Ebios method

Patrick Lacharme

ENSICAEN

2010-2011

Plan

Presentation of EBIOS method

This presentation is directly based from EBIOS guideline : `www.ssi.gouv.fr`.

Description of Ebios version 2 (2004), modified in 2010.

EBIOS means Expression of Needs and Identification of Security Objectives (*Expression des Besoins et Identification des Objectifs de Sécurité*).

Proposed by **ANSSI** (Agence Nationale de la Sécurité des systèmes d'information), and created in **1997** by the **DCSSI**.

Presentation

EBIOS is used to assess and treat risks relating to ISS (elaboration of a protection profile, a ISS policy,...).

Compatibility of EBIOS method with internationals standards such as **common criteria** and **ISO 27000 suite**.

Languages : french, english, german, spanish.

Widely used in France and international (European Union, Quebec, Tunisia, ..) by numerous organizations.

Widely used in the public sector (ministries, administration) and in the private sector (small and large companies).

Ebios guide

Ebios, version 2 in french :

1. Section 1 : Introduction (22 pages).
2. Section 2 : Demarche (27 pages).
3. Section 3 : Techniques (47 pages).
4. Section 4 : Outillage pour l'appréciation des risques SSI (81 pages).
5. Section 5 : Outillage pour le traitement des risques SSI (284 pages)

A concrete example of EBIOS :
Etude d'un cas : @rchimed company (140 pages).

Outline

EBIOS guide (in english, version 2) is composed of five sections :

1. **Introduction :** Context, advantages and positioning of the EBIOS approach, biliography, glossary.
2. **Approach :** The running of the activities of the method.
3. **Techniques :** Description of means for accomplishing the activities of EBIOS which must be adapted to the organization's needs and practices.
4. **Tools for assessing ISS risks :** Types of entity, attack methods and vulnerabilities.
5. **Tools for treating ISS risks :** Security objectives, security requirements, table for determining functional security objectives and requirements.

Target system and assets

Target system (*système cible*) :

System evaluated by the method (TOE in common criteria).

Asset (*bien*) :

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

Entity (*entité*) :

An asset such as an organization, site, personnel, equipment, network, software, system.

Essential element (*élément essentiel*) :

Information or function with at least one non-nil sensitivity.

Plan

Presentation of the approach

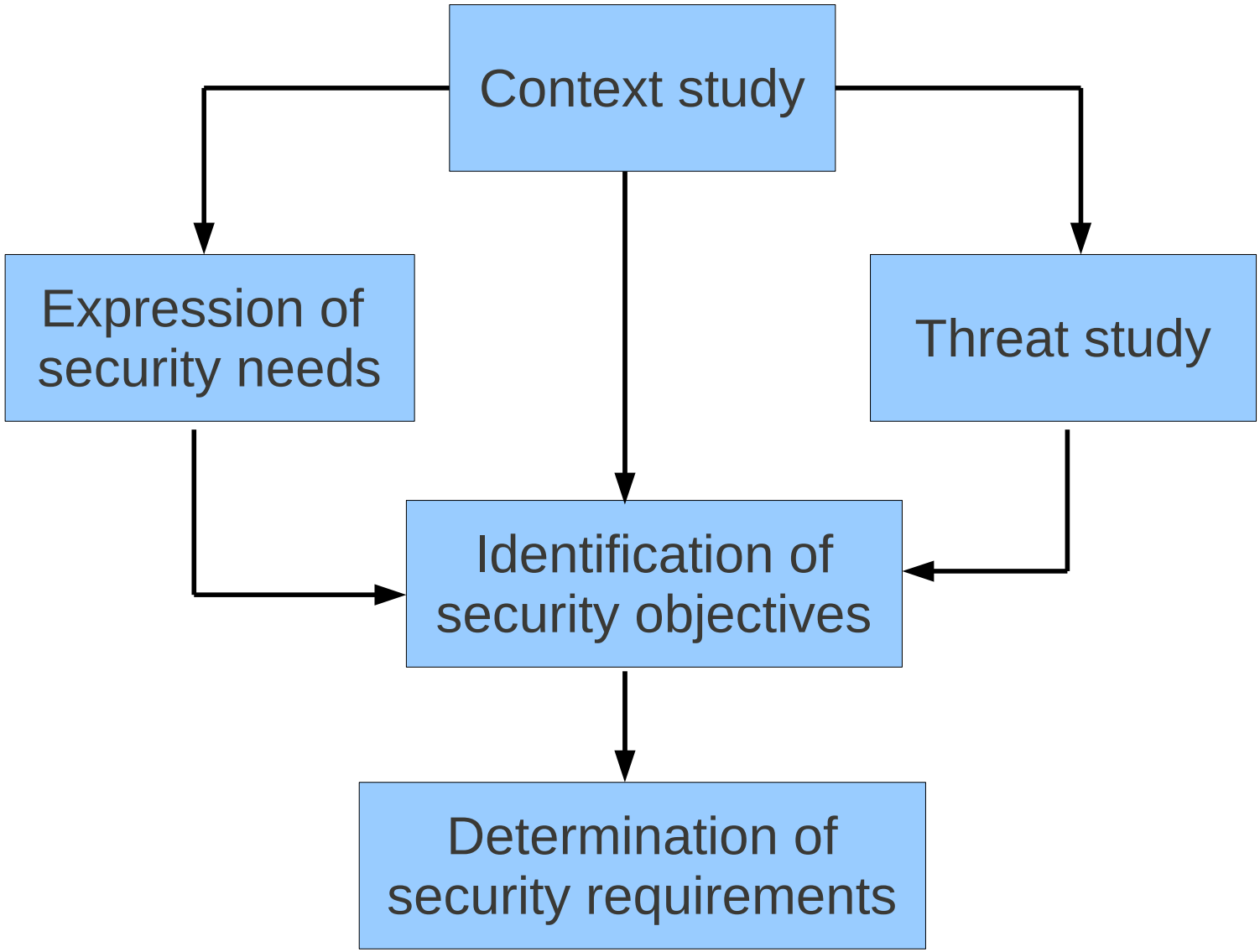

FIGURE: EBIOS global approach

Description of the approach (1/2)

First step : **Context study**

- Presentation of the organisation, environment, purpose and operation of target system.
- Identification of essential elements and entities of the target system.

Second step : **Expression of security needs**

- Risk assessement (contribution to risk estimation).
- Impact formalisation (with a scale of needs).
- Evaluation of security needs of the essential elements (availability, integrity, confidentiality).

Description of the approach (2/2)

Third step : **Threat study**

- Risk assessement (contribution to risk analysis).
- Identification of the threats affecting the system.
- Identification of vulnerabilities on the target system.

Fourth step : **Identification of security objectives**

- Contribution to risk evaluation and risk treatments.
- Formalisation of the real risks affecting the system.
- Description of security objectives.

Fifth step : **Determination of security requirements**

- Contribution to risk treatment.
- Description to security functional requirements.
- Description to security assurance requirements.

