EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels, 21/06/2011
HR.DS5/GV/ac ARES (2011) 663475
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON INFORMATION SECURITY RISK MANAGEMENT

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 21/06/2011

Version 10/03/2011

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1.

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

This standard defines the risk management process for the information systems of the European Commission in line with the risk management framework[1] at the Commission (see reference GMORM and BUDG website). It must be used as described in section 4 of the 'Implementing Rules of Commission Decision C(2006) 3602'.

3. STANDARD OBJECTIVES

This standard for information security risk management aims at providing a consistent framework in which the risks related to information systems are identified, considered and addressed.

This standard defines the minimal steps an information security risk management process must implement. The annex describes in more detail how these steps may be applied practically to an information system.

4. SCOPE

This standard applies to all information systems that have been classified as SPECIFIC according to section 3.4 of the 'Implementing rules of Commission Decision C(2006) 3602'.

---

[1] The Commission's risk management strategy applicable to its business is defined in SEC(2005)1327 of 25 October 2005: "Communication to the Commission from Ms Grybauskaité in agreement with the President and Vice-President Kallas – Towards an effective and coherent risk management in the Commission services.

5. ROLES AND RESPONSIBILITIES

The overall responsibilities for Risk Management in Commission services are described in section 1.4 of the document: Risk management in the Commission – Implementation Guide – Update Version 2008[2].

The system owner is accountable for the security risk management process for an information system. This process must be initiated by the system owner, based on the security classification of the information system. The system owner is also accountable for the continual monitoring of risks and regular reviews of the risk management decisions.

The system owner may delegate the responsibility of managing the process to a project leader and of facilitating to a specialist in information security risk assessment, who could be an IT professional, an information security professional (e.g. LISO or SSO), a business person or an external consultant.

6. PRINCIPLES OF INFORMATION SECURITY RISK MANAGEMENT

Section 3.4 of the Implementing Rules of Commission Decision C(2006) 3602 defines how the risk management process must be applied. The following elements, for which instructions are given in the Annex, must be included in the information security risk management process.

(1) Scope definition — the scope of the information system and of the risk management process must be defined prior to starting and related to the business context under consideration. Any exclusions from the scope and any assumptions on threat or vulnerability level need to be justified.

(2) Asset identification and classification (valuation) — the identification and classification of assets must be performed as documented in the "Standard on Asset Management". The actual classification may be performed as described in the "Guidelines on Asset Classification". It consists of the following steps:

   (a) Identification of assets.

   (b) Classification (valuation) of identified assets.

(3) Risk identification — this step must be performed by identifying the threats to, and vulnerabilities of the system based on its characteristics. This consists of the following steps:

   (a) Identification of threats.

   (b) Identification of vulnerabilities.

[2] See http://www.cc.cec/budg/man/icrm/_doc/services/guidelines/doc_080415_implementationguide2008_en.pdf

(4) Risk assessment — this is performed by taking into account the required level of security needs derived from the asset identification and classification, the identified threats and vulnerabilities, and existing security measures. The risk assessment gives an overview of all risks and calculates the highest risks based on security needs and the possibility of a threat exploiting a vulnerability (threat occurrence likelihood and vulnerability level). It consists of the following steps:

(a) Assessment of the likelihood that a threat materialises by exploiting a vulnerability, which is the same as threat (to the vulnerability) likelihood multiplied by the vulnerability level to this threat.

(b) Identification of planned or existing security measures.

(c) Calculation of risk.

(d) Evaluation of the risks.

(5) Risk treatment — risks are treated through security measures that may be technical, physical, procedural and organisational. They consist of a combination of preventive measures, detective measures, avoidance tactics and/or transfer to another organisation. Priorities for actions are defined in a risk treatment plan to ensure that activities are focused on the significant risks.

For a given risk level and a selected environment, corresponding security measures available in the security standards must be used where available, but additional requirements and measures may always be selected if justified by the risk assessment and based on the rule of proportionality (additional requirements and measures must be proportional to the risk).

(6) Risk acceptance — residual risks, either risk remaining after treatment, or risk not treated and accepted, must be knowingly and objectively documented and approved by the management. This must be done using criteria for risk acceptance that have been approved by management.

(7) Risk monitoring — monitoring and reviewing must be performed concurrently throughout the whole information security risk management process. This includes the following activities:

- Implemented security measures must be monitored and reviewed regularly to ensure that they function correctly and effectively and that changes in the environment have not rendered them ineffective.

