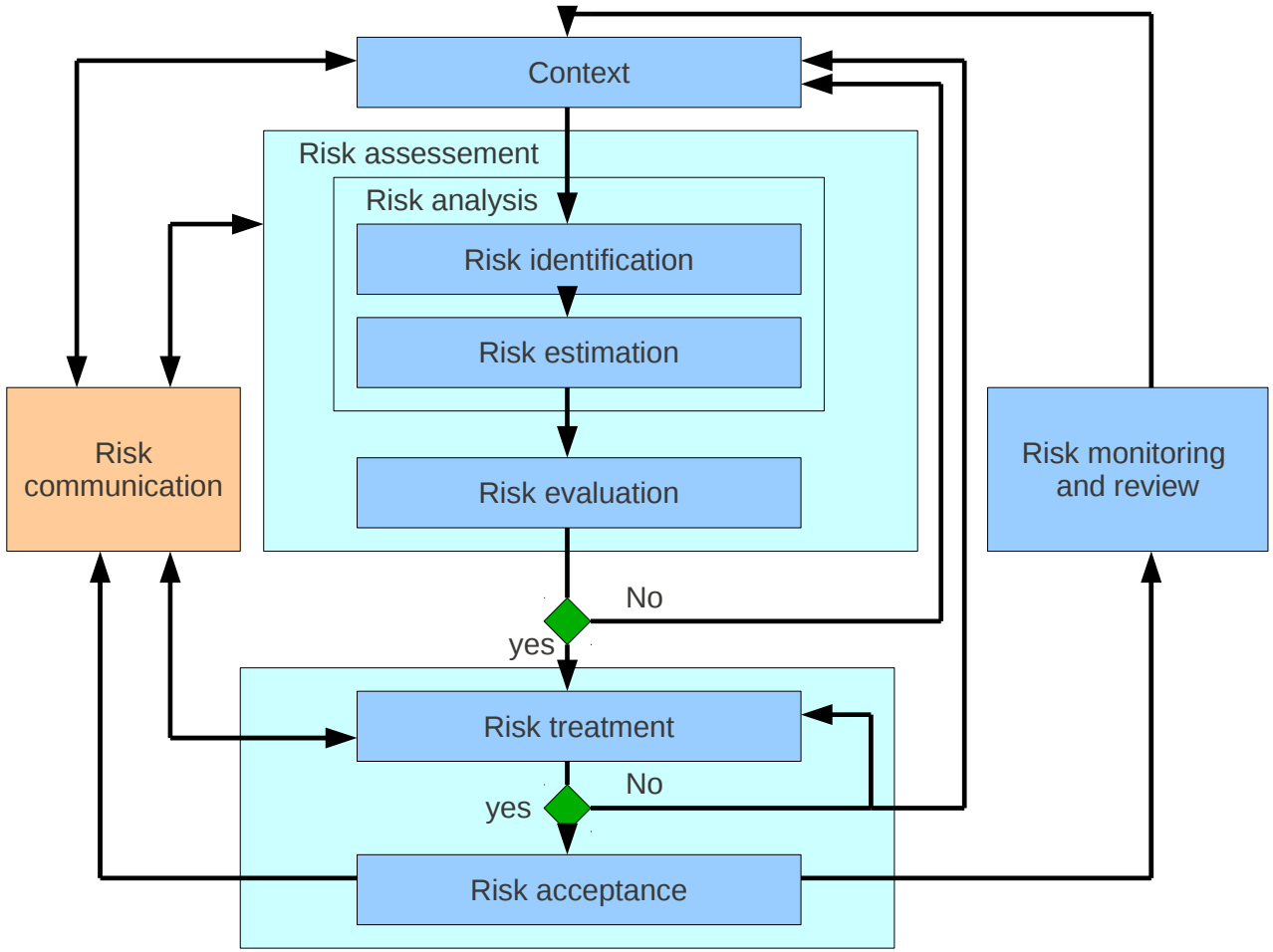

FIGURE: Risk communication

Risk monitoring and review

New threats, new likelihood of threat occurences, change in economical or legal context.