Description of a PSSI

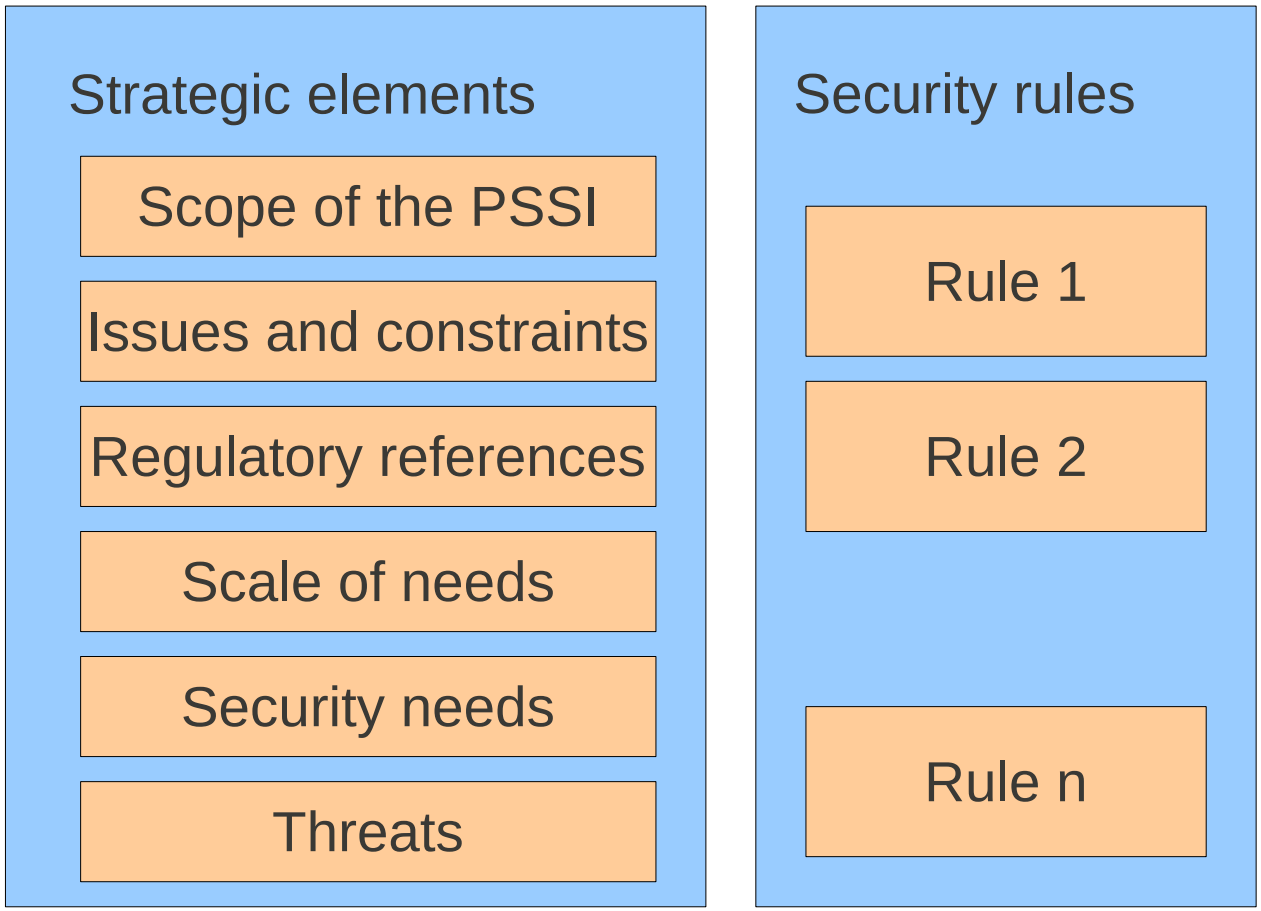

FIGURE: PSSI description

Application of Ebios for a PSSI

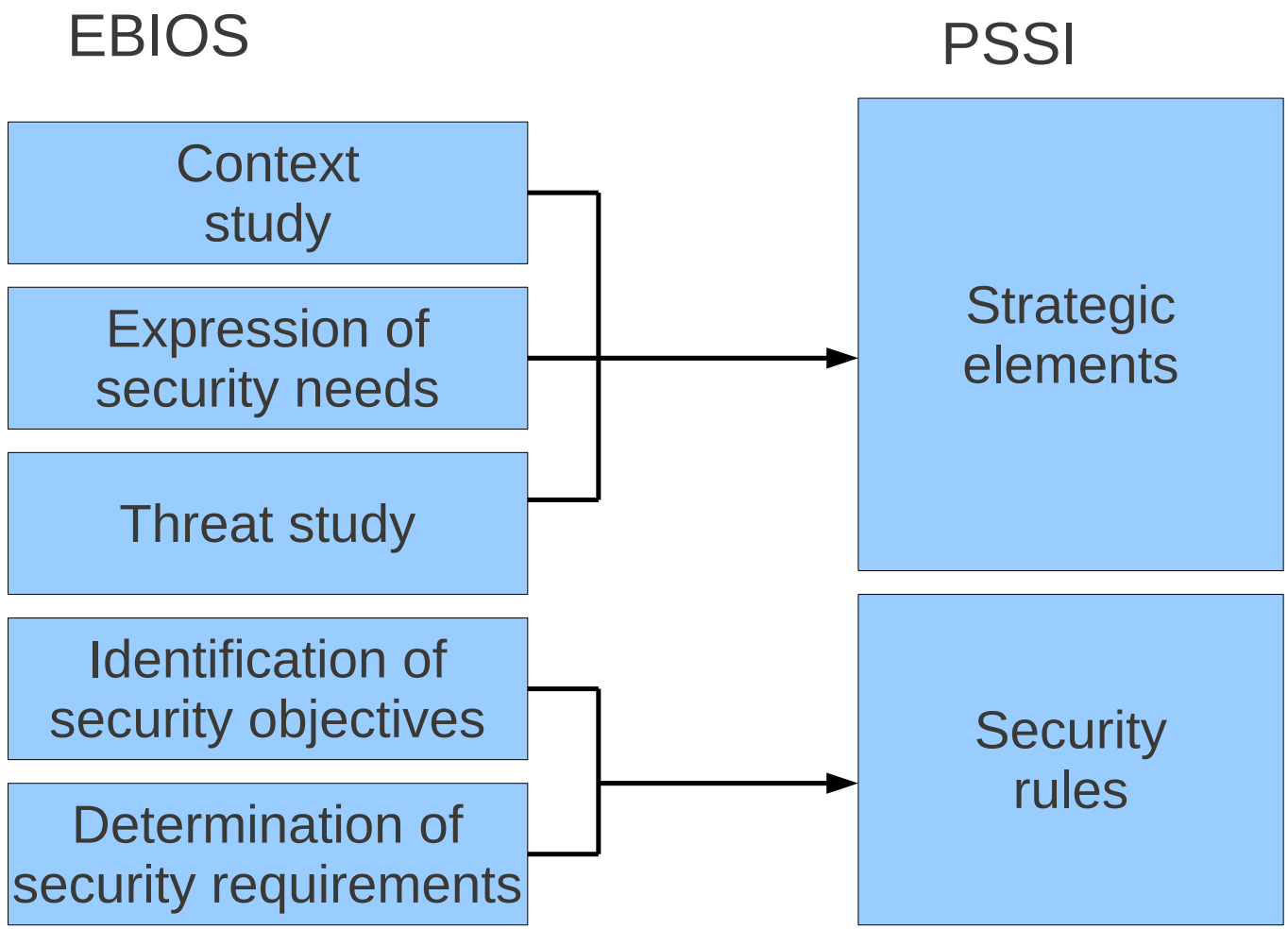

FIGURE: Application of Ebios for a PSSI

Application of Ebios for a Protection profile

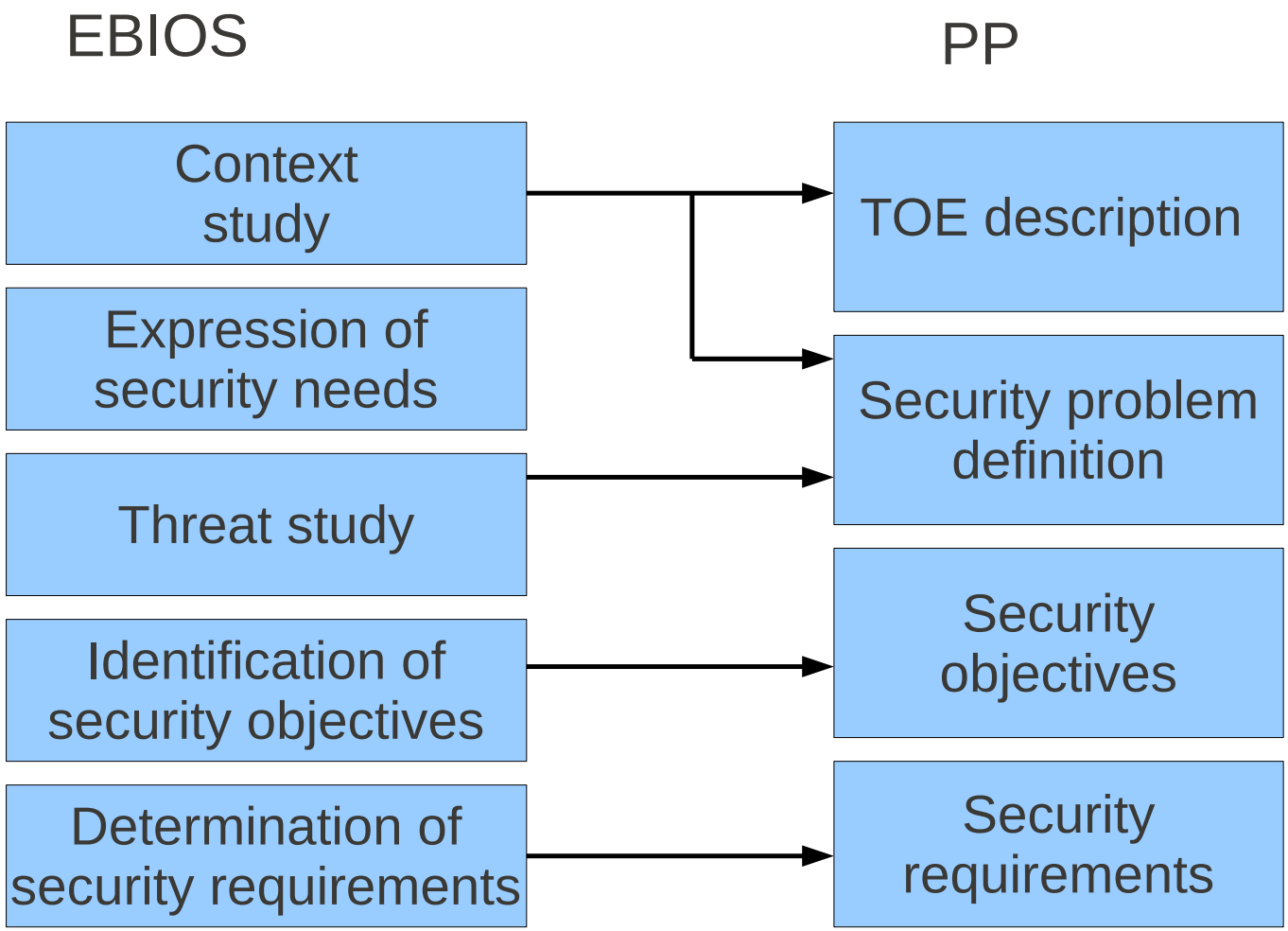

FIGURE: Application of Ebios for a Protection profile

Application of Ebios for a ISO 27000 ISMS

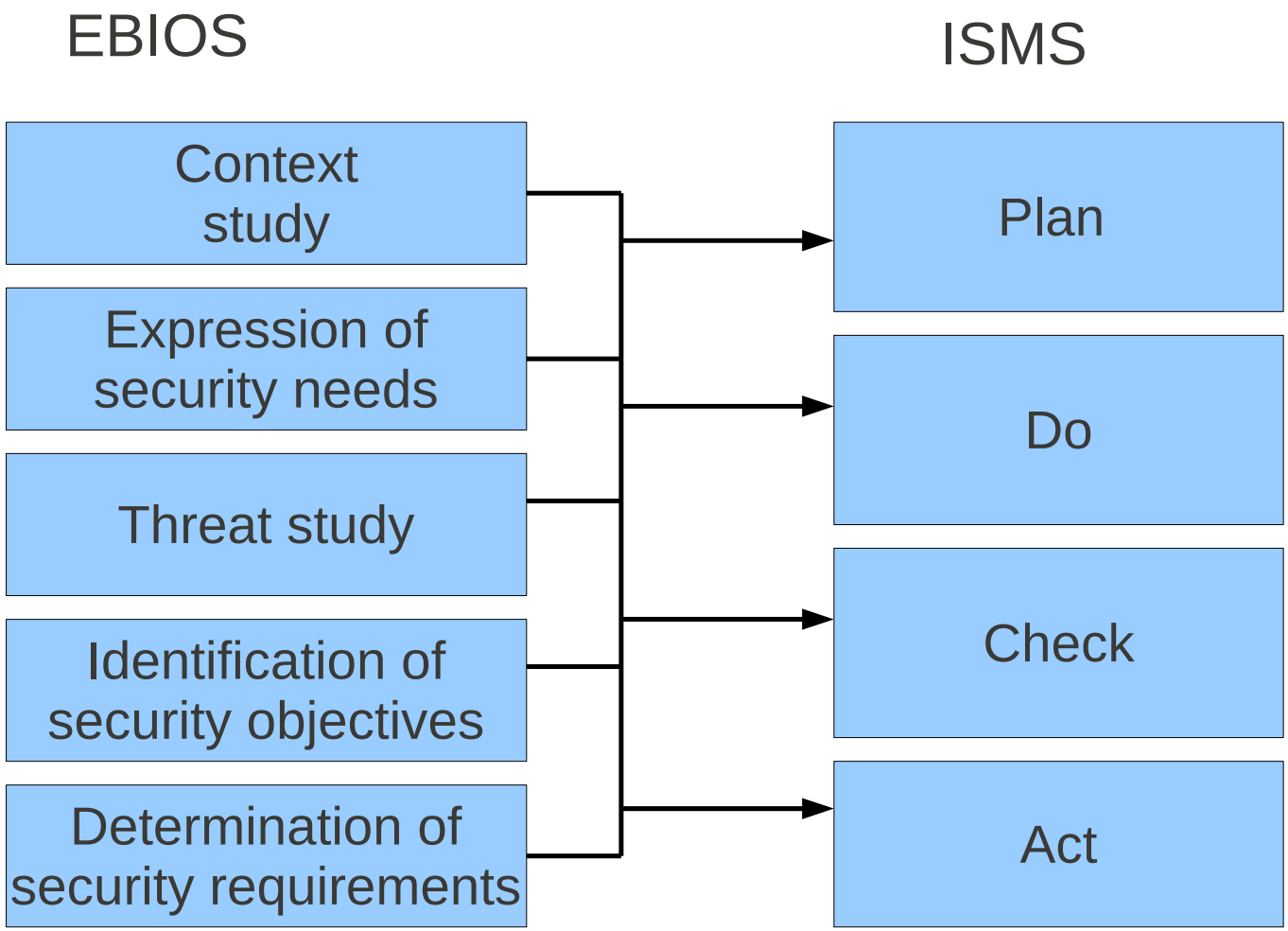

FIGURE: Application of Ebios for a ISO 27000 ISMS

Plan

First step : Context study

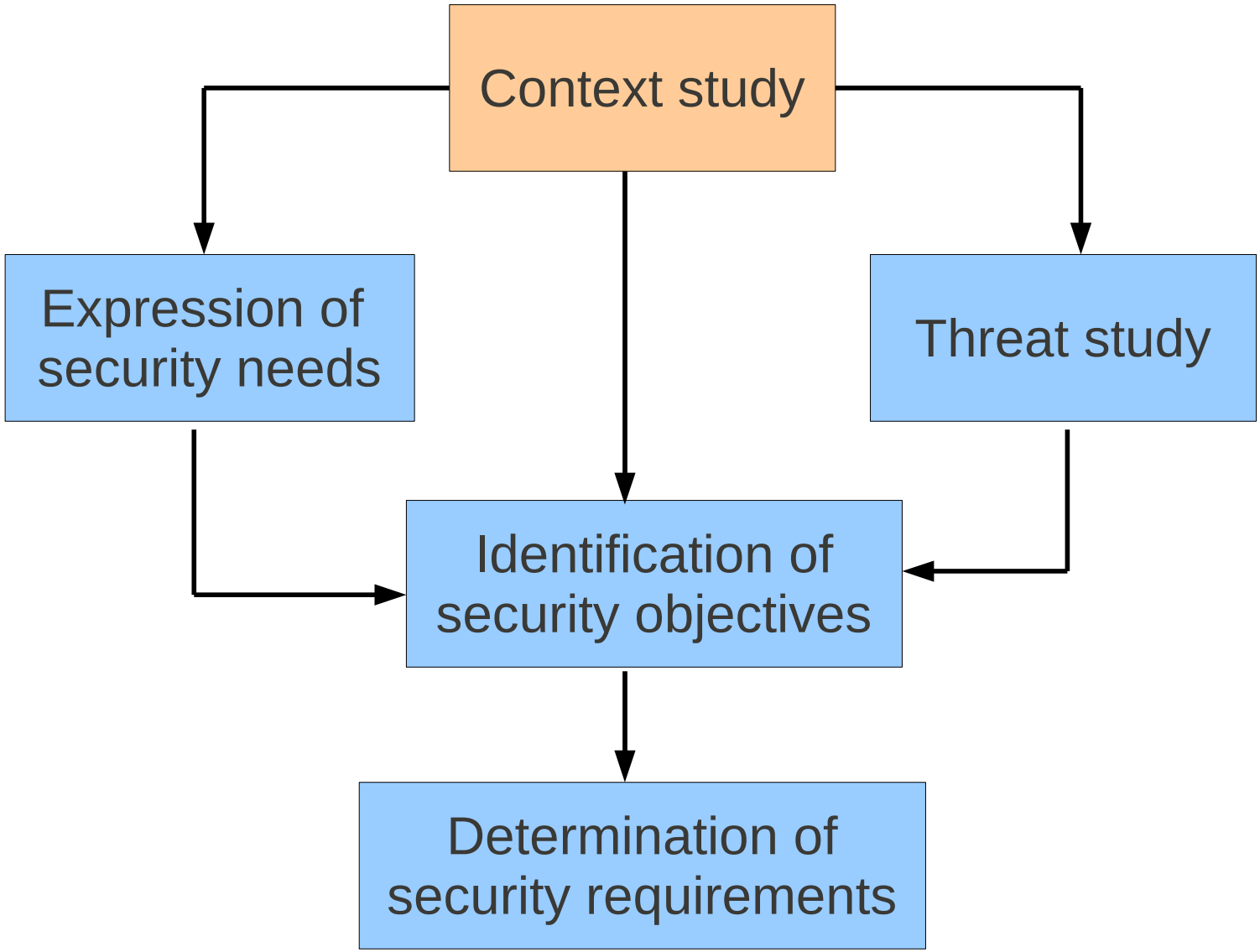

FIGURE: Context study

Context study : activities

Presentation of the organisation, identification of the target system in global terms, with positionment in its environment.

Specification of the issue at stake (*enjeux*) for the target system, with context, missions and services.

Collection of all the information required for planning the study (assets, assumptions, constraints,...).

This step is divided into three activities :

- Activity 1.1 : Study of the organisation.
- Activity 1.2 : Study of the target system.
- Activity 1.3 : Determination of the security study target.

Context study : approach

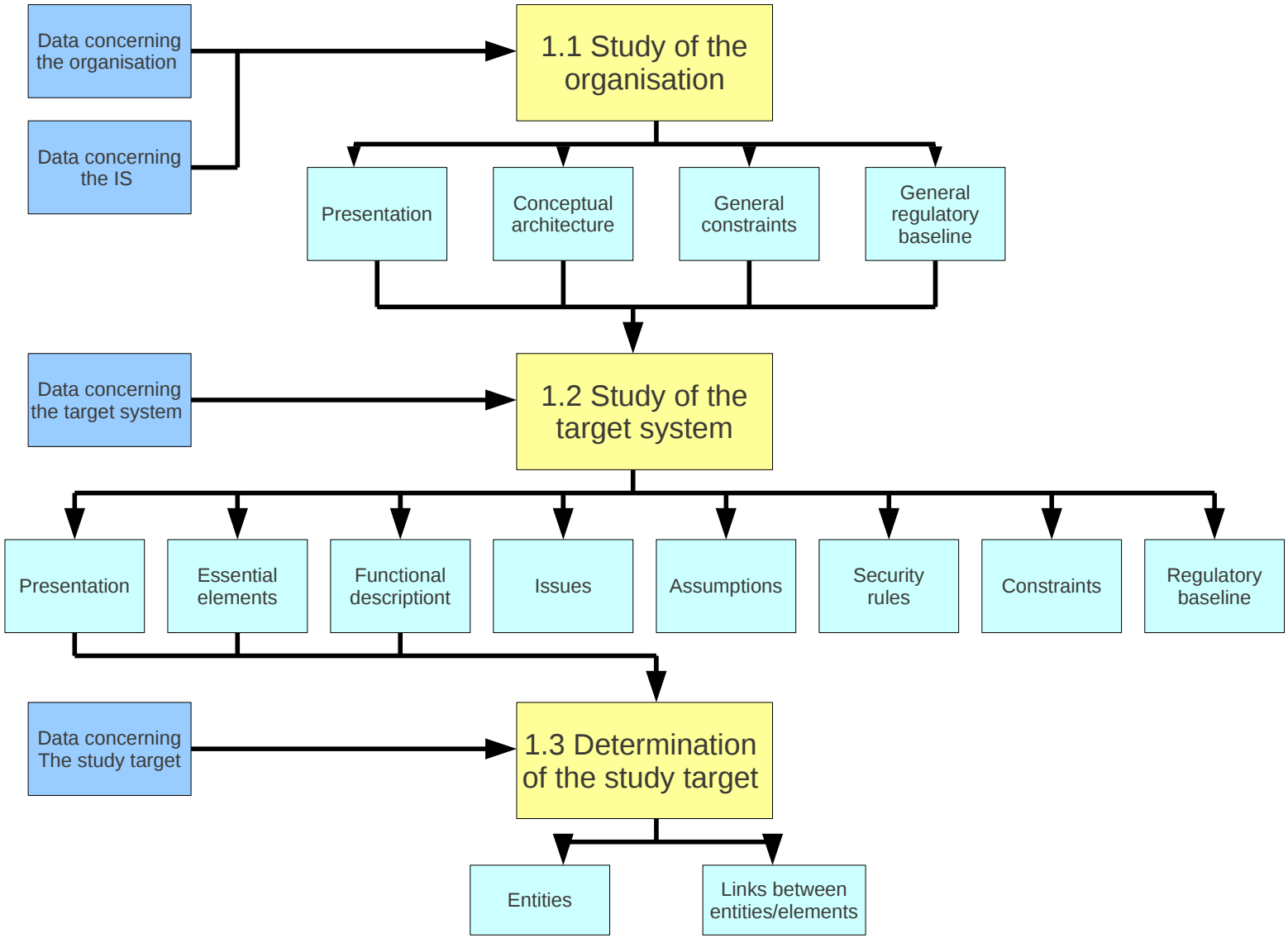

FIGURE: Context study

Activity 1.1 : Study of the organisation

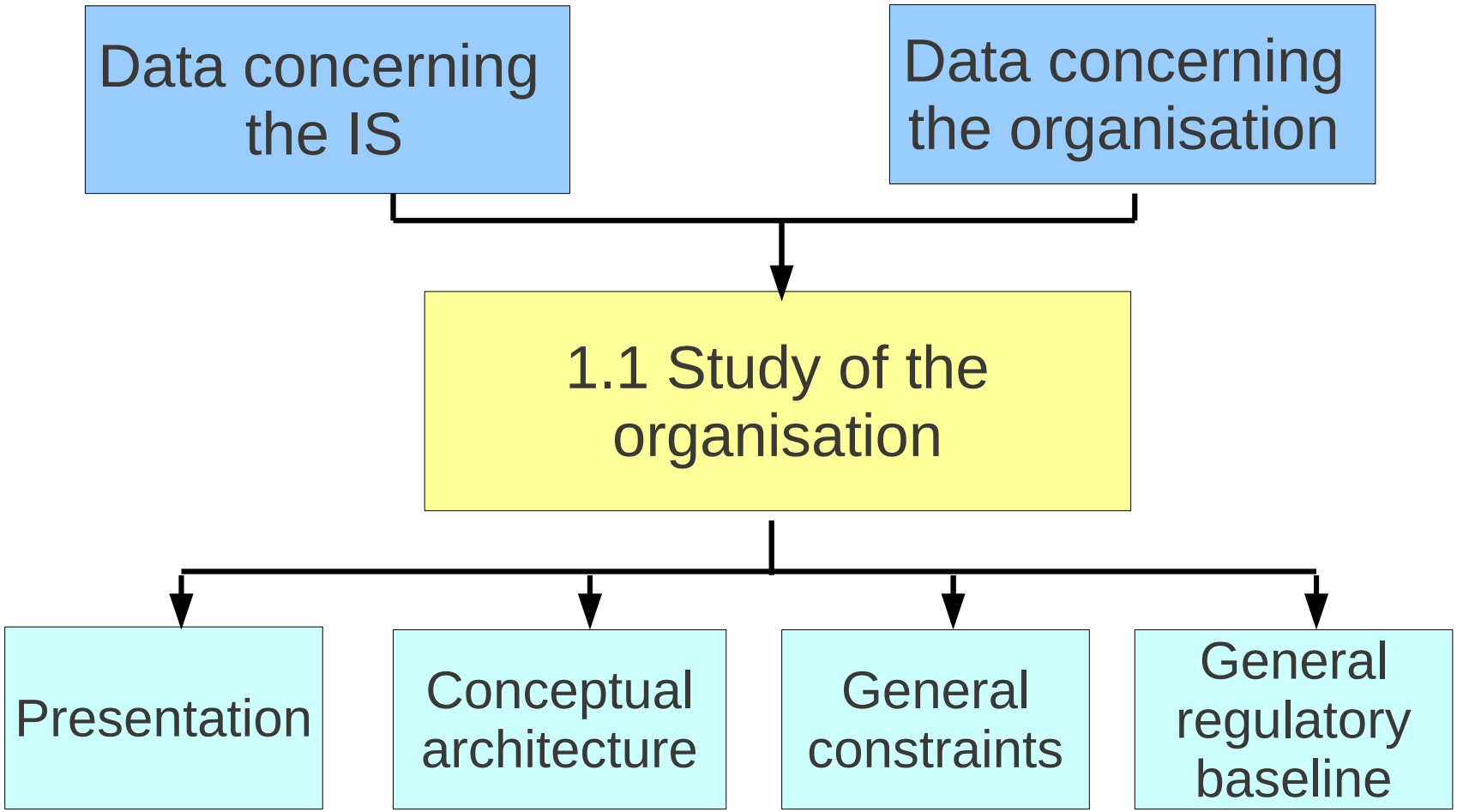

FIGURE: Organisation study

Activity 1.1 : Study of the organisation (1/2)

Collection of general information about organisation in a **presentation** : the organisation's main purpose, its business and its missions, the structure of the organisation and the security management.