- Management must consider the changing risk environment and the ability of the implemented measures to deal with these changed risks. The scope of the information security risk management process may need to be redefined due to changes in the business objectives or to new or modified information assets.

(8) Risk communication — appropriate communication and consultation with internal and external stakeholders must be done at each stage of the

information security risk management process as well as on the process as a whole. The risk communication shall be subject to a strict "need to know" policy.

ANNEX – INFORMATION SECURITY RISK MANAGEMENT PROCESS

1. DEFINITION OF THE SCOPE

Standard statement — The scope of the ICT system and of the information security Risk Management process must be defined prior to starting and related to the business context under consideration. Any exclusion from the scope and any assumption on threat or vulnerability level need to be justified (see 6(1))

Before launching an information security risk management process, it is very important to define the scope of the system and the risk management process.

Defining the scope covers:

- Identification of the information handled by the information system, in any format and considering any input or output to the system (see Appendix A for a list of possible information assets, which comes from Section 3 of the Standard on Asset management).
- Identification of essential functions performed by the system.
- Physical locations and environments.
- The system boundaries (physical or logical) and interfaces.
- The persons (users, roles, system managers or IT service providers).
- The infrastructure (network, hardware, software, storage).
- Regulatory references (laws, policies, best practices, methodologies).
- Constraints, such as political constraints, strategic constraints, territorial constraints, structure constraints, constraints related to personnel, calendar or methods, budgetary constraints.

The information already available in the documentation of the project is helpful for the scope definition, such as the RUP vision document, the documents of the Strategic Planning and Programming cycle (e.g. the Annual Management Plan, Risk Management plans, Annual Activity Report), the "schema directeur" of the Directorate-General, the Business Continuity Plans, etc…

At this stage, assumptions may be made on the basis of the scope definition. Assumptions are very helpful to limit the extent of the risk management process and to focus on critical risks. Assumptions usually concern the Commission's internal or external policies, or financial and planning requirements, e.g. recruitment policy, obligation to use framework contracts, etc. They may also constitute a risk accepted a priori for a given environment.

Assumptions may also be made in the case that some functions are delivered by IT service providers where the service contract (e.g. service level agreements) defines a required security level.

All assumptions must be explicitly documented in the risk management process, particularly where they are used to limit the defined scope.

Roles and responsibilities

The information security risk management process is under the accountability of the system owner who may delegate the performance of the process.

Before launching this process, the scope must be defined under the responsibility of the system owner. This task should not be outsourced to a third party if its results are part of a call for tender for the full information security risk management study ,except if the third-party is excluded from the later study.

During this step, preliminary contacts should be made with all stakeholders to identify boundaries and constraints, and to make the necessary assumptions.

More information

See [EBIOS Activity 1.1 & 1.2 of section 3] for additional guidance.

2. ASSETS IDENTIFICATION AND CLASSIFICATION

Standard statement — Assets identification and classification are done in accordance with the Standard on Asset Management. The actual classification may be performed in accordance with the Guidelines on Asset Classification. (see 6.(2))

2.1. Identification of assets

An asset is something that has value or utility for the organization, its business operations and their continuity. Therefore, assets need protection to ensure correct business operations and business continuity.

The important assets **within the scope of the information system** (as defined in 1 above) must be clearly identified and appropriately classified (see 2.2 below). Examples of assets and more information about asset identification can be found in "Appendix A: Asset identification".

Grouping similar or related assets into manageable collections can help to reduce the effort necessary for the risk assessment process.

The documentation of the information and functions already performed (see section 1 above) may be used to identify supporting assets. Valuable information may also be found in the various inventories available at the Commission: GovIS for information systems, hardware and software inventories maintained by DIGIT or the IRMs, or design models and architecture documents from the project documentation.

Finally, a matrix must be created linking the essential information and functions with their supporting assets. A link between an essential element and supporting asset(s) is shown in the table by one or more crosses where the essential element row intersects with the columns of the assets concerned by this essential element. This matrix is used later to help to identify threats and vulnerabilities since the nature of the supporting asset leads to a collection of generic threats and vulnerabilities.

Roles and responsibilities

Asset identification requires the involvement of the asset owners, as identified as a result of the implementation of the Standard on Asset Management [SASSMGT].

More information

See [EBIOS Activity 1.3 of section 3] and [BS7799-3 5.2] for additional guidance.