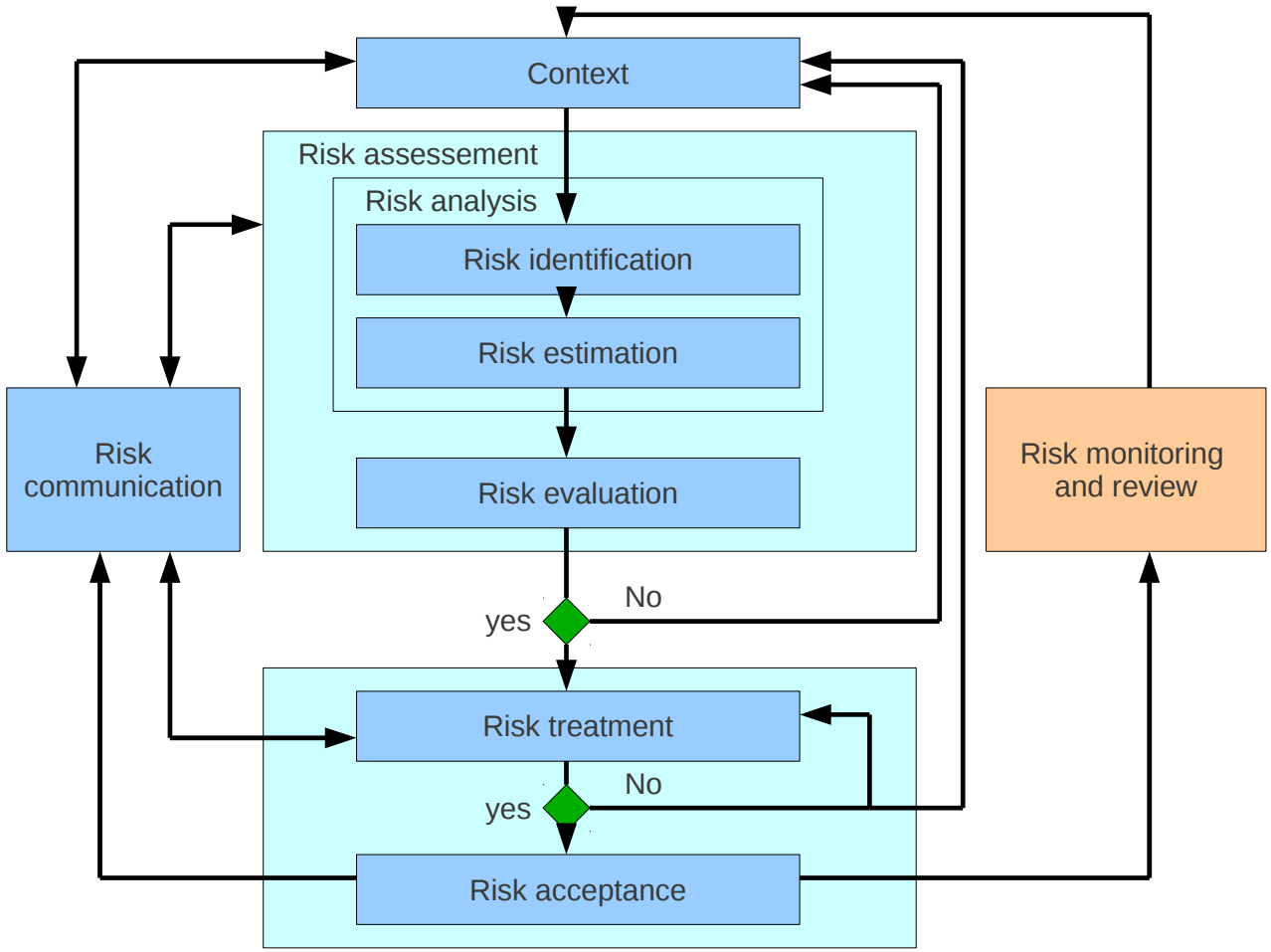

FIGURE: Risk monitoring and review

Plan

Common Criteria

Common Criteria for Information Technology Security Evaluation.

Current version : 3.1, july 2009.
(previous version : 2.3 in 2005).

The current version is available on web site :
`http://www.commoncriteriaportal.org/cc/`

Developped by several countries (including ANSSI), and accepted by ISO organization under the reference **ISO 15408**.

Scope of evaluation

Common Criteria provides a set of requirements for evaluation of the security functionality of IT products or systems.

IT = Information technology.
CC = Common Criteria.

The CC is flexible, with a range of evaluation methods to be applied to several security properties of many IT products.

The CC does not contain security evaluation criteria on measures not related directly to the IT security functionality.

Requirements on cryptographic algorithms are not covered by the Common Criteria.

Organization of the document

Organization of the CC :

1. Part 1 : Introduction and general model (93 pages).
2. Part 2 : Security functional components (321 pages).
3. Part 3 : Security assurance components (232 pages).

Target audience of CC

Provide assurance that the specification, the implementation and the evaluation of a IT target product has been realized in a standardized method

Users of the IT target product specify their security functional requirements.

Developers implement the security attributes of their IT target product.

Evaluators as testing laboratories evaluate the IT target product and determine if it meets the security claims.

Target of evaluation (TOE)

During the evaluation, the Information technology system or product is called **target of evaluation (TOE)**.

A TOE is typically a set of software, firmware (*micro logiciel ou logiciel embarqué*) and/or hardware.

Example of TOE are software application as antivirus system, operating system, smartcard, cryptographic devices, databases, firewalls, biometrics controls, ...

Assets and operational environment

Assets are entities that someone places value upon.

Examples of assets include :

- contents of a file or a server
- the authenticity of votes during an election
- the availability of an electronic commerce process

The environment(s) in which these assets are located is called the **operational environment**.

Examples of operational environments are :