List of **general constraints** affecting the organisation :

Constraint	Thematic	Description
C.constraint1	...	...
C.constraint2	...	...

Thematic of constraints :
personal, budgetary, technical or environmental,...

Activity 1.1 : Study of the organisation (2/2)

List of **general regulatory references** (*références réglementaires*) applicable to the organisation, with exact title :

Security rules	Title	Description
P.rule1	...	...
P.rule2	...	...

Examples :
Compliance with international standards, national laws as *Loi n˚78-17 du 6 janvier 1978 - Informatique et libertés*,...

Functional description of the global information system with a decomposition into functional domains (**conceptual architecture**).

Activity 1.2 : Study of the target system

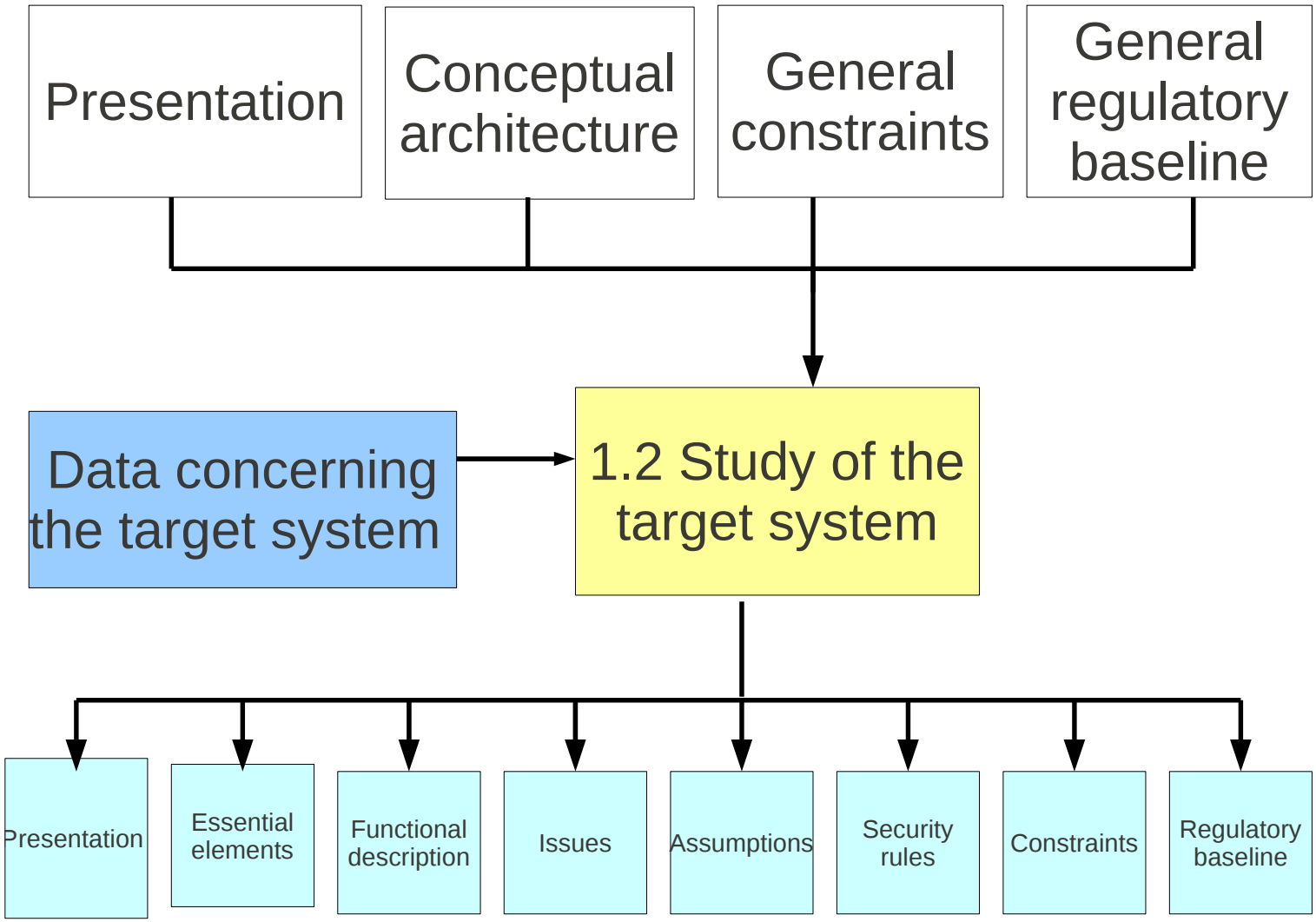

FIGURE: Target system study

Activity 1.2 : Study of the target system (1/4)

Specification of the context of use of the future or existing system, in a **presentation** of the target system.

Identification of the strategic weight of the target system for the organisation.

List the **issues** at stake of the target system (typically of technical, financial or strategic nature).

Production of a **functional description** of the target system. For each essential functions identified, a precise description of input, output and process is required.

Activity 1.2 : Study of the target system (2/4)

List and description of **essential elements** of the target system : functions or information for which availability, integrity, confidentiality or other security criteria must be garanteed.

Information	I.information1
Description	...
Information	I.information2
Description	...

Function	F.function1
Description	...
Input	I.information1
Output	I.information2

Activity 1.2 : Study of the target system (3/4)

List of **assumptions** specific to the target system :

Assumption	Description
H.assumption1	...
H.assumption2	...

Example : trust and formation of the administrator.

List of **securiy rules** specific to the target system :

Security rules	Description
P.rule1	...
P.rule2	...

Examples : activation of alarm during the night, password based access control.

Activity 1.2 : Study of the target system (4/4)

List of **constraints** specific to the target system :

Constraint	Thematic	Description
C.constraint1	...	...
C.constraint2	...	...

Thematic of constraints : technical, environmental, time, financial.

List and description of **regulatory** references specific to the target system.

Examples : national laws, international standards, rules.

Activity 1.3 : Determination of the study target

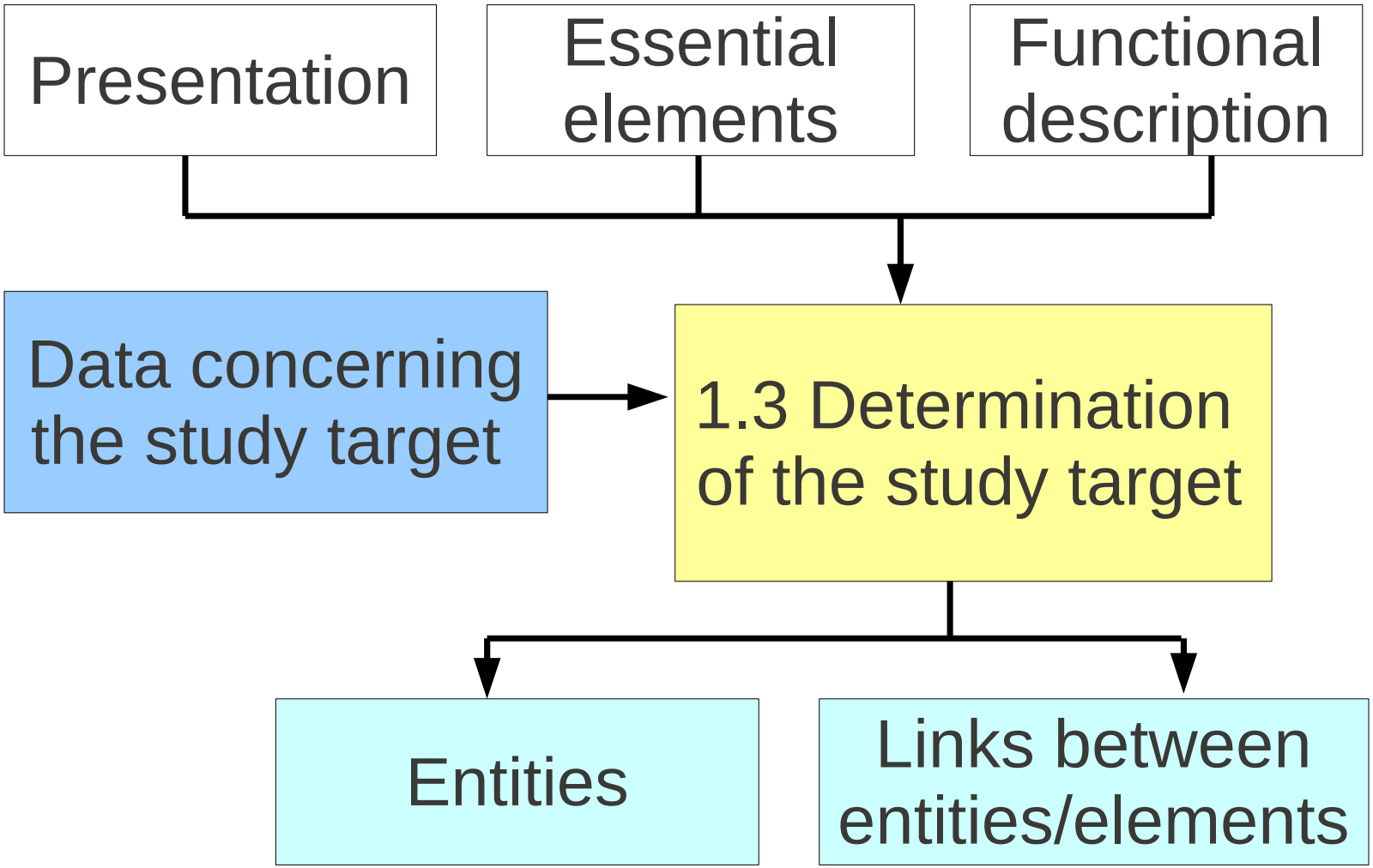

FIGURE: Determination of the study target

Activity 1.3 : Determination of the study target

List and description of **entities** of the target system (use entity types described in *Tools for assessing ISS risks*).

Entity	Type	Description
E.entity1	...	...
E.entity2	...	...

Examples : users, administrators, computers, server, application, windows OS, open office, intranet.

Establish the **link between essential elements and entities**, with an entity / elements tables.

	I.information1	I.information2	F.function1
E.entity1	x	x	x
E.entity2		x	

Entity types (*Tools for assessing ISS risks*)

MAT : Hardware (*matériel*).

LOG : Software (*logiciel*).

RES : Network (*réseaux*).

PER : Personnel (*personnel*).

PHY : Site (*site*).

ORG : Organisation (*organisation*).

SYS : System (*système*).

Example of type of entity : Hardware (MAT)

All physical elements of the information system. There are two sub-types :

MAT_ACT : Data processing equipment (active) (*support de traitement de données (actif)*).

1. Transportable equipment (laptop computer).
2. Fixed equipment (server, computer).
3. Processing peripheral (printer).

MAT_PAS : Data medium (passive) (*support de données (passif)*).

1. Electronique medium (floppy disc, CD ROM, removable hard disc).
2. Other media (paper, documentation).

Example of type of entity : Personnel (PER)

All the groups of persons involved in the information system.
There are 4 sub-types :

PER_DEC : decision maker (*décisionnel*).

PER_UTI : users (*utilisateurs*).

PER_EXP : operators/maintenance (*exploitant/maintenance*).
These are the personnel in charge of operating and maintaining the information system.

PER_DEV : developer (*développeur*).
Developers are in charge of developing the organisation's applications.

Example of type of entity : Site (PHY)

All the places containing the system, or part of the system, and the physical means required for it to operate. There are two sub-types :

PHY_LIE : Places (*lieu*).

1. External environment (*environement externe*).
2. Premises (*locaux*).
3. Zone (*zone*).

PHY_SRV : Essential service (*service essentiel*).

1. Communication (*communication*).
2. Power (*énergie*).
3. Cooling/pollution (*refroidissement/pollution*).

Plan

Expression of security needs

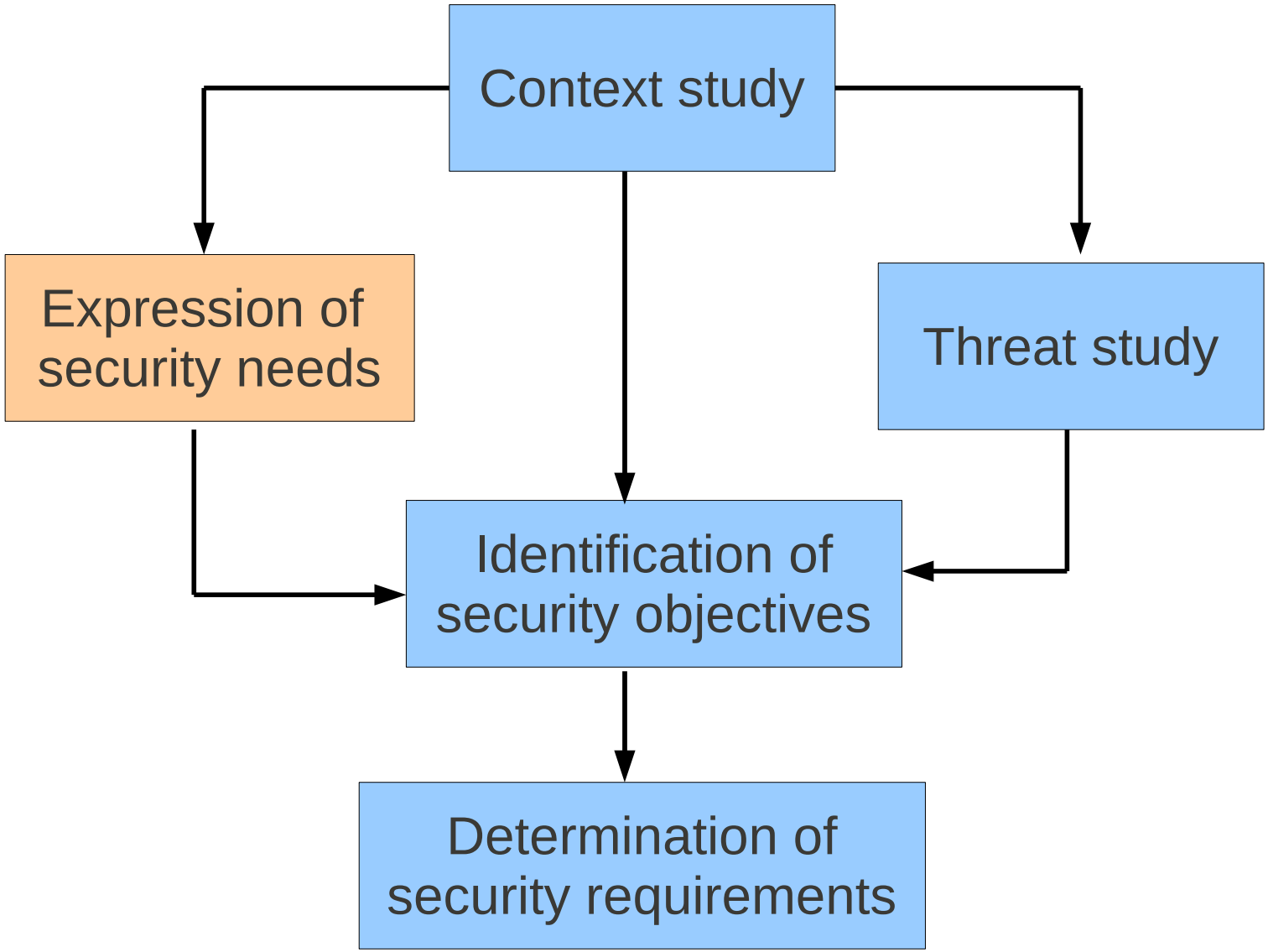

FIGURE: EBIOS global approach : security needs

Expression of security needs : activities

Contribution to risk estimation and definition of risk criteria.