2.2. Classification (valuation) of identified assets

In order to identify the appropriate protection for assets, it is necessary to assess their classification (value) in terms of confidentiality, integrity and availability. The classification levels result from the following:

- Direct or indirect business impacts of a loss of confidentiality, integrity and availability.
- Legal and business requirements.

It recommended that the classification process follows the "Method 3: Formal classification based on business impact assessment" as described in section 7 of the "Guidelines on Asset Classification".

It is not necessary to define the classification (value) for each individual supporting asset (e.g. hardware, software, etc) at this stage since this will be done at the step dedicated to the 'Calculation of risk' taking into account anticipated threats and related vulnerabilities (see section 4.3).

Roles and responsibilities

The roles and responsibilities for the classification of assets are defined in the Standard on Asset Management.

More information

See [SASSMGT].

3. RISK IDENTIFICATION

Standard statement — The Risk Identification must be performed by identifying the threats and vulnerabilities of the system based on its characteristics (see 6(3)).

3.1. Identification of threats

A threat is a potential for the accidental or deliberate compromise of security involving loss of one or more of the properties of confidentiality, integrity and availability of information systems or the information contained therein [Definition in 3602].

Threats may be of natural or human origin, and the source may be accidental or deliberate. Both accidental and deliberate threat sources need to be identified, knowing that the likelihood of their occurrence needs to be assessed further in the process. It is essential that no relevant threat be overlooked since this could result in information system failure or weaknesses in the information system security.

Threat identification starts with the selection of attack methods that are relevant to the scope of the information system. It should be based on the list of generic attack methods and threat agents proposed in Appendix B.

The attack methods listed in appendix B are grouped in different categories or themes under the following headings:

- Physical damage.
- Natural events.
- Loss of essential services.
- Disturbance due to radiation.
- Compromise of information.
- Technical failures.
- Unauthorised actions.
- Compromise of functions.

This classification facilitates the selection of relevant attack methods.

In case relevant attack methods not listed in the Appendix B are identified using past incidents, from security studies about similar systems or from audit reports, they should also be classified in one of the above categories.

Attack methods that have a potential impact on at least one of the confidentiality, integrity or availability of the information system must be selected.

It is advisable to document why an attack method or a complete attack category has not been selected so that the choices made can be traced. For instance, attack methods of physical or environmental origin such as seismic or volcanic phenomenon whose occurrence is linked to the physical location of the asset may be discarded. The same may apply to attack methods that only impact the confidentiality security criteria for information that are classified public.

The selected attack methods should be characterised in accordance with the security criteria (availability, integrity and/or confidentiality) they may directly breach. This characterisation is derived from the **direct impacts** on the security criteria, rather than all the potential indirect impacts. For example: a fire primarily affects the availability of the information system but it may also indirectly affect its integrity and confidentiality; fire is therefore usually related to a breach of availability.

These links between selected attack methods to their affected security criteria (identical to those used for expressing asset classification) make it much easier in the next steps to compare the security needs with the threats in order to determine the real risks.

Roles and responsibilities

To be carried out under the accountability of the system owner. Any exclusion of attack methods and impact categories must be validated by the system owner.

More information

See [EBIOS Section 4], [BS7799-3 Annex C.2].

See [BS7799-3 Annex C.3] for a list of threats related to ISO17799 topics.

3.2. Identification of vulnerabilities

For each attack method selected, the vulnerabilities of the target system that could make the attack possible must be identified.

A vulnerability is a weakness or lack of safeguards that might facilitate or permit the materialisation of a threat to an information system or the information contained therein [Definition of 3602]. The vulnerability in itself does not cause harm, it is merely a condition or set of conditions that might allow a threat to exploit it and cause harm to the assets and the business they support.

An attack method may exploit several vulnerabilities.

A vulnerability that has no corresponding threats[3] may be discarded, but should be identified and monitored for changes. It should also be noted that

[3] For instance, all attack methods that may exploit the vulnerability have been discarded in the previous threats.

incorrectly implemented or malfunctioning measures or measures being used incorrectly should be considered as vulnerabilities.

Practically, for each asset type supporting essential functions or information identified in section 2.1 and for each attack method selected in section 3.1, the relevant vulnerabilities should be selected from the list of generic vulnerabilities given in the Appendix C. In this appendix the identification of vulnerabilities is related to the type of asset they are affecting. The possible asset types are:

- Physical environment, including facilities
- Personnel
- Organisation
- Hardware
- Software
- Media
- Networks

Any other vulnerability relevant to the information system that is not listed in the appendix may also be added to the list.