- the computer room of a bank
- a computer connected to internet

General security concepts and relationships

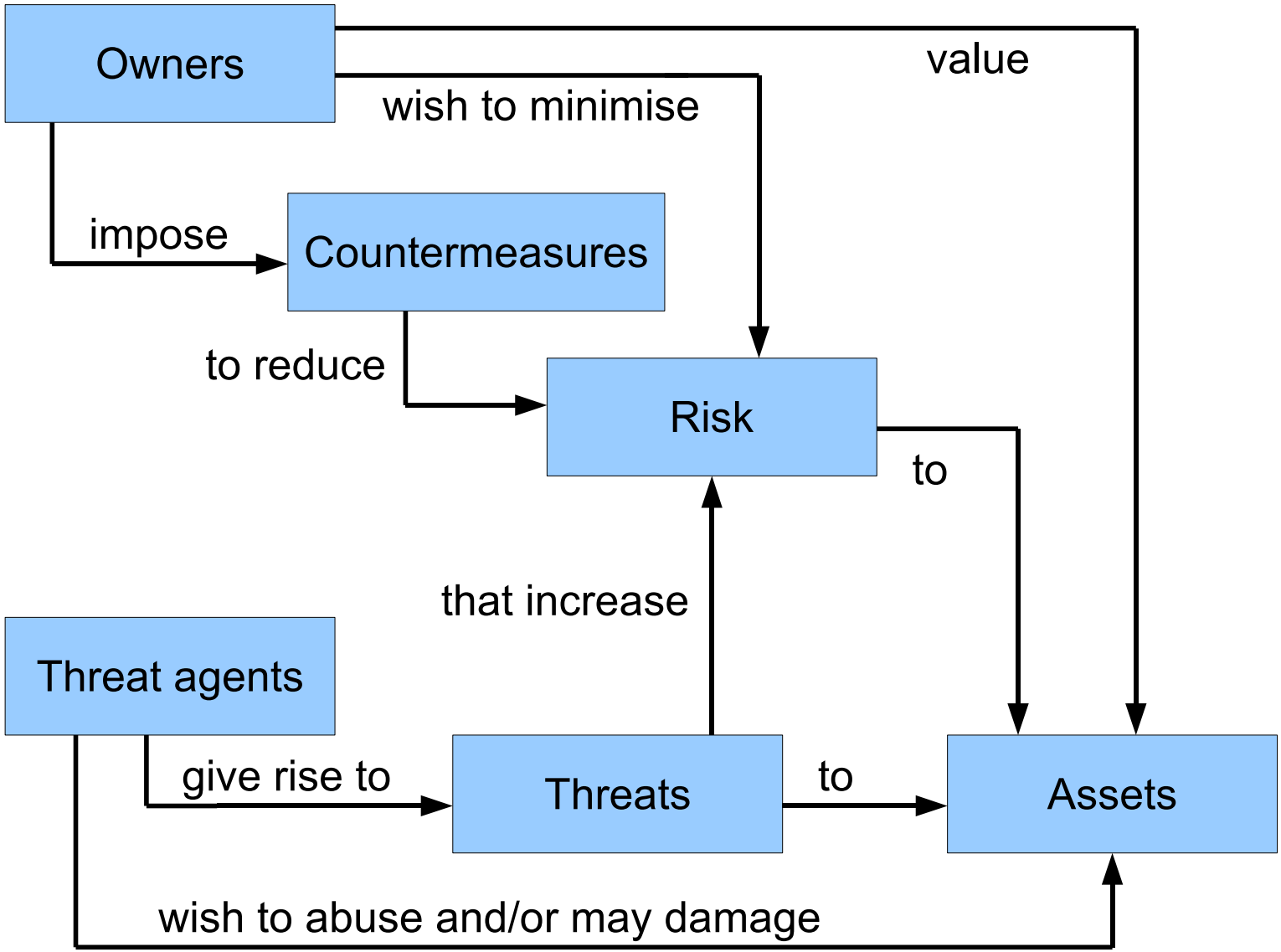

FIGURE: General security concepts and relationships (CC)

Evaluation concepts and relationships

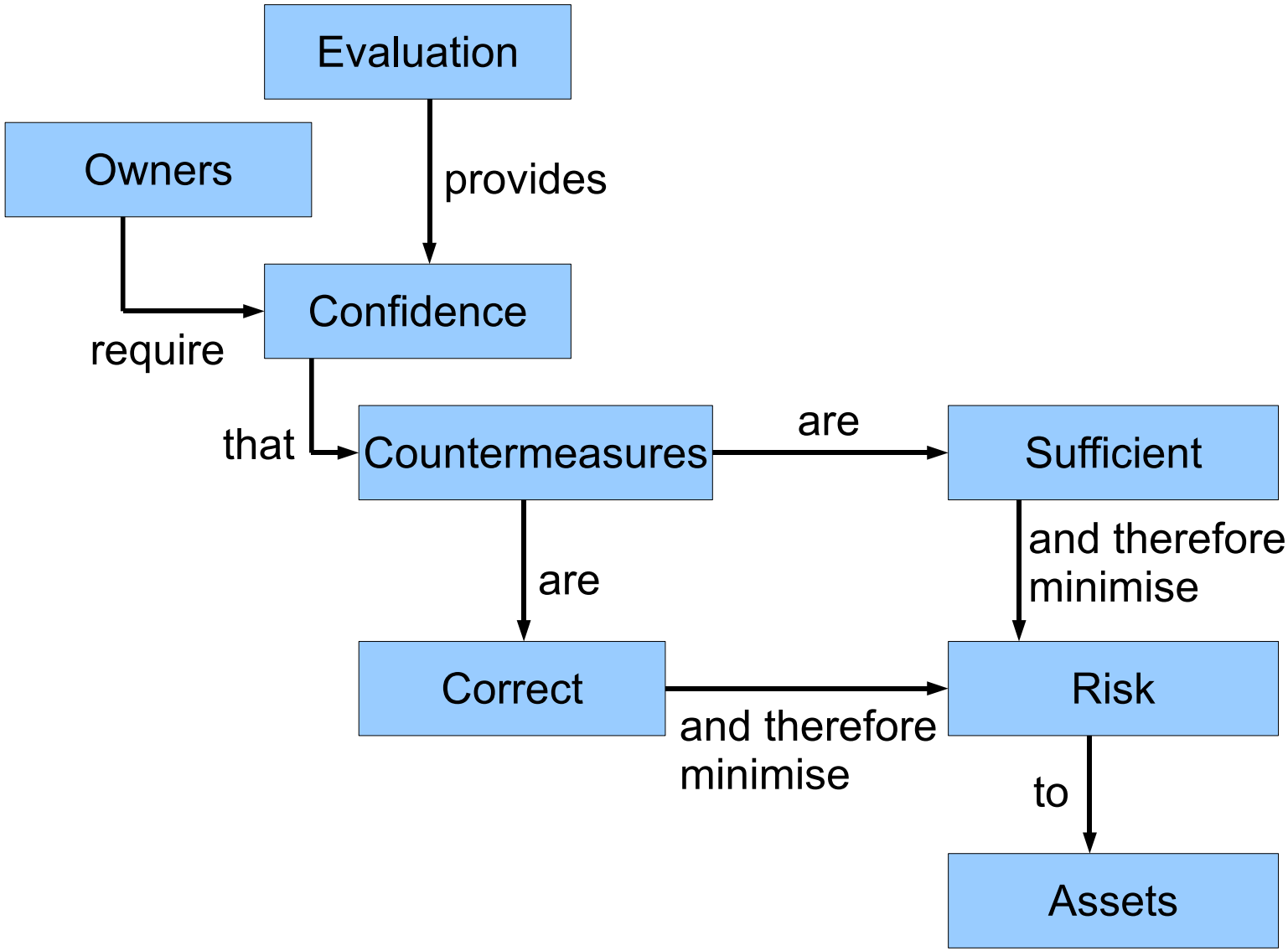

FIGURE: Evaluation concepts and relationships (CC)

Assets and countermeasures

The countermeasures must be **sufficient** : the threats are countered if the countermeasures do what they claim to do.