Result from operational requirements of the system, independently of any technical solution.

Based on the preparation and use of a scale of needs and the detection of impacts that are unacceptable for the organisation.

Divided in two activities :

1. Activity 2.1 : Creation of needs sheets (*fiches de besoin*).
2. Activity 2.2 : Summary of security needs.

Expression of security needs : approach

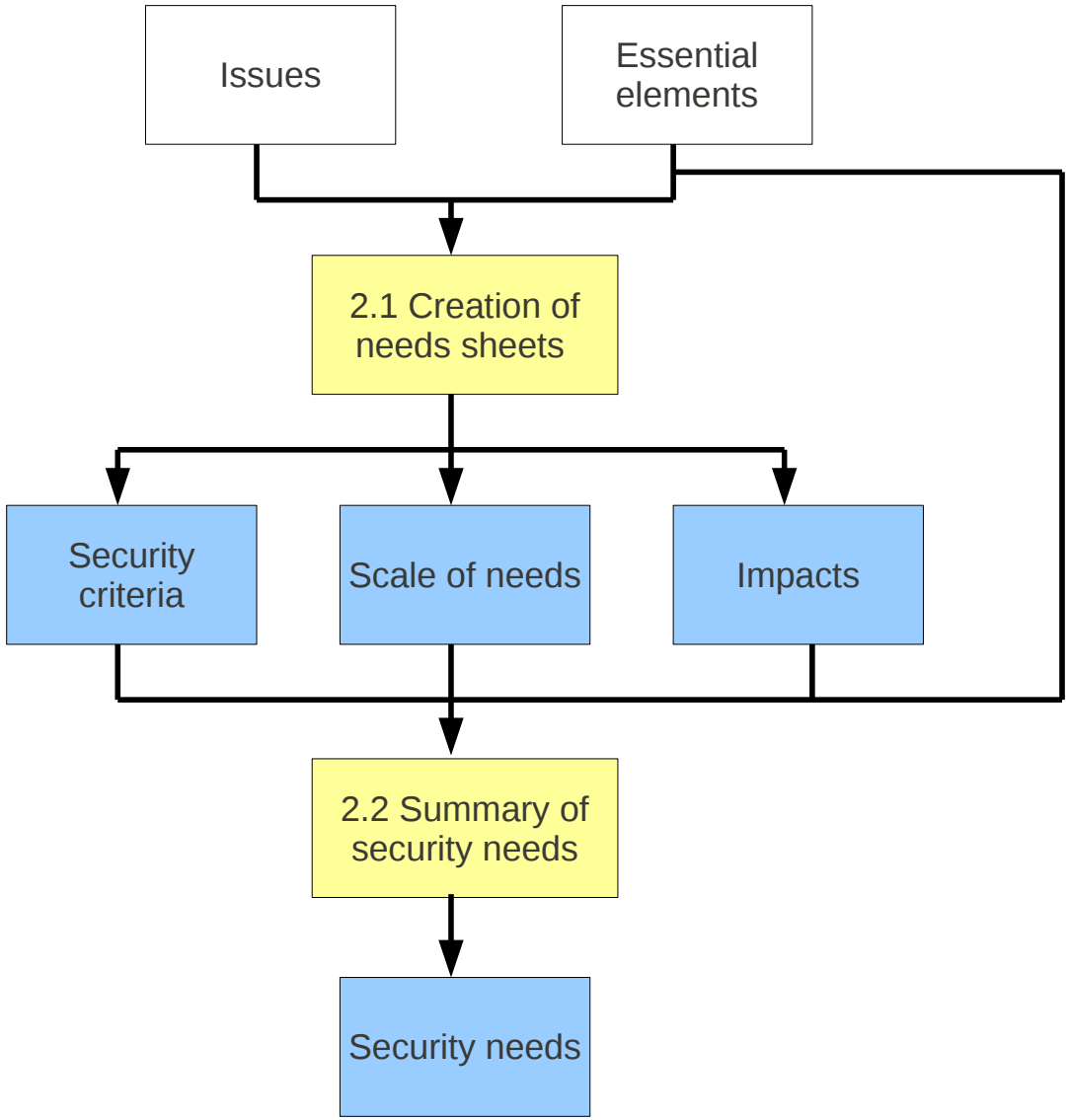

FIGURE: Expression of security needs

Activity 2.1 : Creation of needs sheets

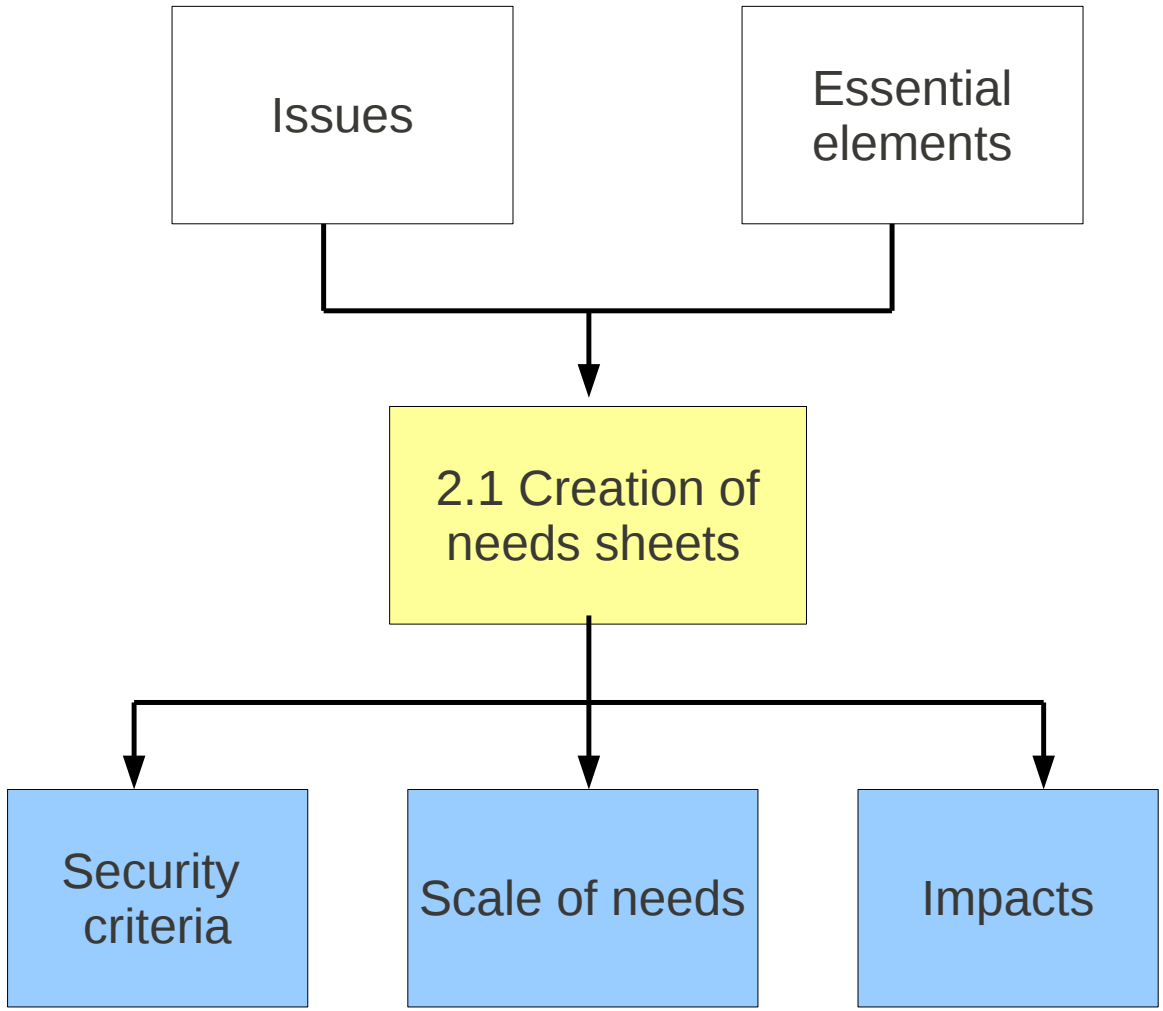

FIGURE: Creation needs sheets

Activity 2.1 : Creation of needs sheets (1/3)

List of the **security criteria** to be taken into account :

1. Availability
2. Integrity
3. Confidentiality

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.

Activity 2.1 : Creation of needs sheets (2/3)

Creation of the table required for the expression of security needs for essential elements, called **scale of needs** :

	Confidentiality	Availability	Integrity
0	Public	No availability need	No integrity need
1	Restricted	Long term	
2	Confidential (partners)	Medium term	Medium integrity need
3	Confidential (internal)	Short term	
4	Secret	Very short term	Total integrity

Activity 2.1 : Creation of needs sheets (3/3)

Creation of a list of relevant **impacts**. Use the non-exhaustive list provided in Ebios guide (techniques, section 3), with explicit examples on the target system :

- Interruption of service
- Loss of customer confidence
- Disruption of internal operation
- Attack on user's privacy private life
- Financial losses
- Judicial proceedings and penalties
- Material damage

For each essential element, a security sheet is realized with impacts in relation to security criteria.

Activity 2.2 : Summary of security needs

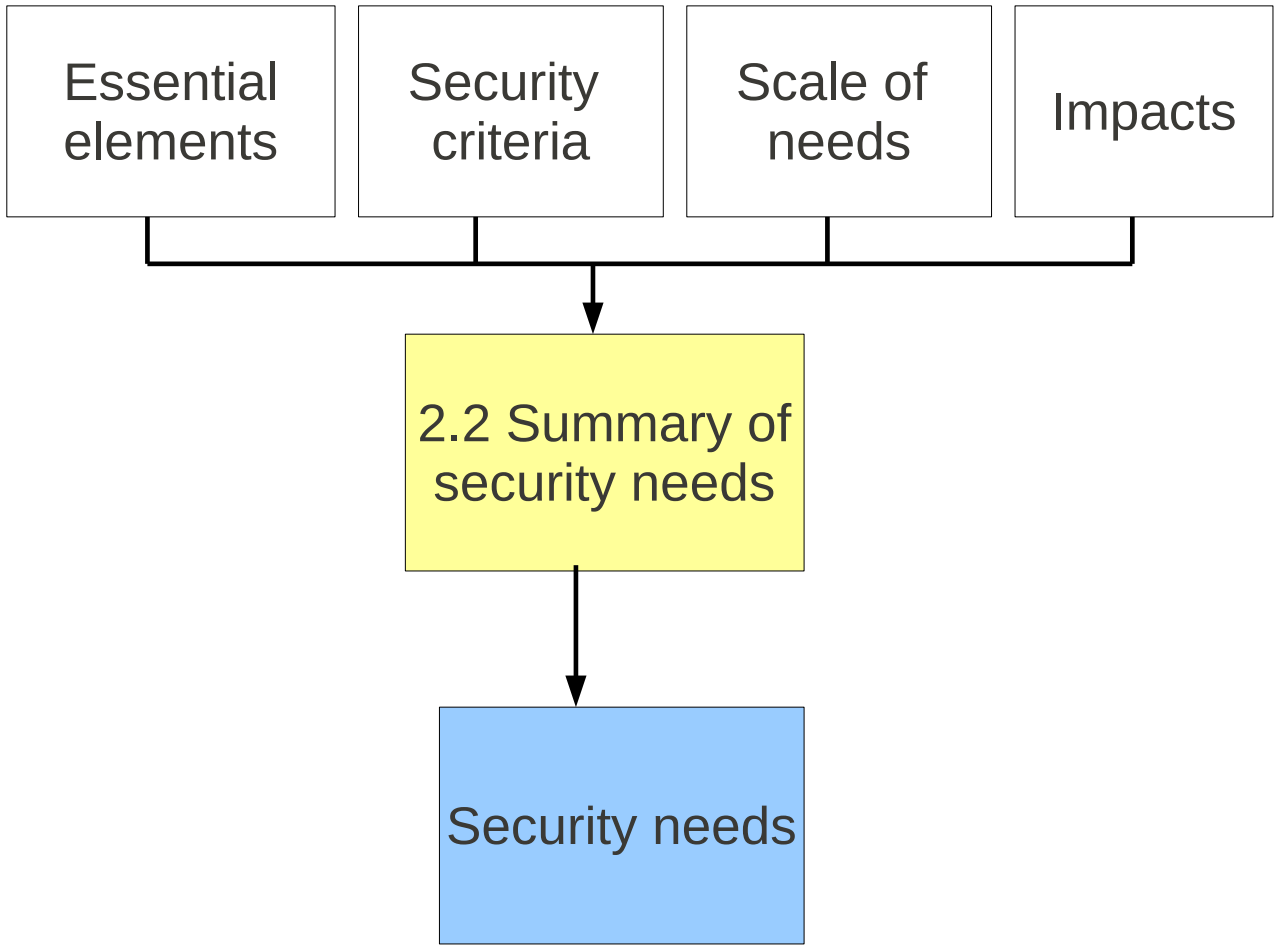

FIGURE: Summary (*synthèse*) of Security Needs

Activity 2.2 : Summary of security needs (1/2)

For each essential element, a security need is associated for each security criteria, in relation to security sheets :

Name of the essential element	impact1	...	impact n	security needs
availability	B11	...	B1n	f(B11,..,B1n)
integrity	B21	...	B2n	f(B21,..,B2n)
confidentiality	B31	...	B3n	f(B31,..,B3n)
...	...	...	...	...

Impact criteria Bij are related to the scale of needs and impacts described in the security sheets.
for example, the function f is the max function.

Activity 2.2 : Summary of security needs (2/2)

Realisation of a **security needs** summary sheet of the system target (*fiche de synthèse des besoins de sécurité*) :

Essential elements	Confidentiality	Integrity	Availability
Function 1	0	3	3
...	...	...	...
Function n	0	4	2
Information 1	2	1	1
...	...	...	...
Information m	2	1	2

Classification and prioritise the essential elements, depending to the level of security needs.