Roles and responsibilities

To be carried out under the accountability of the system owner in collaboration with all asset owners since vulnerabilities are characteristics of the information system.

More information

See [EBIOS Section 4], [BS7799-3 Annex C.4].

4. RISK ASSESSMENT

Standard statement — The Risk Assessment is performed by taking into account the required level of security needs derived from the assets identification and classification, the identified threats and vulnerabilities and the existing security measures. Risk assessment gives an overview of all risks and calculates the highest risks based on security needs and the possibility of a threat to materialise by exploiting a vulnerability (threat occurrence likelihood and vulnerability level). (See 6(4)).

4.1. Assessment the possibility of a threat to materialise by exploiting a vulnerability (threat occurrence likelihood and vulnerability level)

After identifying the threats and vulnerabilities (see section 3) it is necessary to assess the likelihood that they will come together to cause harm. This includes assessing the likelihood of threats occurring and how easily vulnerabilities can be exploited by the threats.

The assessment of likelihood of threats should take the following into account:

- Deliberate threats — the likelihood of deliberate threats of human origin depends on the motivation, knowledge, capacity and resources available to possible attackers, and the attractiveness of the assets to sophisticated attacks.

- Accidental threats:

  – The likelihood of accidental threats can be estimated using statistics and experience.

  – The likelihood of these threats might also be related to the organization's location or proximity to sources of danger, such as major roads or rail routes, and factories dealing with dangerous material such as chemical materials or petroleum.

  – The organization's geographical location will also determine the possibility of extreme weather conditions.

  – The likelihood of human errors (one of the most common accidental threats) and equipment malfunction should also be estimated.

- Past incidents — incidents that occurred in the past can illustrate problems in the current protective arrangements.

- New developments and trends — this includes reports, news and trends obtained from the Internet, news groups or other organizations that can help to assess the threat situation.

Depending on the need for accuracy in the risk or threat exposure, it may be necessary to split assets into smaller components and relate the threats to these components.

The second factor influencing the possibility of a threat to materialise by exploiting a vulnerability is the vulnerability level to that threat i.e. how easily the vulnerability could be exploited by a threat agent. A vulnerability should be assessed in relation to each threat that might exploit it in a particular situation. For example, a system may have a vulnerability to the threats 'masquerading of user identity' and 'misuse of resources'. The vulnerability to 'masquerading of user identity' may be high because of lack of user authentication. On the other hand, the vulnerability to 'misuse of resources' may be low because, even with lack of user authentication, the means by which resources might be misused are limited.

Valuation scales are proposed in Appendices D and E.

Roles and responsibilities

To be carried out under the accountability of the system owner in collaboration with all asset owners since vulnerabilities are characteristics of the information system.

More information

See [EBIOS Section 3, Activity 3] and [BS7799-3 Annex C.5.2].

4.2. Identification of existing measures

It is important to assess the existence and the effectiveness of the existing security measures for the following reasons:

- A measure that does not properly mitigate a risk is a source of vulnerability and should be replaced by a more effective one.
- Effective measures should be taken into account for the calculation of the risk (see 4.3).
- New security measures selected at the risk treatment stage (see 5) should be additional to, and compatible with the existing effective measures.
- Effective measures might be replaced by more suitable ones for reasons of cost, coverage or effectiveness.

The result of this step is a list of all existing measures, their method of risk mitigation (reduce threat, reduce vulnerability, reduce impact, detect incident or recover from incident) and their implementation and use status.

This step may be omitted when performing an assessment of a new system for which a full new set of security measures has to be identified and implemented.

Roles and responsibilities

To be carried out under the accountability of the system owner in possible collaboration with all asset owners and other security staff with knowledge of security measures.

4.3. Calculation of risk

The objective of this step is to identify and calculate the risks to which the IT system and its assets are exposed in order to identify and select appropriate and justified security measures.

The calculation of risk is a function of the following:

(a) Classification (valuation) of the assets expressing the likely **impact** (I referred to below) resulting from a loss of confidentiality, integrity and/or availability (outcome of section 2).

(b) Likelihood of threats occurring to cause the potential adverse business impacts (outcome of section 4.1).

(c) Vulnerability level to threats or ease of exploitation of the vulnerabilities by the identified threats (outcome of section 4.1).