Sufficiency of the countermeasures is analyzed through the Security Target using the **Security functional Requirements (SFR)** (*exigences fonctionnelles de sécurité*).

The countermeasures must be **correct** : the countermeasures do what they claim to do.

Requirements for correctness of the TOE are proposed in the Security Target, using **the Security Assurance Requirements (SAR)** (*exigences d'assurance de sécurité*).

Protection Profile and Security Target

Security Target (ST) and Protection Profile (PP) are two key concepts in common criteria.
The Security Target depends to a Protection Profile.

Security Target (*Cible de sécurité*).
Implementation-dependent statement of security needs for a specific identified TOE.

Protection Profile (*Profil de protection*).
Implementation-independent statement of security needs for a TOE type.

For example, a protection profile concerns a network firewall, and a security target concerns a proposed firewall.

Simplified view of Security Target

The Security Target describes the **assets**, the **threats** on these assets, the **countermesaures** (called **Security Objectives**), and demonstrates that they are sufficient to counter the threats.

The countermeasures are divided in two groups : the **security objectives for the TOE** and the **security objectives for the operational environment**.

Security objective for the TOE are detailed in a **standardized language** in the **SFR**.

Correctness of the TOE is detailed in the SAR and correctness of the operational environment is only assumed.

Security Target content

1. Security Target introduction (ASE_INT)
2. Conformance claims (ASE_CCL)
3. Security problem definition (ASE_SPD)
4. Security objectives (ASE_OBJ)
5. Optional components (ASE_ECD)
6. Security requirements (ASE_REQ)
7. TOE summary specification (ASE_TSS)

Protection profile and package

A package is a set of security requirements :

1. A functional package containing only SFRs.
2. An assurance package containing only SARs.

Examples of assurance packages are the evaluation assurance levels (EALs). There are no predefined functional packages.

An ST describes requirements for a TOE and is written by the developer, while a PP describes the general requirements for a TOE type and is typically realized by a user community or a governement.

Protection Profile content

1. Security Target introduction (APE_INT)
2. Conformance claims (APE_CCL)
3. Security problem definition (APE_SPD)
4. Security objectives (APE_OBJ)
5. Optional components (APE_ECD)
6. Security requirements (APE_REQ)