Plan

Threat study

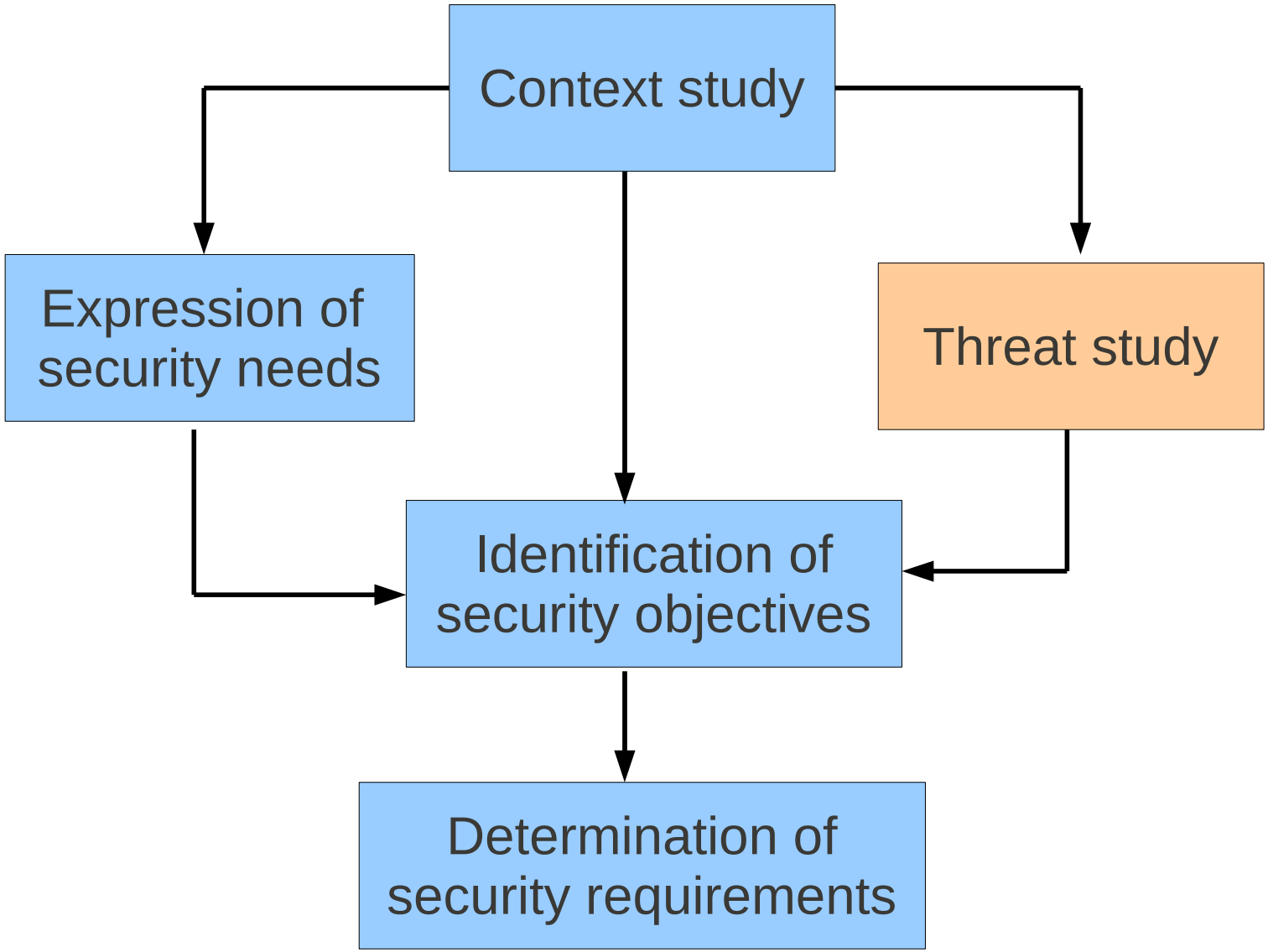

FIGURE: Threat study

Threat study : activities

Contribution to risk assessement by determining the threats affecting the system (threat agents and vulnerabilities).

The threats are formalised by identifying their components :

- The attack methods to which the organisation is exposed.
- The threat agents that may use these methods.
- The vulnerabilities exploitable on the system entities and their level (opportunity).

The threat study includes three activities :

- Activity 3.1 : Study of threat sources.
- Activity 3.2 : Study of vulnerabilities.
- Activity 3.3 : Formalisation of threats.

Threat study : approach

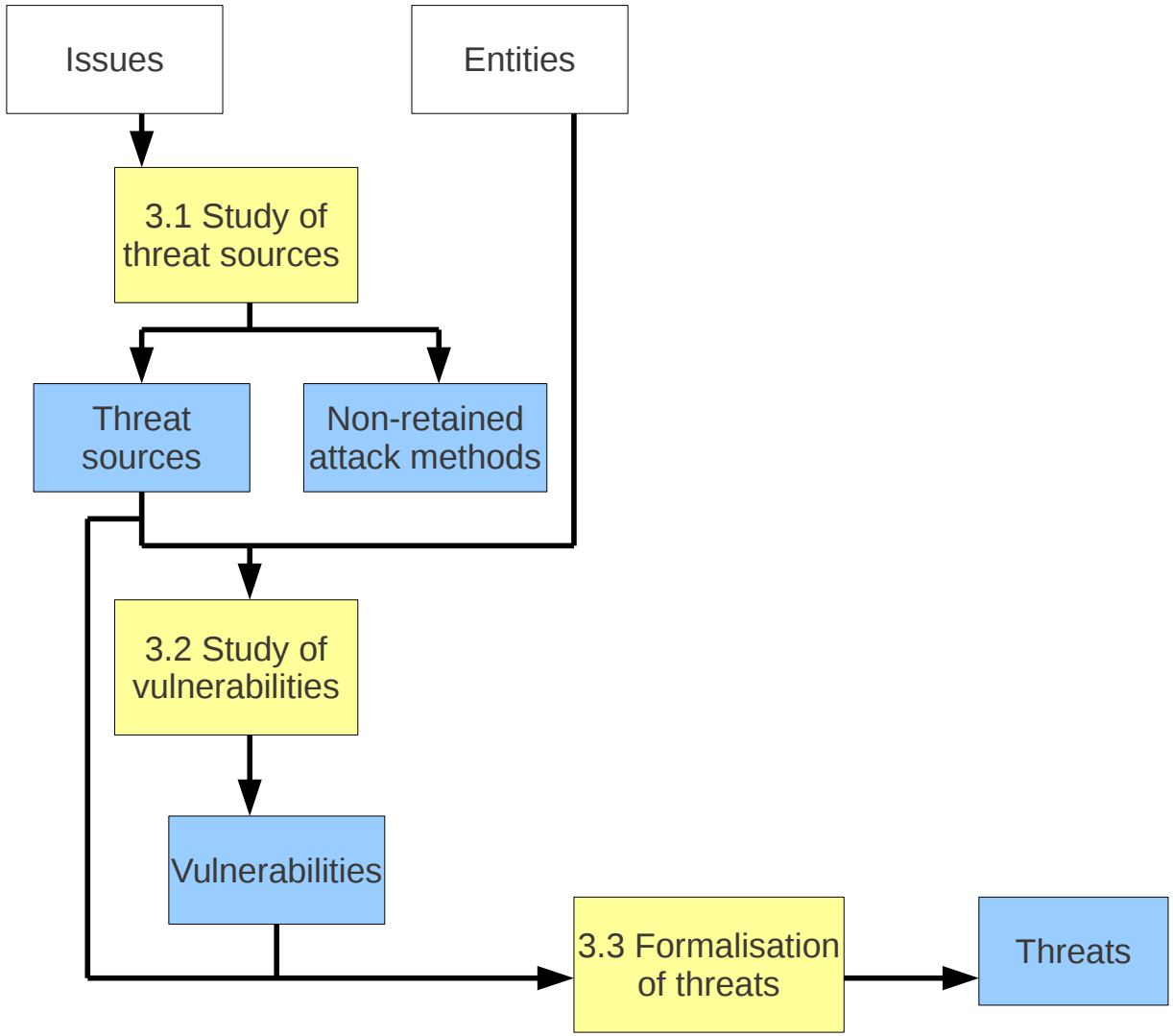

FIGURE: Threat Study

Activity 3.1 : Study of threat sources

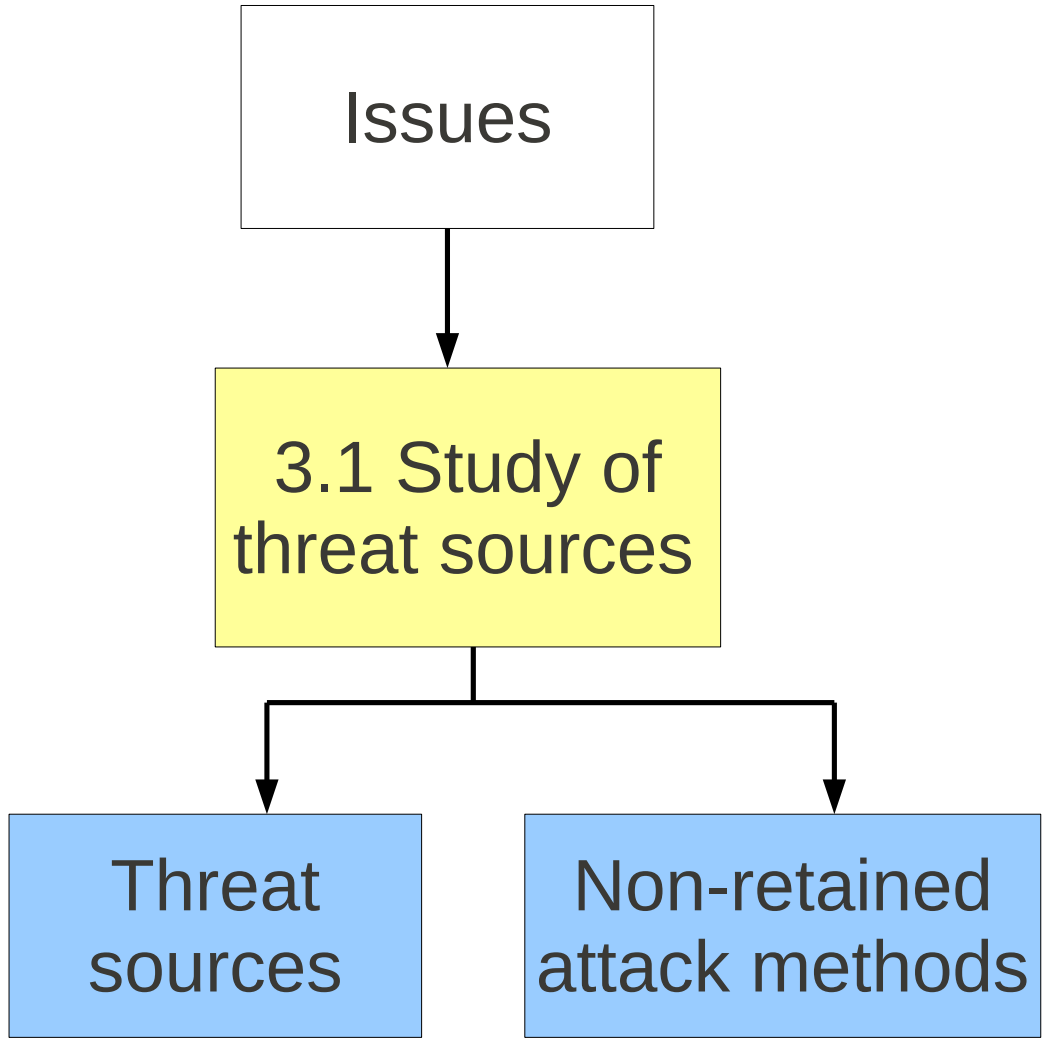

FIGURE: Study of threat sources

Activity 3.1 : Study of threat sources (1/3)

List and description of the relevant attacks methods (42 methods proposed in *Tools for assessing ISS risks*).

Threat agents are characterized with their type (natural, human or environmental) and their cause (accidental or deliberate).

N	Attack	Description
1	fire	...
21	theft of equipment	...
30	saturation of the IS	..
...	...	...

Highlight the **threat sources** and the **non-retained attack methods**, with justifications.

Activity 3.1 : Study of threat sources (2/3)

Characterization of attack methods according to the security criteria they may affect, with *Tools for assessing ISS risks*.

Examples :
Fire affects primarily the availability and integrity criteria.
Theft of document affects the confidentiality criteria.
Saturation of the IS affects the availability criteria.

A value represents the attack potential of the threat agent :

1. 1 : accidental or random
2. 2 : limited opportunities
3. 3 : high level of expertise, opportunity and resources.

Activity 3.1 : Study of threat sources (3/3)

N = natural, H = Human, E = environmental, A = accidental, D = deliberate, A = availability, I = integrity and C = confidentiality.

Attacks methods	Type			Cause		Attack potential	Security criteria		
	N	H	E	A	D		A	I	C
Fire	x	x	x	x	x	2	x	x	
Loss of means of telecommunication			x	x	x	1	x		
Eavesdropping		x	x		x	2			x
Theft of documents			x		x	2			x
Theft of equipment			x		x	1	x		x
Divulgation		x	x	x	x	1			x
...	...	...	...	...	...	...	...	...	...

Themes of threats and attack methods

1. Physical damage (*Sinistres physiques*)
2. Natural events (*Évènements naturels*)
3. Loss of essential services (*Perte de services essentiels*)
4. Disturbance due to radiation (*Perturbations dues aux rayonnements*)
5. Compromise of information (*Compromission des informations*)
6. Technical failures (*Défaillances techniques*)
7. Unauthorized actions (*Actions illicites*)
8. Compromise of functions (*Compromission des fonctions*)

Example of threats : natural events

- Climatic phenomenon
- Seismic phenomenon
- Volcanic phenomenon
- Meteorological phenomenon
- Flood

Attack methods	Type			Cause		Criteria		
	N	H	E	A	D	A	C	I
Climatic phenomenon	x			x		x		x
Seismic phenomenon	x			x		x		x
Volcanic phenomenon	x			x		x		x
Meteorological phenomenon	x			x		x		x
Flood	x			x		x		x

Example of threats : unauthorized actions

1. Unauthorized use of equipment
2. Fraudulent copying of software
3. Use of counterfeit or copied software
4. Corruption of data

Attack methods	Type			Cause		Criteria		
	N	H	E	A	D	A	C	I
Unauthorized use of eq.		x			x	x	x	x
Fraudulent copying..		x			x		x	
Use of counterfeit ...		x	x	x	x	x		
Corruption of data		x			x		x	x
Illegal processing of data		x			x		x	

Example of threat : Fire (01)

(Theme 1 : Physical damage)

- Type : Natural / Human / Environmental.
- Accidental cause : concentration of flammable or explosive materials in a confined environment,..
- Examples : lightning, short circuit, ...
- Deliberate cause : terrorists or vandals...
- Examples : ...
- Type of consequence : Destruction of assets,danger to personal safety, financial loss, disturbance of internal operation.
- Security criteria : integrity, availability.

Example of threat : Theft of equipment (21)

(Theme 5 : Compromise of information)

- Type : Human.
- Deliberate cause : someone inside or outside the organization accessing equipment.
- Examples : theft of a laptop computer.
- Type of consequence : loss of information and/or functions, disclosure of the information stored in the equipment, financial loss.
- Security criteria : confidentiality, availability.

Activity 3.2 : Study of vulnerabilities

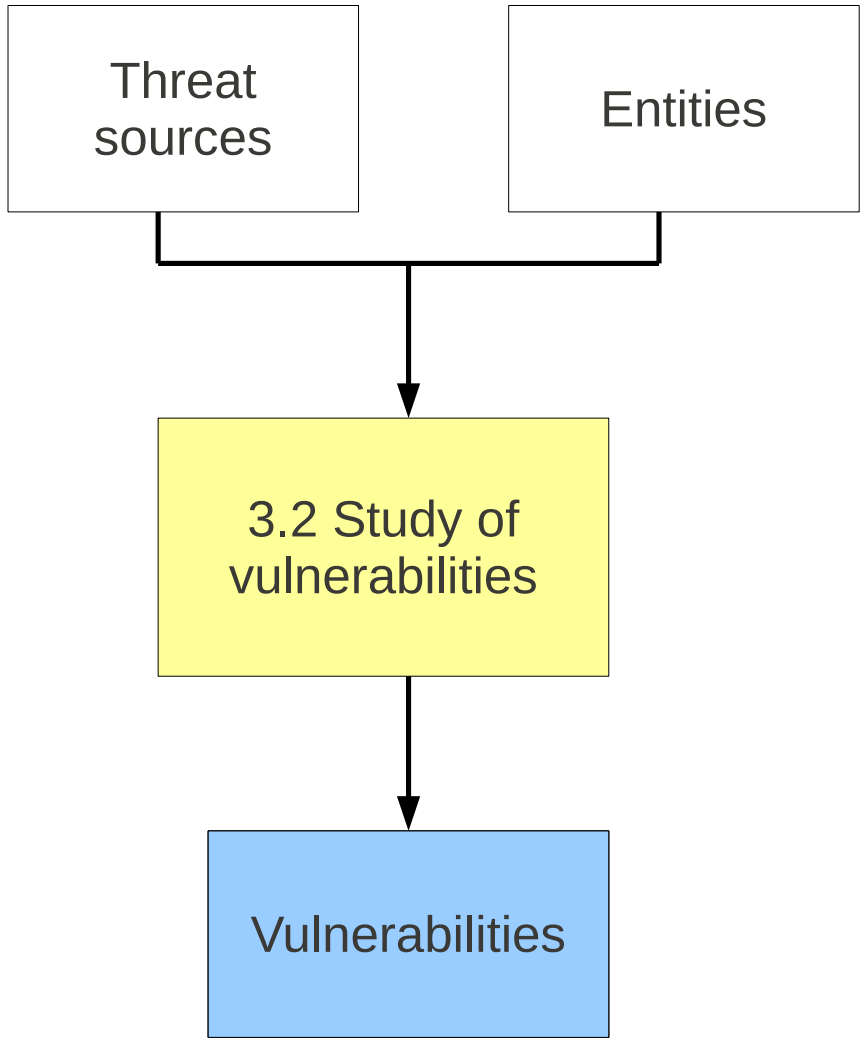

FIGURE: Study of vulnerabilities

Activity 3.2 : Study of vulnerabilities (1/2)

Determine the specific **vulnerabilities** of the target system, according to attack methods (Use generic vulnerabilities described in *Tools for assessing ISS risks*).