(d) Effective existing measures or measures that reduce the risk (outcome of section 4.2).

The result of this step is a list of measured risks for each of the impacts on confidentiality, integrity or availability for the information system under consideration. Furthermore the determination of the measures of risk helps identify which risks should be dealt with first when selecting security measures. The method used should be repeatable and traceable.

Appendices D and E propose two approaches to calculate risk.

The first approach, which is described in appendix D, is based a single assessment for the likelihood of the attack of the threat against a vulnerability. In this case the calculation of risk is the product of the likelihood of the attack (A), and the impact (I): R= A * I.

The second approach, which is described in appendix E, is based on separate assessment of the threat likelihood (bullet point (b) above) and of the vulnerability level to a threat (bullet point (c) above). In this case, the calculation of the risk is the product of the threat likelihood (T), the vulnerability level (V, including the effect of existing measures) and the impact (I): R = T * V * I).

Roles and responsibilities

To be carried out under the accountability of the system owner who can delegate the actual calculation.

4.4. Evaluation of the risks

The final step of the risk assessment is to express the risks in terms of impacts for the business and recovery time, such as "serious damage for the Commission's activities, from which the Commission cannot recover in less than half a year".

Relating the risk levels to the Commission's activities is necessary to realistically assess the impact the calculated risks have on the Commission's activities and helps to convey the meaning of the risk levels to management as required by [COMRM].

This also helps to identify which risk could be accepted, by taking into account the generally acceptable risk levels as defined in [COMRM 2.2], i.e. those risk levels where the estimated damage is small enough for the Commission to cope with in continuing their day-to-day business and where, therefore, further action is not necessary.

All other risks require further action and should be subject to the risk treatment and management decision, as discussed in section 5.

Evaluation of the risks uses the results of the calculation of the risks of section 4.3, together with the impacts identified in the asset valuation in section 2.2. This translates the results of the risk assessment into business impacts that can be analysed and reported to management.

The table given in Appendix F: Risk scenario report should be used, as it also facilitates the selection of adequate measures.

Finally, in compliance with [GMORM 2.2], the most significant risks (high business impact value) must be recorded in a risk register. Access to the register shall be granted on a strict “need to know” basis.

Roles and responsibilities

To be carried out under the accountability of the system owner, in accordance with the roles and responsibilities defined in [COMRM].

More information

See [COMRM], [GMORM].

5. RISK TREATMENT

Standard statement — Risks are treated through a combination of technical, physical, procedural and organisational security measures. They consist in a combination of prevention measures, detection measures, avoidance tactics and/or transfer to another organisation. Priorities for action are defined in a risk treatment plan to ensure that activities are focused on the significant risks. For a given risk level and a selected environment, corresponding security measures available in the Commission information systems security policy must be used where available, but additional requirements and measures may always be selected if justified by the risk assessment and based on the rule of proportionality (additional requirements and measures must be proportional to the risk) (See 6(5)).

5.1. Decision making

Once a risk has been assessed a management decision needs to be made concerning how the risk must be treated. Different circumstances dictate what kind of decision is made.

The main factors that might influence the decision are:

- The possible impact if the risk materialises, i.e. the cost related to each occurrence of the risk, as evaluated in section 4.4
- How frequently incidents are expected to occur over a defined period of time, which may be difficult to estimate due to the lack of publicly available statistics on their frequency.

The product of the two factors above gives an indication of the total impact that can be expected over a same period of time if nothing is done to mitigate the risks and thereby lead to the definition of critical risks in accordance with [COMRM 2.4].

In addition to considering the estimated cost of security risks, the cost of the risk treatment decision should be considered. For example, a comparison between the investment needed to implement an appropriate set of measures as opposed to doing nothing, and the potential impact if something goes wrong, can show whether the measures are cost-effective. If not, then it may be worth investigating alternative solutions (e.g. a solution which provides lower coverage of the risks but which costs much less, so that the total cost of the measures and the unmitigated risks is lower).

Other factors that might also influence the information security risk management decision-making process are:

- Willingness to accept risks (also known as the risk tolerance or appetite for risk), which is sometimes necessary in order to make progress.
- Ease of implementation of the measure.
- Resources available.

- Current business/technology priorities and constraints.
- Organizational and management policies.

5.2. Reduce the risk

Where the option to reduce the risk has been chosen, appropriate measures should be implemented to reduce the risks to the level that has been identified as acceptable, or at least as much as feasible towards that level.