Relation between PP and ST

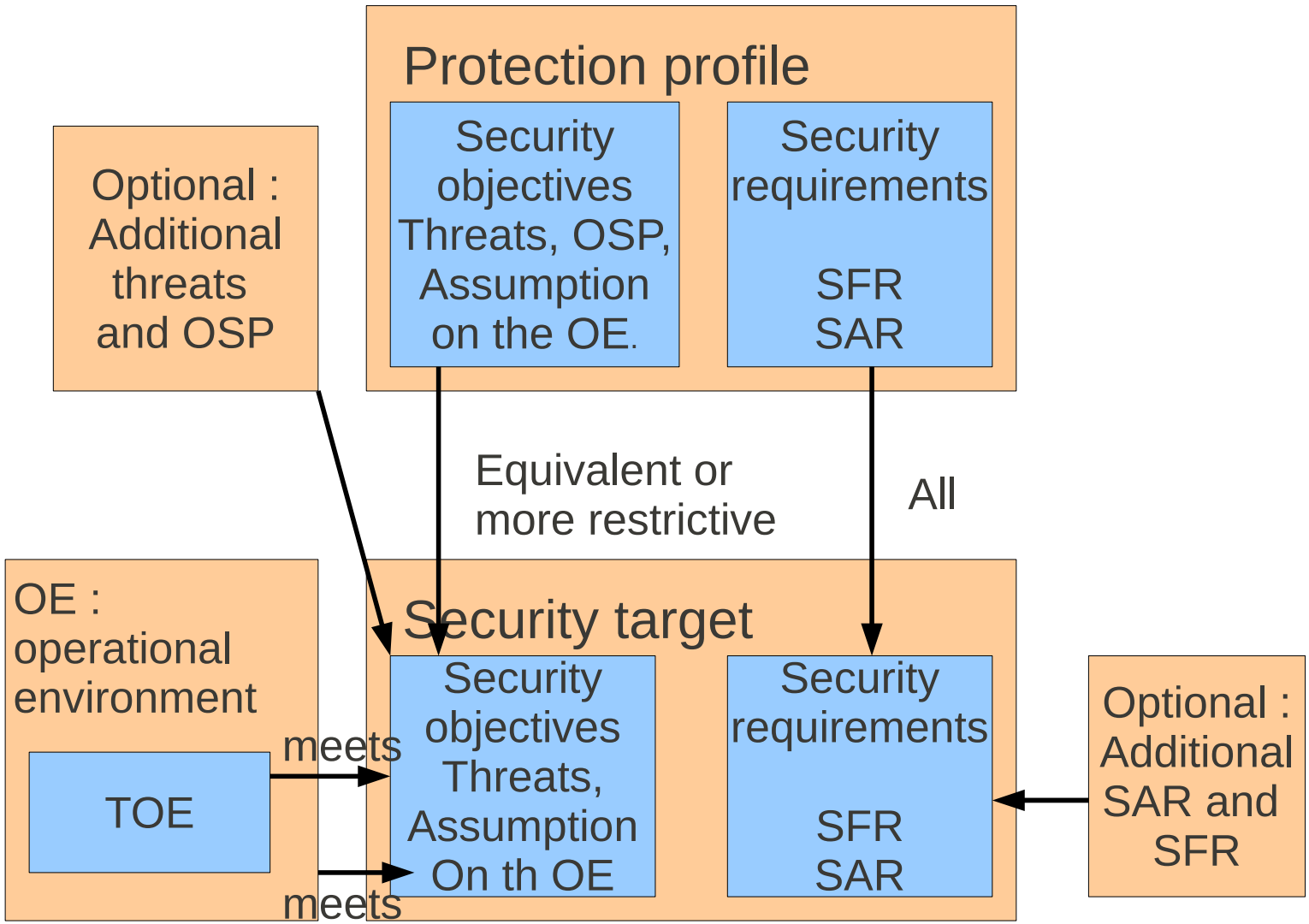

FIGURE: Relation between PP and ST

Security functional components

1. Security audit (class FAU)
2. Communication (class FCO)
3. Cryptographic support (class FCS)
4. User data protection (class FDP)
5. Identification, authentification (class FIA)
6. Security management (class FMT)
7. Privacy (class FPR)
8. Protection of the TSF (class FPT)
9. Resource utilisation (class FRU)
10. TOE access (class FTA)
11. Trusted path/channels (class FTP)

Security assurance requirements

Assurance is used for confidence that an IT product meets its security objectives.

Establishment of a **security assurance levels (EAL)** (*niveau d'assurance de l'évaluation*).

- **EAL1 :** functionally tested.
- **EAL2 :** structurally tested.
- **...**
- **EAL7 :** formally verified design and tested.

The EAL defines a set of required security assurance components, classes and families.

Security assurance classes

1. Class APE : Protection Profile Evaluation.
2. Class ASE : Security Target Evaluation.
3. Class ADV : Development.
4. Class AGD : Guidance Documents.
5. Class ALC : Life-cycle support.
6. Class ATE : Tests.
7. Class AVA : Vulnerability assessement.
8. Class ACO : Composition

Plan

Security Target content

1. Security Target introduction (ASE_INT)
2. Conformance claims (ASE_CCL)
3. Optional components (ASE_ECD)
4. Security problem definition (ASE_SPD)
5. Security objectives (ASE_OBJ)
6. Security requirements (ASE_REQ)
7. TOE summary specification (ASE_TSS)

Security Target introduction (ASE_INT)

The security target introduction is divided in three parts :

1. The ST reference and the TOE reference.
2. The TOE overview.
3. The TOE description.

The **ST reference** and the **TOE reference** for identification (title, author, date, version, keywords,..).

The **TOE overview** with a brief description of the TOE(several paragraphs). This description is intended to give a general idea of what the TOE is capable in terms of security. Identification of the **TOE type** (firewall, smartcard, web server,...).

TOE description

The **TOE description** with more details : a list of all security devices that constitute the TOE (hardware and software), with a description of group users and their security attributes.
This description is expected to be in more detail than the major security features described in the TOE overview.

Eventually a **description of the assets and data of the TOE**, with the sensibility of these assets (confidentiality, integrity, availability,...) as proposed by the Ebios method

Data	Confidentiality	Integrity	Availability
D.data1		x	x
D.data2	x	x	

Conformance claims (ASE_CCL)

Description of the compliance of the ST with :

- The part 2 and 3 of Common criteria. The version of C must be precised and if requirements of extended security are needed or not.
- Protection Profile (if any), with a list and a description of conformance of the ST.
- Packages (if any),with a list and a description of conformance of the ST.

Security problem definition (ASE_SPD)

Provide a list and a precise description of

1. Threats
2. Organisational security rules
3. Assumptions

Security problem definition : threats

A **threat** consists of an adverse action performed by a threat agent (individual entities or group of entities) on an asset.

List of different threats that are to be countered by the TOE or the organisational environment, with a description of resources, opportunity and motivation :

N	Threat	Description
1	T.threat1	...
2	T.threat2	...

Examples : Replay attack, insecure state during the start-up of the TOE, a system administrator violating user privacy, a technical failure of the server,...

Security problem definition : organisational security rules

Organisational security rules (OSP) are security rules, procedures, or guidelines imposed by an organisation for the TOE or the operational environment.

List of organisational security policies, with a precise description of them :

N	OSP	Description
1	OSP.policy1	...
2	OSP.policy2	...

Examples : Anonymity of authorized individual, all products must be compliant with national standard for password generation,...

Security problem definition : assumptions

Assumptions are hypothesis on the operational environment in order to be able to provide security functionality.

List and description of assumptions :

N	Assumptions	Description
1	A.assumption1	...
2	A.assumption2	...

Examples : Trust in the administrator, Linux OS is used,...

During the evaluation these assumptions are considered to be true : they are not tested in any way.

Security objectives (ASE_OBJ)

This section is divided in four parts :

1. High-level solution
2. Security objectives for the TOE
3. Security objectives for the operational environment
4. Relation between security objectives and security problem.

Security objectives for the TOE

Concise and high-level statement on the TOE of the intended solution to certain problem defined by the security problem definition.

N	Objective	Description
1	O.objective1	...
2	O.objective2	...

Examples :
The TOE shall kepp confidential the content of all files transmitted between it and a server, the TOE shall identify and authenticate all users before allowing them access to a service provided by the TOE.

Security objectives for the operational environment

Concise, high-level statement on the operational environment of the intended solution to certain problem defined by the security problem definition.

N	Objective	Description
1	OE.objective1	...
2	OE.objective2	...

Examples :
The Linux version executing the TOE, the trust of the administrator needs a constant formation,...