A vulnerability is a characteristic of the system that could be exploited by a threat agent.

Characterisation of these vulnerabilities in terms of level :

0	Totally improbable or unfeasible
1	Low probability or needing very considerable means
2	Medium probability or needing some degree of expertise
3	High probability or possible using standard means
4	Certain or possible for anyone

Activity 3.2 : Study of vulnerabilities (2/2)

Provides the list of estimated vulnerabilities associated with the selected attack methods for each type or sub-type of entity.

Possibility of several entity for each vulnerabilities :

Attack methods	Vulnerabilities	Hardware	Software	...	Org.
Attack1	vulnerability1		2	...	2
	vulnerability2	1	1	...	3
	...	...	...	...	...
Attack2	vulnerability3	1		...	1
	...	...	...	...	...

130 pages of vulnerabilities in section 4 of the english version ! (*Tools for assessing ISS risks*).

Example of vulnerabilities for Fire

No substitution equipment (entity : MAT_ACT).

Equipment using flammable materials (entity : MAT_ACT).

No insurance cover for serious damage (entity : ORG).

Single internally-developped appications (entity : LOG).

Unfamiliarity with security measures (entity : PER).

...

Example of vulnerabilities for Theft of equipment

No substitution equipment (entity : MAT_ACT).

No equipment inventory (entity : AMT_ACT).

No organisation for management and treatment of security incident linked to theft (entity ORG_GEN).

Low awareness of the need to protect equipment outside the organisation (entity : PER).

Use of equipment outside the organisation (entity PHY_LIE).

...

Activity 3.3 : Formalisation of threats

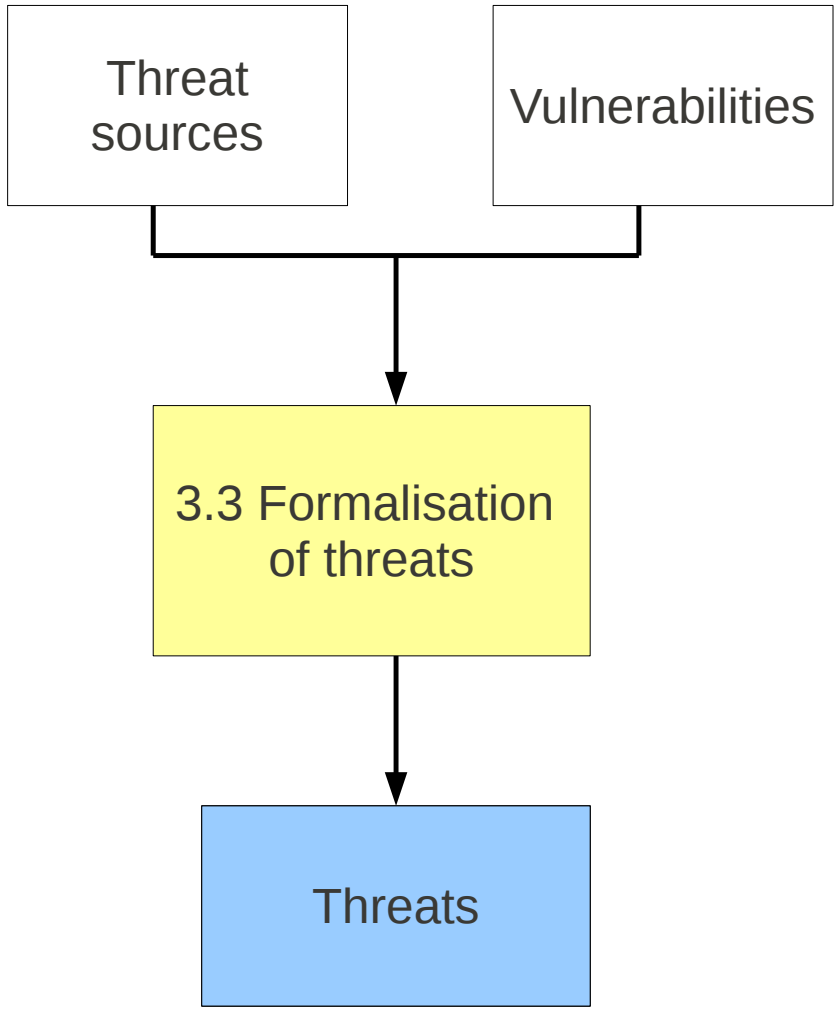

FIGURE: Formalisation of threats

Activity 3.3 : Formalisation of threats

Formulate the **threats** explicitly on the target system.

If the threat involves the exploitation of a single vulnerability, the threat opportunity is equal to the level of the vulnerability.

If a threat involves the exploitation of several vulnerabilities, the threat opportunity has to be determined according to the respective levels of the vulnerabilities (max,...).

Threats	Description	Attack potential	Sec. criteria			Opportunity
			A	I	C	
Attack 1	...	1	x	x		4
...						
Attack n	...	3	x		x	1

Prioritise the threats according to their opportunity.

Plan

Identification of security objectives

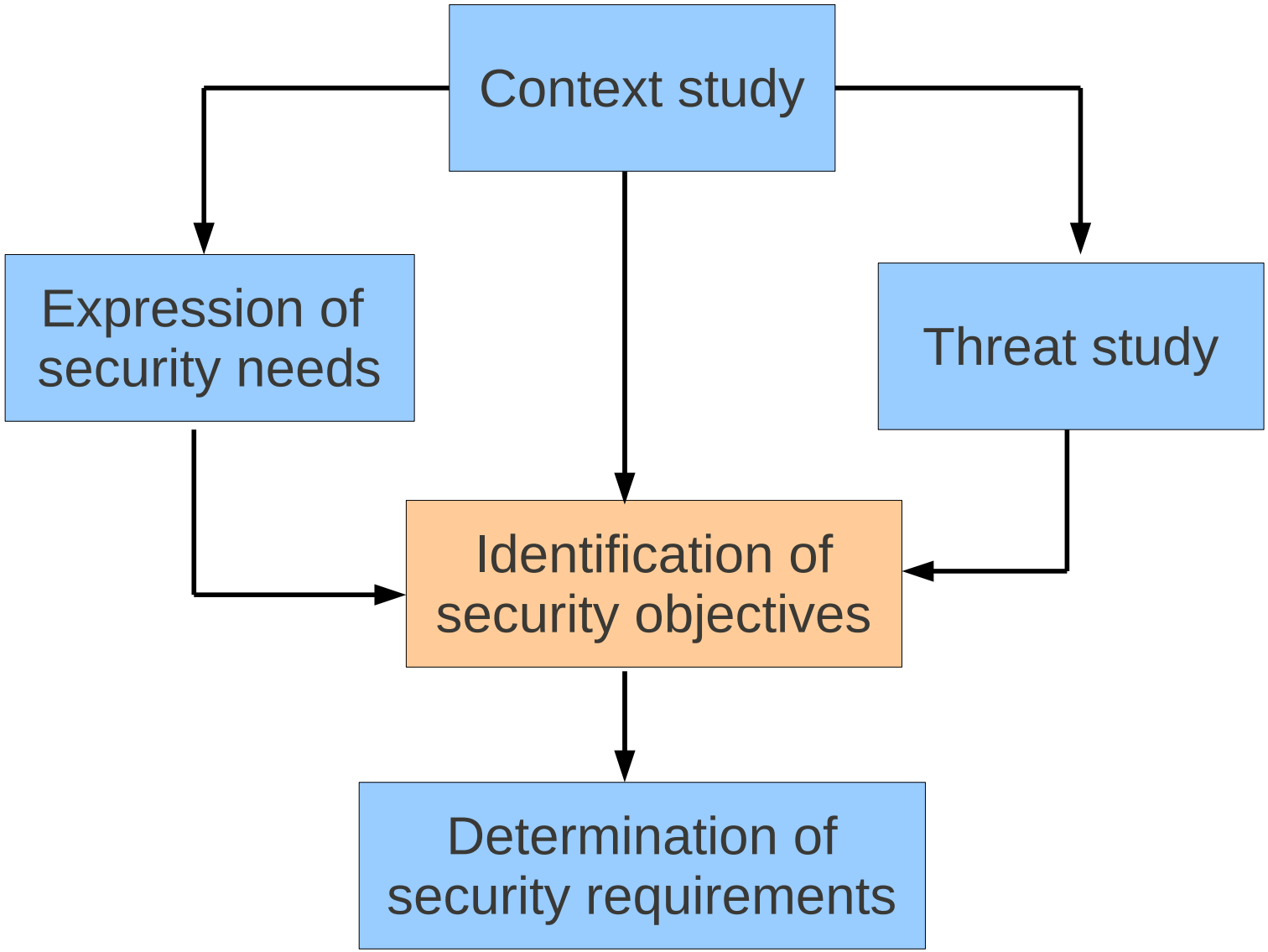

FIGURE: Identification of security objectives

Identification of security objectives : activities

Evaluation and treatment of the risks affecting the system.

Comparaison of threats with security needs and determination of the risks to be covered by the security objectives

The level of security objectives and the assurance level must be determined during this step.

The step includes three activities :

- Activity 4.1 : Comparison of the threats with the needs.
- Activity 4.2 : Formalisation of security objectives.
- Activity 4.3 : Determination of security levels.

Identification of security objectives : approach

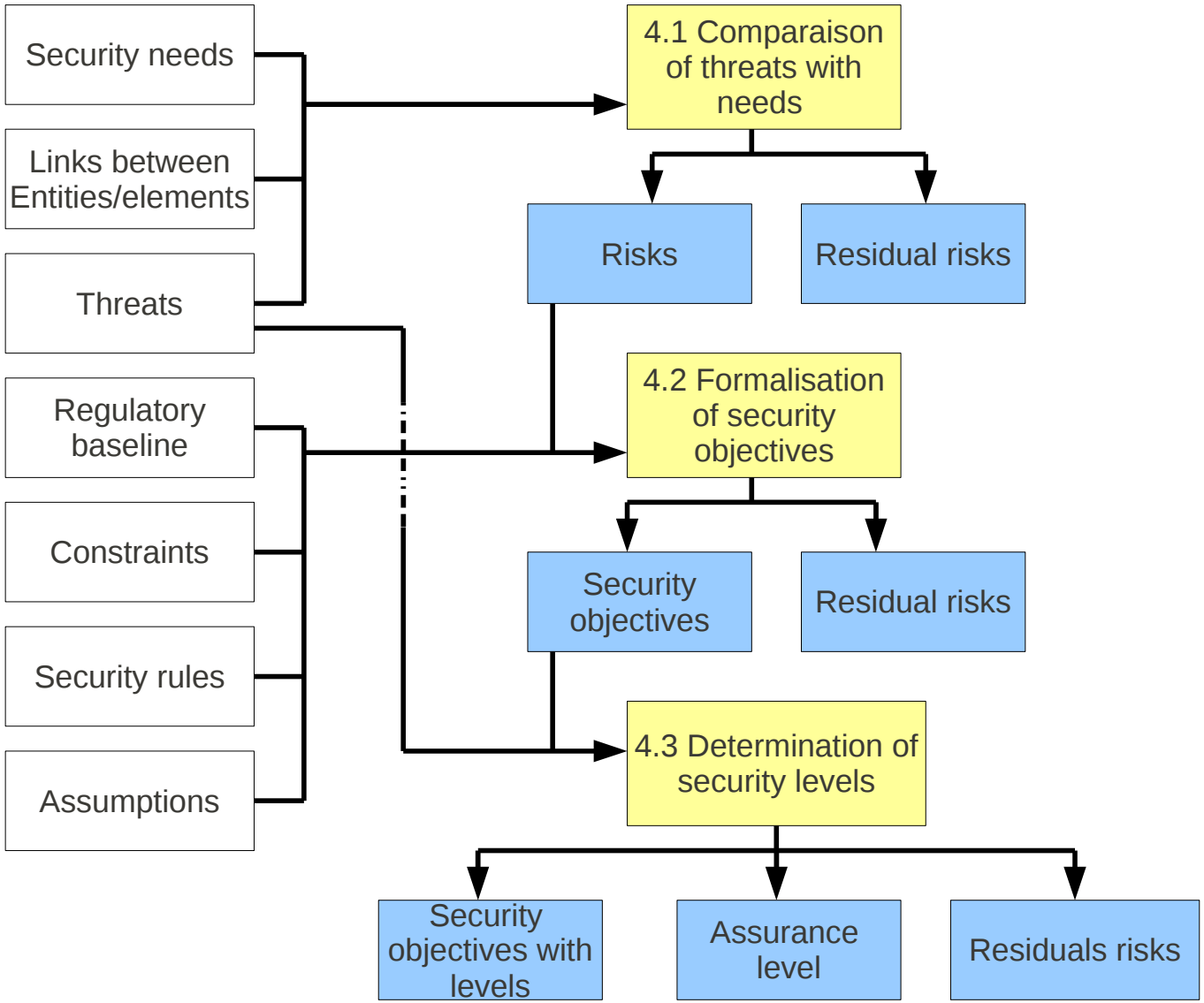

FIGURE: Identification of security objectives

Activity 4.1 : Comparison of threats with needs

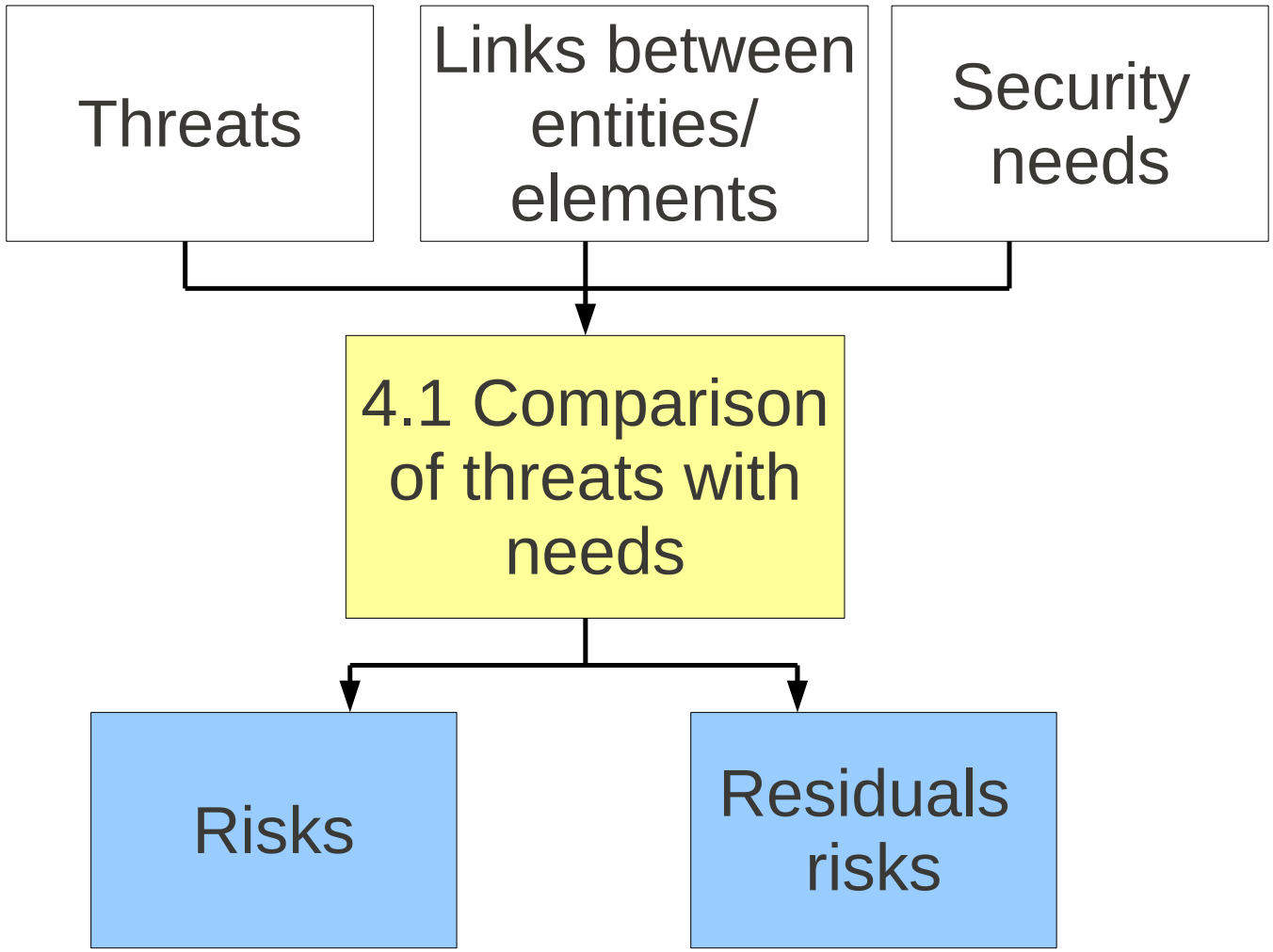

FIGURE: Comparison of threats with needs

Activity 4.1 : Comparison of threats with needs

Contribution to risk estimation in the risk management process.