Measures can reduce the assessed risks in many different ways, for example by:

- Reducing the threats or reducing the threat agent motivation by increasing the cost of the attack.
- Reducing the likelihood of the vulnerability being exploited by decreasing the vulnerability level to the threat.
- Reducing the possible impact if the risk occurs.
- Detecting unwanted events, reacting, and recovering from them.

The choice between the different ways of reducing the risk (or a combination of them) depends on the business requirements, the environment and the circumstances in which the Commission needs to operate. It is always important to match the measures to the specific needs of the Commission's mission, activities or objectives, and to justify their selection.

Measures may be grouped in different categories:

- Physical measures.
- Procedural measures.
- Organisational measures.
- Technical measures.

The required strength[4] of the security measures should mainly be based on the risk level as assessed in section 4.4.

When selecting measures for implementation, a number of other factors should be considered including:

- Ease of use and cost of the measure.

[4] By strength, it is meant the degree of resistance of the security measures to an attack, but also the assurance we can have that the measure is effectively protecting against the threats

- Reliability and repeatability of the measure (whether- formally structured or- ad-hoc. and whether- performed manually or programmed).

- Relative strength of the measure.

- Operational type of the measure (directive, preventive, detective, corrective, recovery).

Roles and responsibilities

To be carried out under the accountability of the system owner. Moreover there is no universal or common approach to the selection of measures. The selection process is likely to involve a number of decision steps, consultation and discussion with different parties of the business and with a number of key individuals, as well as a wide-ranging analysis of business objectives.

More information

Selected measures must be compliant with the high-level security objectives of the Implementing Rules and its related security standards that provide the security measures for the security needs of systems classified as STANDARD (see section 5 of the Implementing Rules). Additional measures may be selected from ISO/IEC 17799:2005, from [EBIOS Section 5] and also from additional sources, as and when necessary.

5.3. Accept the risk

There are risks for which either no measure can be identified, or the cost of implementing the measure(s) outweighs the potential loss if the risk materialises. In these cases, a decision may be made to accept the risk and live with the consequences if the risk occurs.

These decisions must be documented so that all key stakeholders are made aware of, and agree to accept, the risk and its impact.

Where such a risk is deemed to be unacceptable by key stakeholders but too costly to mitigate through measures, it may still be decided to transfer the risk.

Risk acceptance requires a wide consultation of all stakeholders. It is important to avoid possible bias in decision-making

Roles and responsibilities

All key stakeholders should be consulted on the acceptance of risk (see also section 6).

More information

See [COMRM 2.2].

5.4. Transfer the risk

Risk transfer is an option when it is difficult to reduce or control the risk to an acceptable level or it can be more economically transferred, fully or partly, to a third party. There are several mechanisms for transferring risk to another organization:

- The use of insurance, although there is still an element of residual risk because there are usually conditions and exclusions that will be applied depending on the type of risk occurrence for which an indemnity is not provided.

- The use of third parties or outsourcing partners to handle critical business assets or processes, although care must be taken that all security requirements, control objectives and controls are included in associated contracts to ensure that sufficient security will be in place. In addition, it is advisable to specify the security activities that should be undertaken in service levels, together with specific performance measures, so that activity and performance can be measured. There is always still a level of residual risk since the ultimate responsibility for the security of the outsourced information and information processing facilities remains with the Commission. Moreover, through the act of outsourcing, new risks will be introduced which will need to be assessed and managed.

Roles and responsibilities

This is the accountability of the system owner in collaboration with the project leader and, if applicable, with legal and resources department dealing with internal or external service providers.

5.5. Avoid the risk

Risk avoidance describes any action by which the activities or objectives are changed to avoid any risk occurring (for example, simply stop performing a risky activity). Risk avoidance needs to be balanced against business, regulatory or contractual needs. Under such constraints, one of the other options, i.e. risk transfer or risk reduction should be considered.

Roles and responsibilities

To be carried out under the accountability of the system owner although the project leader can propose risk avoidance possibilities.

5.6. Risk treatment plan

Once the risk treatment decisions have been taken, the activities to implement these decisions need to be identified and planned. Clear responsibilities must be allocated to individuals.

In summary, the following activities need to be undertaken when formulating a risk treatment plan.

- Limiting factors and dependencies should be identified.