Relation between security objectives and security problem

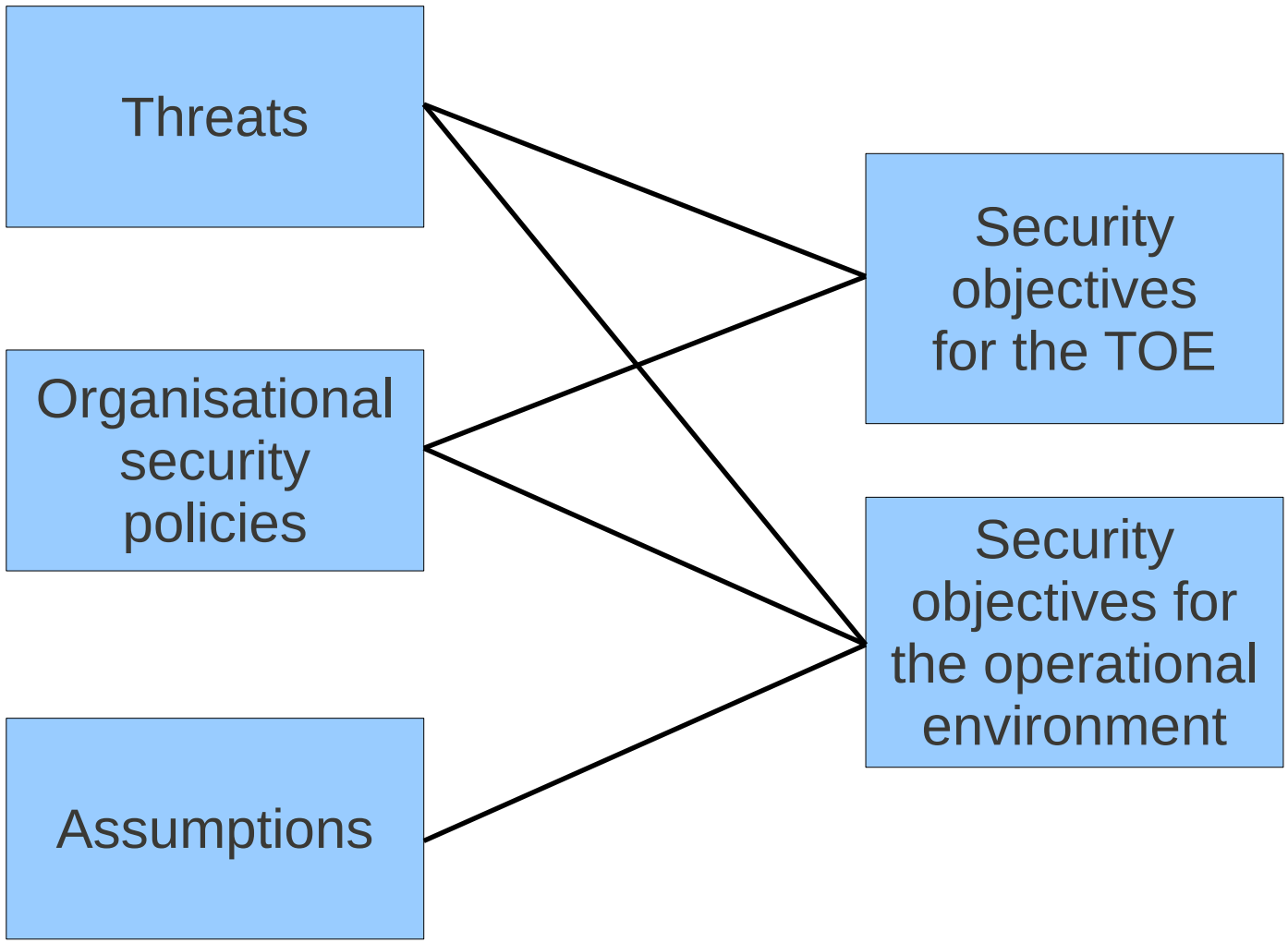

FIGURE: Relation between security objectives and security problem

Relation between security objectives and security problem

Relation between security objectives and security problem definition. Several lines of justification, removing or diminishing each threats :

T.threat1 : precise description of the threat.
OE.objective1 : used for a solution to the threat1.

...

OSP.policy1 : precise description of this rule.
O.objective1...
OE.objective1...

...

A.assumption1 : ...
OE.objective1 ..

Relation between security objectives and security problem

Establishment of a globale table for the relation between security objectives and security problem definition :

	O.obj1	O.obj2	...	OE.obj1	OE.obj2	...
T.threat1		x		x		
T.threat2				x		
OSP.policy1	x			x		
OSP.policy2				x		
A.assumption1				x		
A.assumption2				x	x	
...						

Extended components definition (ASE_ECD)

Optional components :
Security requirements is based on components of part 2 and part 3. However, additional family can be defined.

Example : an additional family of the class FCS (cryptographic support) can be described : the family of Random Number Generation, called FCS_RNG. A description of the family behaviour, dependencies to other families,...

Security requirements (ASE_REQ)

The security requirements consist of two groups of requirements :

1. Security functional requirements (SFR)
2. Security assurance requirements (SAR)

Security functional requirements (SFR)

Translation of the security objectives into a standardized language (use part 2 of this document).

Provide a SFR - TOE security objective mapping (with justification for each objectives) :

	O.obj1	O.obj2	O.obj3
family1	x		
family2	x	x	
family3			x

Security assurance requirements (SAR)

Description of how the TOE is to be evaluated. Uses a standardized language and explains why the SAR is appropriate (use part 3 of this document).

Provides the level of the EAL and the corresponding security assurance families.

Additional security assurance families are possible.

TOE summary specification (ASE_TSS)

Description of how the TOE satisfies all the SFRs.

This section is only used in the Security Target (ST), not in the Protection Profile (PP).

Example :
The family FDP_ACC (Cryptographic key management) is realized by the TOE in this way...

Plan

Security functional components (part. 2 of CC)

Security functional components are the basis for the security functional requirements (SFR) expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST.

Almost all security families are presented in the following section.

Correspondance between part. 2 of CC and *Generic functional security requirements* of EBIOS (part 5, section 3).