Determine reals **risks** affecting the target system by comparing threats with security needs.

Risks must be explicitly described in relation to the target system. Description uses the previous risk summary table, the formulation of threats, the scale of needs and the description of concerned essential elements.

Prioritise the risks according to the essential elements and the threat opportunity (justify **residual risks**).

Risk summary table

Example : security needs for element1 are availability : 1, integrity : 1, confidentiality : 2.

Attacks methods	Security			element 1			...	element m		
				A	I	C		A	I	C
	A	I	C	1	1	2		2	0	1
Fire	x	x		1	1			2		
Loss of means of telecommunication	x			1				2		
Eavesdropping		x			1					
Theft of documents			x			2				1
Theft of equipment	x		x	1		2		2		1
Divulgation			x			2				1

Formulate risks explicitly

Explicit formulation of risk on the target system.

Risks depends of the following parameters :

1. Max = maximum of security needs (impacts).
2. Op = threat opportunity (level of vulnerabilities, section 3).
3. Pot = Attack potential (of the threat agent, section 3).

Risks		Max	Op	Pot
R.Theft	Theft of equipment, with confidentiality on element1,... and availability on element m.	2	3	2
...	...	...	...	...

This formulation is used for prioritize risks (and residual risks).

Activity 4.2 : Formalisation of security objectives

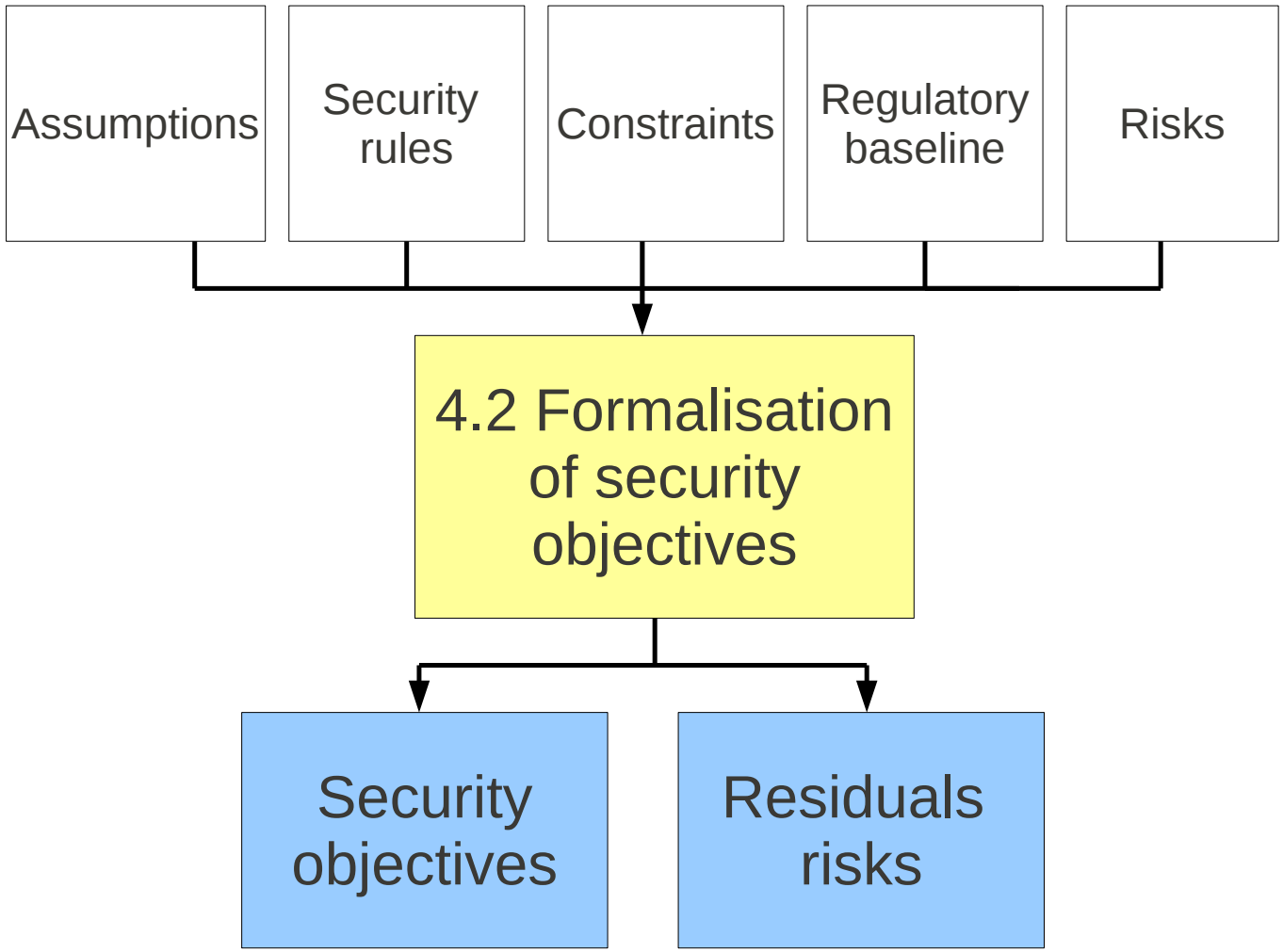

FIGURE: Formalisation of security objectives

Activity 4.2 : Formalisation of security objectives

Contribution to risk treatment.

Determine, list and describe the **security objectives** to cover the risks (and other requirements as constraints,...).

Use Generic security objectives of *Tools for treating ISS risks* (classified by entity types).

Where appropriate, classify the security objectives into two categories : on the target system or on the environment.

Example of security objectives : Hardware

MAT_01
A stock of emergency equipment must be available in the event of equipment failure.

MAT_02
It must be possible to restore all or part of a system, application, data set and track in the event of damage, failure or negligence.

MAT_06
There must be a description of all IT equipment and its position.

...

MAT_15
Reliability must be taken into account when choosing equipment, software and media.

Example of security objectives : Organisation

ORG_01
The organisation must protect the equipment and media against physical access by unauthorised persons.

ORG_02
The entrance and exit procedures must be designed to combat theft of equipment.

ORG_06
The anti-virus policy must prevent any malicious code from entering and spreading in the systems.

...

ORG_45
The organisation must ensure that work conditions are satisfactory.

Coverage of risks by security objectives

Justification of the risks coverage :

1. All risks, security rules, regulatory references, constraints, assumptions,... are (fully) covered by security objectives.
2. Each security objectives must be the response to at least one risk, one security rule, one assumption,...

Tools for treating ISS risks proposes a list of coverage of vulnerabilities by security objectives.

Level of coverage : possibly use of a coverage scale :

- 0 : no cover.
- 1 : partial cover.
- 2 : fully cover.

Sufficient coverage by security objectives

All risks, assumptions, constraints, regulatory references, issues must be covered by security objectives :

	Security objectives	Justification of coverage	Level of coverage
R.Fire	O.objective1 O.objective2 ...	...	1
A.assumption1	...	...	...
C.constraint1	...	...	...
R.reference1	...	...	...
...	...	...	...

The level of coverage hightlights the **residual risks** (in our case, the risk R.Fire is not completely covered).

Necessary coverage by security objectives

All security objectives must cover at least one risk, assumtion, issue, constraint or regulatory reference :

Security objectives	R.Fire	A.assumption1	C.constraint1	...
O.objective1	x			...
O.objective2	x			...
O.objective3		x		...
O.objective4			x	...
...	...	...	...	...

Examples of coverage

Vulnerabilities concerning the threat *Fire* and its corresponding coverage :

No substitution equipment covered by MAT_01.
Equipment using flammable materials covered by PHY_09.

Remark : vulnerability *Equipment using flammable materials* concerns the entity MAT, but is covered by a entity PHY.

Vulnerabilities concerning the threat *Theft of equipment* and its corresponding coverage :

No substitution equipment covered by MAT_01.
Low awareness of the need to protect equipment outside the organisation covered by PER_01.

Activity 4.3 : Determination of security levels

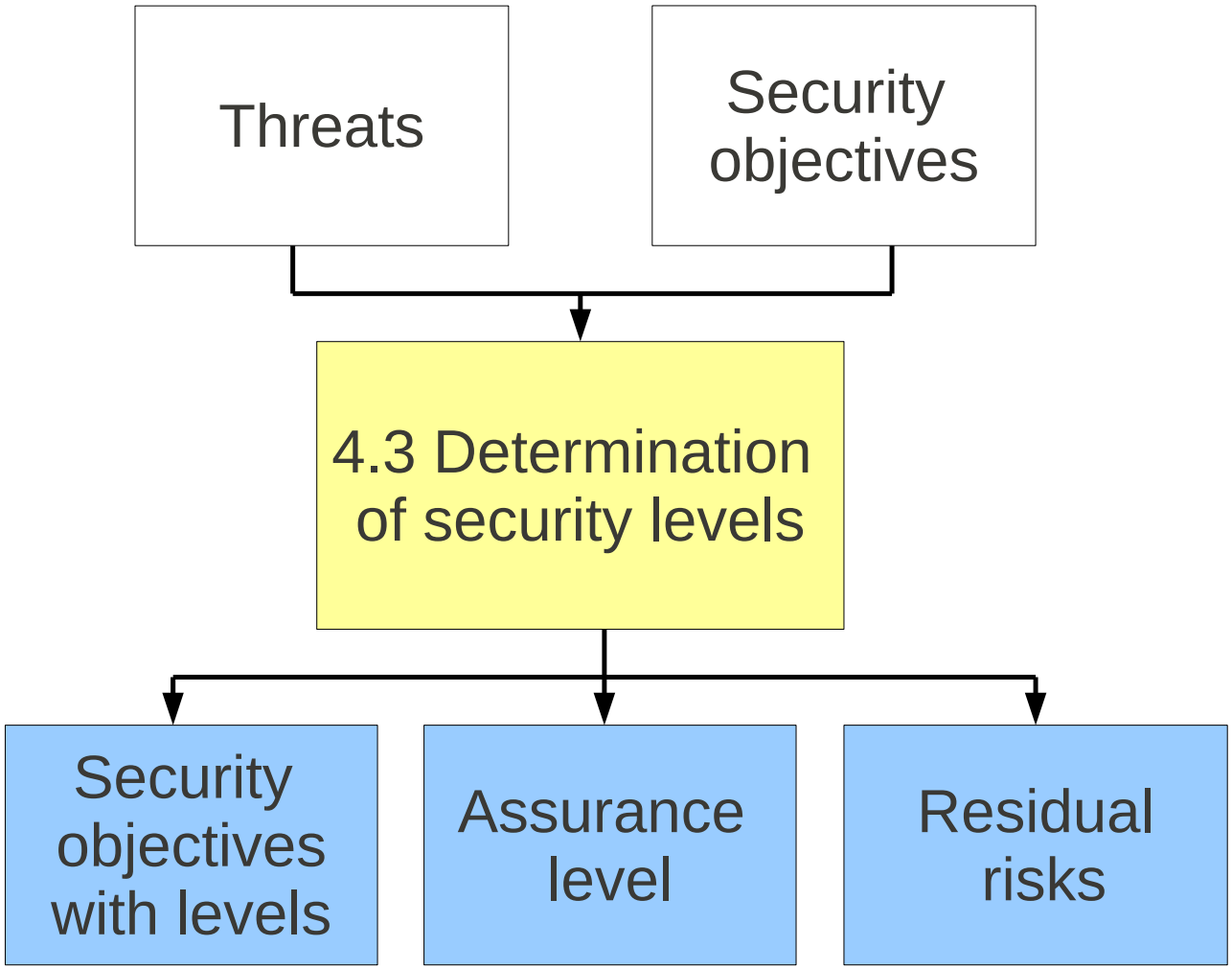

FIGURE: Determination of security levels

Activity 4.3 : Determination of security levels

Determination of the adequate **level of each security objectives** (use generally attack potential of the threat agents) and **residuals risks** (with justification).

Three security levels are considered :

1. Basic level for an adequate protection against a random violation of system security with a low attack potential.
2. Medium level for an adequate protection against easily-implemented or intentional violation of system security with a moderate attack potential.
3. High level for an adequate protection against deliberately planned or organised violation of system security with a high attack potential.

Level of security assurance requirements

Choose the **level of security assurance requirements**, among the 7 predefined levels, taken from the common criteria :

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

These levels are made up of increasingly rigorous components used to evaluate the implemented security.

There is no simple method for determining the assurance level, which remains primarily a financial or marketing choice.

An organisation does not necessarily have to use the EAL and can define its own assurance requirements.

Plan

Determination of security requirements

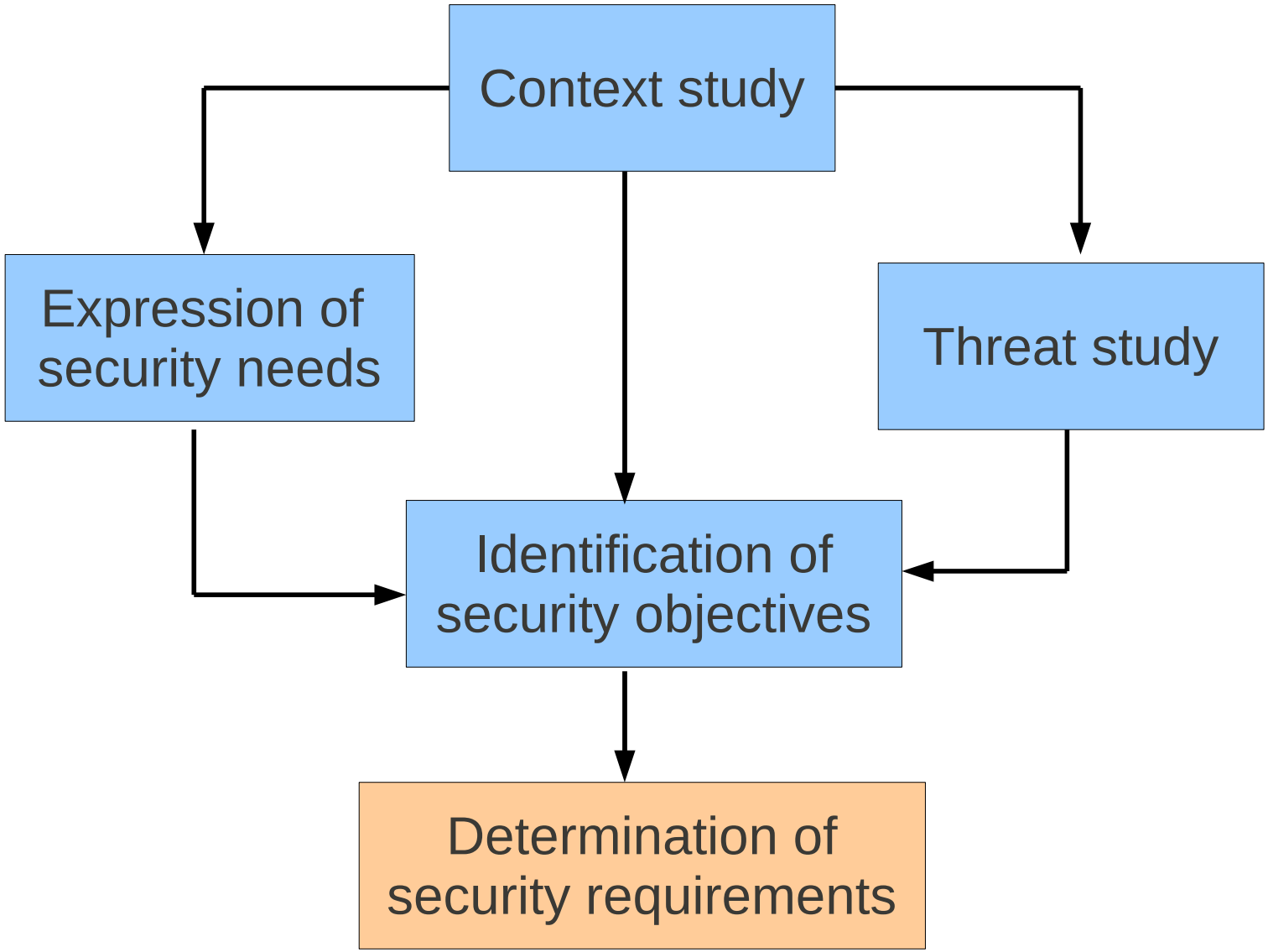

FIGURE: Determination of security requirements

Determination of security requirements : activities

Determine how to achieve the security objectives with the following requirements :

- The security functional requirements (SFR) describing the required security behaviour and designed to satisfy the security objectives.
- The security assurance requirements (SAR) forming the grounds for confidence that the product or system satisfies its security objectives.