- Measures should be described.
- Priorities should be established.
- Deadlines should be identified and milestones should be agreed.
- Resource requirements should be estimated and resources identified.
- Approvals to spend or allocate resources should be obtained.
- The critical path should be identified.

Once the risk treatment plan has been formulated, resources can be allocated and the activities to implement the risk treatment decisions can be started. At this stage, there is a clear review process in place to ensure that activities are undertaken as planned, deliverables are of the desired quality, milestones are met and resource estimates are not exceeded (see also 7.3).

Roles and responsibilities

The project leader integrates risk treatment decisions in the overall project plan and is responsible for its implementation. The system owner is accountable and approves the plan beforehand.

More information

Project planning information can be found in the RUP and TEMPO methodologies.

6. RISK ACCEPTANCE

Standard statement — Residual risks, either risk remaining after treatment, or risk not treated and accepted, must be knowingly and objectively documented and approved by the management. It must be done against criteria for risk acceptance that have been approved by the management.

After the risk treatment decisions have been implemented, there are always risks remaining (residual risks). It should be assessed how much the risk treatment decisions help to reduce the risk, and how much residual risk remains to ensure that sufficient protection is achieved.

If the residual risk is unacceptable, a business decision needs to be made about how to resolve this situation. The risk treatment options described in chapter 5 should be reviewed to determine how to further reduce the risk to an acceptable level.

Whilst it is generally good practice not to tolerate unacceptable risks, it might not always be possible or financially feasible to reduce all risks to an acceptable level. In these circumstances, it might be necessary to knowingly and objectively accept the risk (see section 5.3). The accepted residual risks must be documented and approved by management.

Roles and responsibilities

The management, i.e. the Director General, must approve any residual risks that are above acceptable levels.

More information

See [COMRM 2.2].

7. MONITORING RISK[5]

Standard statement — Risk monitoring and reviewing must be done concurrently throughout the whole information security risk management process. This must include the following activities:

• Implemented security measures must be monitored and reviewed regularly to ensure that they function correctly and effectively and that changes in the environment have not rendered them ineffective.

• Management must consider the changing risk environment and the ability of the implemented measures to deal with these changed risks. The scope of the risk management process might need to be redefined due to changes in the business objectives or to new or modified information assets.

7.1. Monitoring and maintenance

Implemented security measures should be regularly monitored and reviewed to ensure that they function correctly and effectively and that changes in the environment have not rendered them ineffective. Monitoring is intended to detect any deterioration of the performance of the security measures and initiate corrective action.

The majority of security measures require maintenance and administrative support to ensure their correct and appropriate functioning during their life. These activities should be planned and performed on a regular, scheduled basis. In this manner their overhead can be minimised, and the relevance of the security measures preserved. Maintenance activities include:

- Checking the log files.
- Modifying parameters to reflect changes and additions.
- Reviewing the security measures and the compliance with them.
- Updating the measures, policies and procedures with new versions.

These monitoring and maintenance activities must be part of the security measures applied to the system.

Roles and responsibilities

[5] This section contains information that is also covered in the Standard on Compliance.

To be carried out under the accountability of the system owner. The IT service providers and system managers are responsible for the maintenance and correct operation of the security measures. The project leader must plan the necessary activities.

7.2. Risk reviews and re-assessments

The results of the original security risk assessment and management reviews must be regularly reviewed for changes. There are several factors that could change the originally assessed risks.

Any new function could lead to new or changed information assets.

Other changes in the risk situation might result of modifications of the organization, objectives and/or activities, of the review of the correctness and effectiveness of the implemented security measures (see section 7.1), and of external changes (e.g. environmental, social, regulatory and political).

New or changed threats and/or vulnerabilities may also be identified.

A good source for the above is the feedback and experience gathered from security incidents which may lead to the fine-tuning and/or upgrading of security measures, and which may in turn change the initial risk assessment.

After all these different changes have been taken into account, the risks should be re-calculated and necessary changes to the risk treatment decisions and security measures identified and documented. These changes should be agreed with management and implemented.

In compliance with [GMORM 2.2], the most significant new risks (high business impact value) must be recorded in a risk register. The access to the register shall be granted on a strict "need to know" basis.

Risk assessment studies, risk treatment plans and risk acceptance decisions must be part of the information system documentation. Access to the information system documentation must be granted according to its classification.

Roles and responsibilities

The risks reviews and reassessment are under the responsibility of the system owner who can delegate the performance of these tasks to others in collaboration with all asset owners, who should inform him of any change of conditions.