Functionnal classes and families

1. Security audits (class FAU) : *audit de sécurité*.
2. Communication (class FCO) : *communication*.
3. Cryptographic support (class FCS) : *support cryptographique*.
4. User data protection (class FDP) : *protection des données de l'utilisateur*.
5. Identification, authentification (class FIA) : *identification et authentification*.
6. Security management (class FMT) : *administration de la sécurité*.
7. Privacy (class FPR) : *protection de la vie privée*.
8. Protection of the TSF (class FPT) : *protection de la TSF*.
9. Resource utilisation (class FRU) : *utilisation des ressources*.
10. TOE access (class FTA) : *accès à la TOE*.
11. Trusted path/channels (class FTP) : *chemins et canaux de confiance*.

Security audits 1/3 (class FAU)

Security audit automatic response (FAU_ARP).
(*réponse automatique de l'audit de sécurité*).

The response to be taken in case of detected events, indicative of a potential security violation (action to inform authorized user, to end the violation, to limit impacts,..).

Security audit data generation (FAU_GEN).
(*génération des données de l'audit de sécurité*).

Recording the security relevant events (with date, time, type of event, outcome), and identification of types of events that are auditable, with the identity of the user that caused the event.

Security audit 2/3 (class FAU)

Security audit analysis (FAU_SAA).
(*analyse de l'audit de sécurité*).

Requirements on automated methods that analyse system activity, with several attacks heuristics (simple, complex) and several profile target groups (single user, group ID, system).

Security audit review (FAU_SAR).
(*revue de l'audit de sécurité*).

Requirements for authorized users to obtain and interpret audit information (selection of the audit data to be reviewed and definition of used criteria as basic informations or parameters).

Security audit 3/3 (class FAU)

Security audit event selection (FAU_SEL).
(*sélection des événements de l'audit de sécurité*).

Requirements for the selection of the set of events to be audited from the set of all auditable events (determined in FAU_GEN), for example depending to the identity of the object or user.

Security audit event storage (FAU_STG).
(*stockage d'événements de l'audit de sécurité*).

Requirements for storing audit data for later use, including requirements controlling the loss of audit information due to failure, attack and/or exhaustion of storage space.

Communication (class FCO)

Non repudiation of origin (FCO_NRO).
(*non-répudiation de l'origine*).

Assure the identity of the origin of transmitted information (for example with a digital signature).
Two levels : a selective proof or a mandated proof of origin.

Non-repudiation of receipt (FCO_NRR).
(*non-répudiation de la réception*).

Assure the identity of the receipt of transmitted information (for example with a digital signature).
Two levels : a selective proof or a mandated proof of receipt.

Cryptographic support (class FCS)

Cryptographic key management (FDP_ACC).
(*gestion de clés cryptographiques*).

Key management must be based on a assigned standard (national or international standard). Includes typically key generation (depends to FCS_COP), key distribution, key access and key destruction.

Cryptographic operation (FCS_COP).
(*opération cryptographiques*).

Must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. Includes typically operations for data encryption, digital signature, message authentication code,...

User data protection 1/5 (class FDP)

Access control policy (FDP_ACC).
(*politique de contrôle d'accès*).

Definition of the scope of access control of the policies, related to the SFP. This scope is characterized by three sets : subjects, objects and operations controlled by subjects and objects.

Access control functions (FDP_ACF).
(*fonctions de contrôle d'accès*).

Description of the rules for the specific functions that can implement an access control policy named in previous access control policy (FDP_ACC).

User data protection 2/5 (class FDP)

Data authentication (FDP_DAU).
(*authentification des données*).

Description of method used to verify that the information content has not been forged or modified, possibly with a proof of data authentication.

Export from the TOE (FDP_ETC).
(*Exportation vers une zone hors de contrôle de la TSF*).

Description of functions for user data export from TOE such that its security attributes either can be explicitly preserved or can be ignored.

User data protection 3/5 (class FDP)

Import from outside of the TOE (FDP_ITC).
(*importation depuis une zone hors du contrôle de la TSF*).

Mechanisms for importing of user data into the TOE such that it has appropriate security attributes and is appropriately protected.

Internal TOE transfer (FDP_ITT).
(*transfert interne à la TOE*).

Requirements that address protection of user data when it is transferred between separated parts of a TOE across an internal channel, particulary for integrity protection.

User data protection 4/5 (class FDP)

Residual information protection (FDP_RIP).
(*protection des informations résiduelles*).

Any data in a resource is not available when the resource is de-allocated from one object and reallocated to a new object.

Rollback (FDP_ROL).
(*annulation*).

Involves undoing the last operation, bounded by some limit, such as a period of time, and return to a previous known state.

Stored data integrity (FDP_SDI).
(*intégrité des données stockées*).

Protection of user data while it is stored, instead of Internal TOE Transfert (FDP_ITT) used for the transfer.

User data protection 5/5 (class FDP)

Inter-TSF user data confidentiality transfer protection (FDP_UCT).
(*protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF*).

Requirements for ensuring the confidentiality of user data when it is transferred using an external channel between the TOE and another trusted IT product.

Inter-TSF user data integrity transfer protection (FDP_UIT).
(*protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF*).

Requirements for providing integrity for user data in transit between the TOE and another trusted IT product and recovering from detectable errors.

Identification, authentication 1/3 (class FIA)

Authentication failures (FIA_AFL).
(*échecs de l'authentification*).

Requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures.

User attribute definition (FIA_ATD).
(*définition des attributs de l'utilisateur*).

Description of the set of security attributes, other than the user's identity, that is used to enforce the SFRs (e.g. groups, access rights).

Identification, authentication 2/3 (class FIA)

Specification of secrets (FIA_SOS).
(*spécification de secrets*).

Requirements for mechanisms on provided secrets (e.g. size of keys) and generate secrets (e.g. pseudo-random number generator).