This step includes two activities :

- Activity 5.1 : Determination of security functional requirements.
- Activity 5.2 : Determination of security assurance requirements.

Determination of security requirements : approach

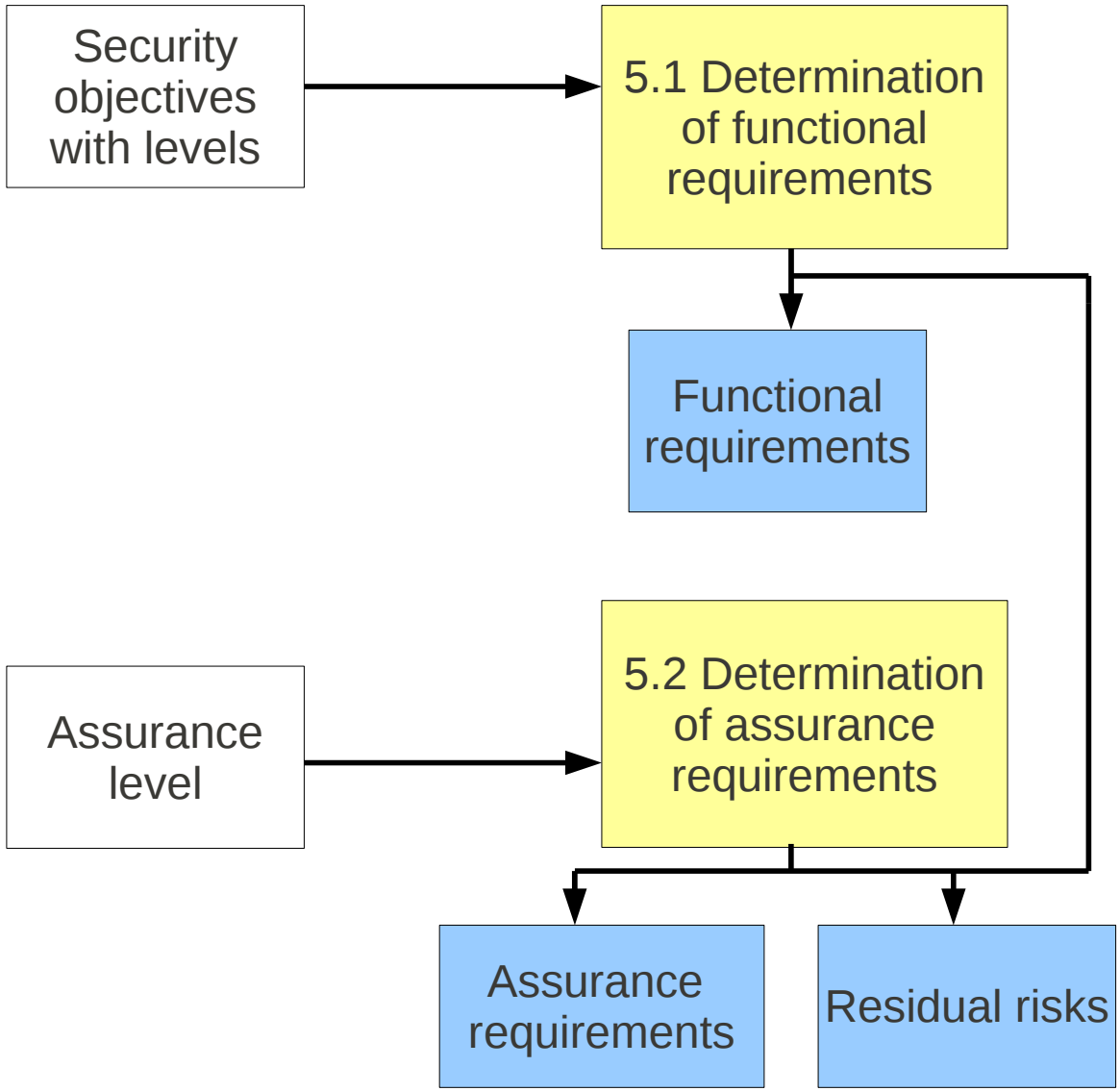

FIGURE: Determination of security requirements

Activity 5.1 : Security functional requirements

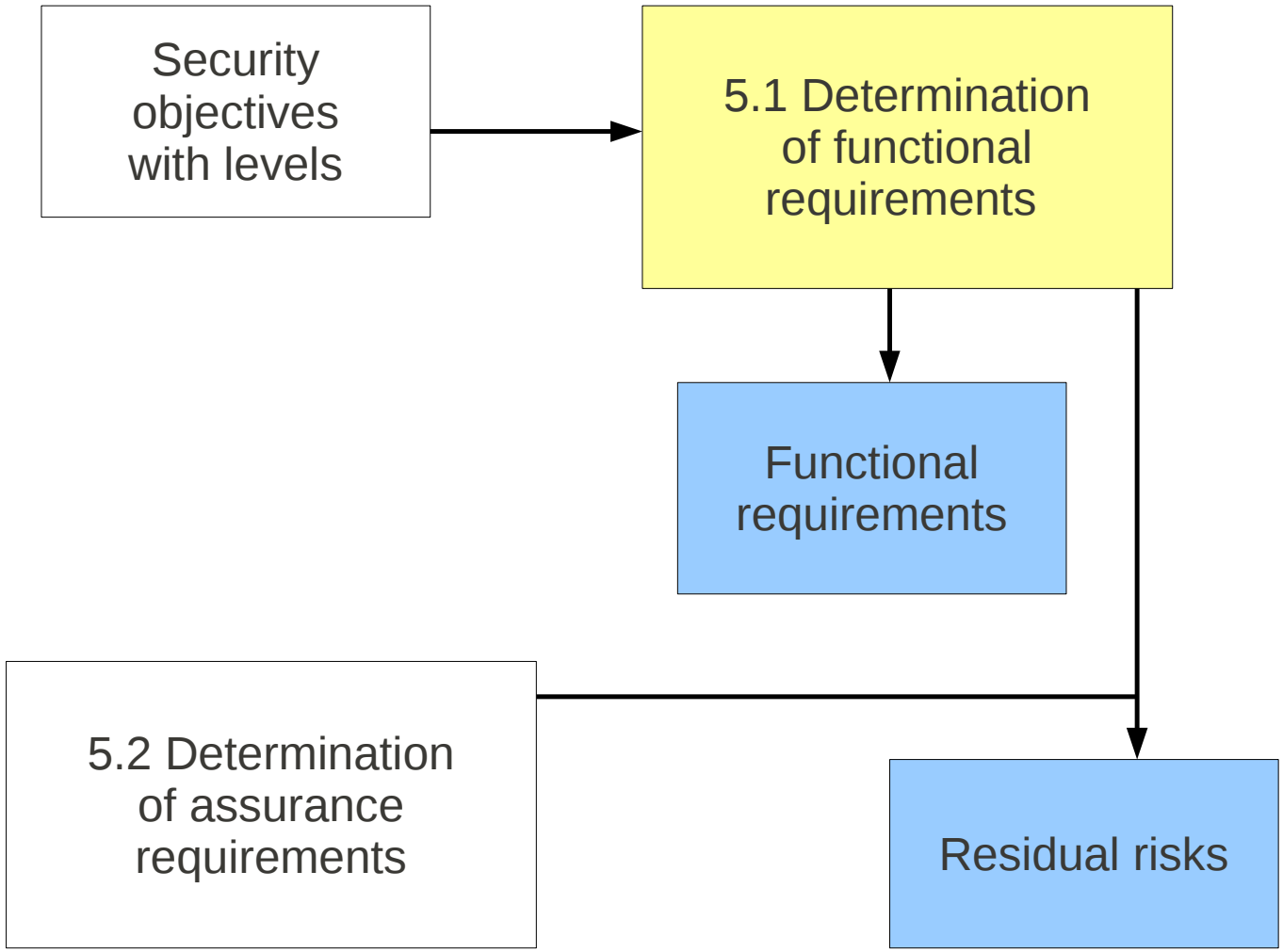

FIGURE: Determination of security functional requirements

Activity 5.1 : Security functional requirements

Contribution to risk treatment in the risk management process.

Provide a list of security **functional requirements**, used to decide how each identified risk must be treated.

Security functional requirements are described in the guide *Tools for treating ISS risks*, in section *Generic functional security requirements*.

Security functional requirements use common criteria, ISO 27002, PSSI requirements and other security requirements.

Additional security functional requirements can be created.

Security requirements taken from Common Criteria

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

Security requirements taken from ISO 27002

1. Security policy (BPS).
2. Organisational security (BOS).
3. Asset classification and control (BCM).
4. Personnel security (BSP).
5. Physical and environmental security (BPE).
6. Communications and operations management (BGC).
7. Access control (BMA).
8. Business continuity management (BCA).
9. Compliance (BCC).

Risk treatment with functional requirements

The risks may be rejected, reduced, transferred or accepted and the **residual risk** must be clearly identified :

1. Reduction of a risk is ensured by specific security functional requirements.
2. Rejection of a risk needs for the security functional requirements eliminating the exposure to the risk.
3. Transfer of a risk needs for the security functional requirements the use for example of an insurance.
4. Acceptation of a risk means that no security functional requirements are used.

Justification to the adequacy of coverage

Coverage of security objectives by security functional requirements is established with a coverage grid :

1. All security objectives are covered by security functional requirements (sufficient coverage).
2. All security functional requirements cover at least one objective (necessary coverage).

The level of coverage is used to highlight the residual risks, and use a scale of values :

1. 0 : no cover
2. 1 : partial coverage
3. 2 : complete coverage

Coverage grid of security objectives

Sufficient coverage :

Security objectives	Functional security requirements	Justification of coverage	level of coverage
O.objective1	EF.requirement1 EF.requirement2	...	2
...	...	...	...

Necessary coverage :

Security requirements	O.objective1	O.objective2	...
EF.requirement1	x		...
EF.requirement2	x	x	...
...	...	...	...

Example of coverage

Examples of coverage are described in the guide *Tools for ISS treating risks*. These examples concern hardware entity (MAT) :

Coverage of **MAT_01** (*a stock of emergency equipment must be available in the event of equipment failure*).

BGC_INT and BGC_PRE (*communication and operations management*), FRU_FLT (*resource utilisation*), CGS_GSS and CGS_SVG (*security management*).

Coverage of **MAT_02** (*it must be possible to restore all or part of a system, application, data set and track in the event of damage, failure or negligence*).

BGC_INT (*communication and operations management*), CGS_SVG (*security management*).

Activity 5.2 : Security assurance requirements

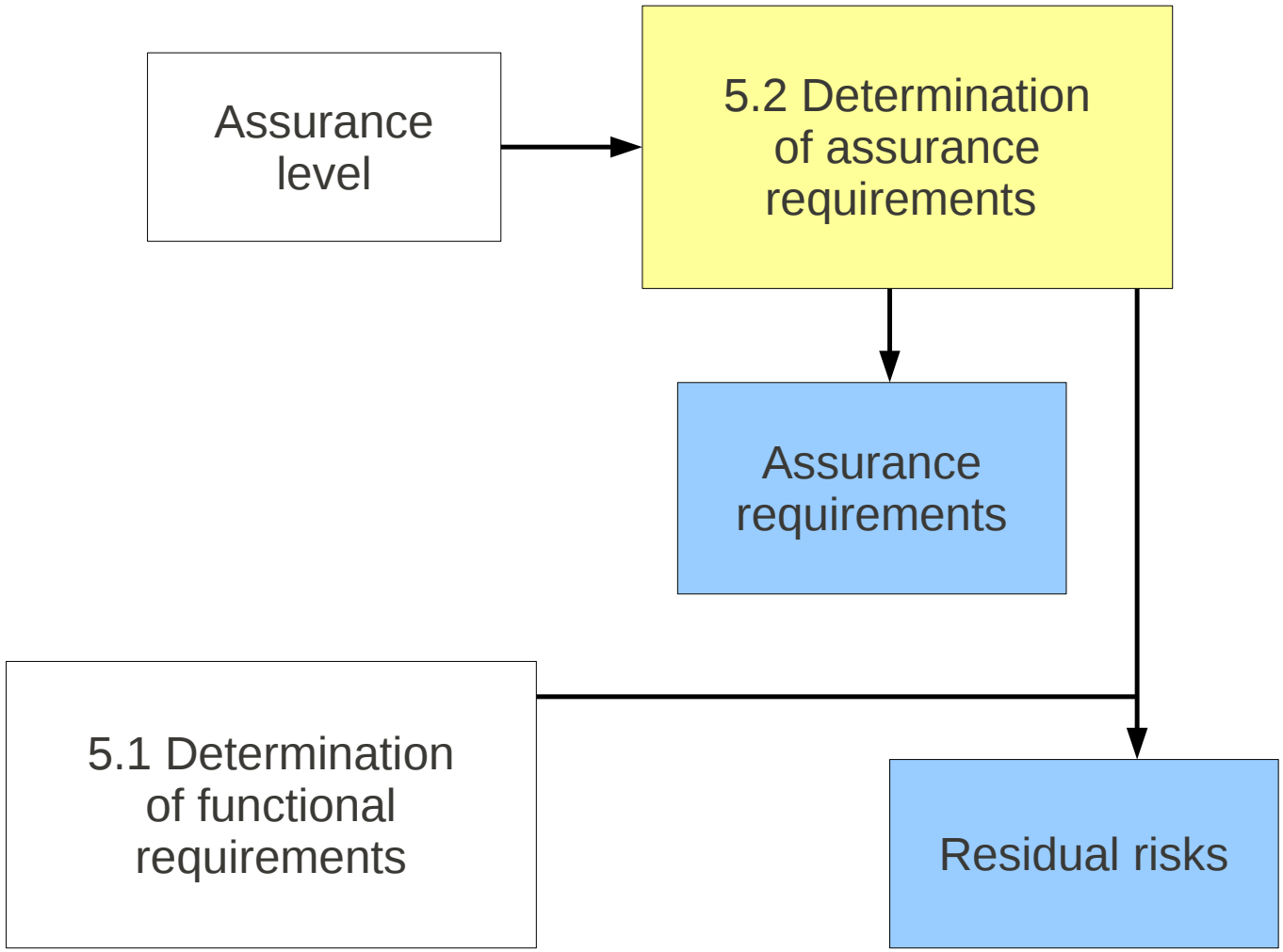

FIGURE: Determination of security assurance requirements

Activity 5.2 : Security assurance requirements

Contribution to risk treatment in the risk management process.

Provide a complete expression of the security **assurance requirements** of the security study target, depending to the EAL assurance level (activity 4.3).

Assurance requirements are used for the estimation that security functions are correctly implemented and that they satisfy the security objectives.

A list of **residual risks**, not covered by security assurance requirements, is provided.

Security assurance requirements

Security assurance requirements come from common criteria :

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

Remark : ACM class described in the Ebios guide does not exist in the last version 3.1 of common criteria.

Plan

Scientific description of risk

The first scientific definition of risk is given by Bernoulli in 1738 :

Le risque est l'espérance mathématique d'une fonction de probabilité d'événements.

For an event e_i, the likehood of occurence is denoted by p_i and the consequence is denoted by c_i.
The risk r concerned by n events $e_1, \ldots, e_n$ is defined by

$$r = \sum_{i=1}^{n} p_i c_i.$$