User authentication (FIA_UAU).
(*authentification de l'utilisateur*).

Description of authentication mechanisms and definition of the required attributes on which the user authentication mechanisms must be based.

Identification, authentication 3/3 (class FIA)

User identification (FIA_UID).
(*identification de l'utilisateur*).

Definition of required identity that users shall provide before performing any other actions, which require user identification.

User-subject binding (FIA_USB).
(*lien utilisateur-sujet*).

Requirements to create and maintain the association of the user's security attributes to a user's subject.

Security Management 1/3 (class FMT)

Management of functions in TSF (FMT_MOF).
(*administration des fonctions de la TSF*).

Control by authorised users over the management of functions in the TSF, for example, the audit functions or the definition of user security characteristics.

Management of security attributes (FMT_MSA).
(*administration des attributs de sécurité*).

Control by authorised users over the management of security attributes. For example capabilities for viewing and modifying of security attributes, as group, roles and rights.

Security Management 2/3 (class FMT)

Management of TSF data (FMT_MTD).
(*administration des données de la TSF*).

Control by authorised users over the management of TSF data (For example audit informations, clock and other TSF configuration parameters).

Revocation (FMT_REV).
(*révocation*).

Rights management for revocation of security attributes.

Security Management 3/3 (class FMT)

Security attribute expiration (FMT_SAE).
(*expiration des attributs de sécurité*).

Capability to enforce time limits for the validity of security attributes (for example, key certificates such as ANSI X509 or access control attributes).

Security management roles (FMT_SMR).
(*rôles pour l'administration de la sécurité*).

Reduces the likelihood of damage resulting from users abusing their authority by taking actions outside their assigned functional responsibilities.

Privacy 1/2 (class FPR)

Anomymity (FPR_ANO).
(*anonymat*).

Ensures that a user may use a resource or service without disclosing the user's identity.

Pseudonymity (FPR_PSE).
(*possibilité d'agir sous un pseudonyme*).

Ensures that a user may use a resource (or service) without disclosing its identity, but can still be accountable for that use.

Privacy 2/2 (class FPR)

Unlinkability (FPR_UNL).
(*impossibilité d'établir un lien*).

Ensures that a user may make multiple uses of resources or services without others being able to link these uses together.

Unobservability (FPR_UNO).
(*non-observabilité*).

Ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

Protection of the TSF 1/5 (class FPT)

Fail secure (FPT_FLS).
(*mode sûr après défaillance*).

Failure with preservation of secure state. The TSF preserve a secure state in the face of the identified failures.

Availability of exported TSF data (FPT_ITA).
(*disponibilité de données de la TSF exportées*).

Inter-TSF availability requires that the TSF ensure, to an identified degree of probability, the availability of TSF data provided to another trusted IT product.

Protection of the TSF 2/5 (class FPT)

Confidentiality of exported TSF data (FPT_ITC).
(*confidentialité des données de la TSF exportées*).

Inter-TSF confidentiality requires that the TSF ensures that data transmitted between the TSF and another trusted IT product is protected from disclosure while in transit.

Integrity of exported TSF data (FPT_ITI).
(*intégrité des données de la TSF exportées*).

Detection and correction of modification TSF data during transmission between the TSF and another trusted IT product.

Protection of the TSF 3/5 (class FPT)

Internal TOE TSF data transfer (FPT_ITT).
(*transfert des données de la TSF à l'intérieur de la TOE*).

Protection of TSF data when it is transferred between separate parts of a TOE across an internal channel.

TSF physical protection (FPT_PHP).
(*protection physique de la TSF*).

Restrictions on unauthorised physical access to the TSF, and resistance to, unauthorised physical modification of the TSF.

Protection of the TSF 4/5 (class FPT)

Trusted recovery (FPT_RCV).
(*reprise sûre*).

The TSF must determine that the TOE is started up without protection compromise and can recover without protection compromise after discontinuity of operations.

Replay detection (FPT_RPL).
(*détection de rejeu*).

The replay of identified entities must be detected, eventually with specific actions.

Protection of the TSF 5/5 (class FPT)

State synchrony protocol (FPT_SSP).
(*protocole de synchronisation d'états*).

Ensures that two distributed parts of the TOE (e.g. hosts) have synchronised their states after a security-relevant action, using for example return receipt.

Time stamps (FPT_STM).
(*horodatage*).

Requirements for a time stamp function within a TOE.

Resource utilisation (class FRU)

Fault tolerance (FRU_FLT).
(*tolérance aux pannes*).

Protection against unavailability of capabilities caused by failure of the TOE.

Priority of service (FRU_PRS).
(*priorité de service*).

Ensures that the resources will be allocated to the more important tasks and not monopolised by lower priority tasks.

Resource allocation (FRU_RSA).
(*allocation des ressources*).

Provides limits on the use of available resources, preventing users from monopolising the resources, such that DOS.

TOE access 1/2 (class FTA)

Limitation on multiple concurrent sessions (FTA_MCS).
(*limitation du nombre de sessions parallèles*).

Limits on the number of concurrent sessions that belong to the same user.

Session locking and termination (FTA_SSL).
(*verrouillage de session*).

Capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

TOE access 2/2 (class FTA)

TOE access history (FTA_TAH).
(*historique des accès à la TOE*).

Display to a user, upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account.

TOE session establishement (FTA_TSE).
(*établissement d'une session de la TOE*).

Requirements to deny a user permission to establish a session with the TOE (based on attributes).

Trusted path/channels (class FTP)

Inter-TSF trusted channel (FTP_ITC).
(*canal de confiance inter-TSF*).

Requirements for the creation of a trusted channel between the TSF and other trusted IT products for the performance of security critical operations.

Trusted path (FTP_TRP).
(*chemin de confiance*).

Requirements to establish and maintain trusted communication to or from users and the TSF. A trusted path may be required for any security-relevant interaction.