7.3. Audits

Regular internal audits are scheduled and conducted by an independent party (e.g. the Internal Audit Capacity of the DG, the Internal Audit Service of the Commission).

When internal audits discover a need for actions to adjust the management or the operation of security, these should be fully documented, responsibility should be assigned and a target date should be determined.

Roles and responsibilities

The different audit services establish their annual audit work plan that is approved by their hierarchy. System owners may request an audit of his system to be planned. In accordance with the results of the audit, the system owner and the project leader must propose an action plan and report regularly on progress to audit services.

8. RISK COMMUNICATION

Standard statement — Appropriate communication and consultation with internal and external stakeholders must be done at each stage of the risk management process.

8.1. Documentation control

Complete, accessible and correct documentation and a controlled process to manage documents are necessary to support the security process and to provide evidence that the security process is operating correctly and efficiently. The documentation is an asset of the information system; therefore it must be managed accordingly and its access must be granted in accordance with its classification.

Roles and responsibilities

Documentation control is under the accountability of the system owner but he can delegate the responsibility for overseeing the process of managing documentation lies to the project leader.

8.2. Communication plan

The information security risk management process requires co-operation with, and input from many levels and functions of an organization and from key stakeholders. Effective risk reporting and communications are therefore essential.

A communication plan should be established, which identifies key players and decision-makers as well as mechanisms for disseminating decisions and for collecting feedback. The plan should contain a risk communication policy describing which risk is communicated to whom and to what level of detail. The communication policy shall be based on a strict “need to know” basis. The plan should include mechanisms for regular updating of risk information as part of the ongoing security awareness programme. It should also include procedures for dealing with public relations issues that might arise from publicity about security incidents.

Feedback is an essential ingredient in making a risk management process more effective. The aim is to ensure that information security risk

management becomes part of the organizational culture. Identification and reporting of problems, increased risks and security incidents should be encouraged. These should be collected and evaluated systematically. An effective risk management process should draw information from all possible sources, including management and all employees and contractors, irrespective of their function, as well as external parties such as outsourcers, suppliers and customers, where relevant.

Roles and responsibilities

The system owner must communicate to all parties their commitment to the risk management process. He is accountable for the communication plan, which he establishes in collaboration with the different asset owners. He must report all critical risks to the top management, i.e. the Director General, who may decide to include them in the Annual Activity Report.

More information

See [COMRM 2.5]

9. REFERENCE DOCUMENTS

	Description	Version or date
DECPRO	EC 844/2001: COMMISSION DECISION amending its internal Rules of Procedure - COMMISSION PROVISIONS ON SECURITY	29 Nov 2001
DECSIS	C(2006) 3602: COMMISSION DECISION concerning the security of information systems used by the European Commission	16 Aug 2006
IR	Implementing rules for Commission Decision C (2006) 3602 of 16/8/2006	29/05/2009
COMRM	SEC(2005) 1327: COMMUNICATION TO THE COMMISSION " Towards an effective and coherent risk management in the commission services"	28 Oct 2005
COMGOV	SEC(2004) 1267: COMMUNICATION TO THE COMMISSION on the improvement of information technology governance in the Commission	20 Oct 2004
REGPERS	EC 45/2001: REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data	1 Feb 2001
COMBCM	SEC(2006) 898: COMMUNICATION TO THE COMMISSION on a "Framework for Business Continuity Management in the Commission	12 Jul 2006
COMeCOM	C(2005) 4473: COMMUNICATION TO THE COMMISSION on e-Commission 2006-2010: enabling efficiency and transparency	23 Nov 2005
GMORM	See BUDG website for documents related to Risk management at the Commission at the page : http://intracomm.cec.eu-admin.net/budg/man/icrm/services/guidelines/rmguidelines_en.html See the following implementation guide: Risk Management Implementation Guide See also the following document for IT risk guidance: http://intracomm.cec.eu-admin.net/budg/man/icrm/_doc/services/guidelines/doc_081218_itguidance_en.pdf	2008
EBIOS	Risk Management method (Expression des Besoins et Identification des Objectifs de Sécurité) http://www.ssi.gouv.fr/site_article45.html	Version 2
SASSMGT	Standard on asset management	22/06/2009
BS7799-3	Information security management systems – Part 3: Guidelines for information security risk management	2006

APPENDIX A: ASSET[6] IDENTIFICATION[7]

One of the most valuable and important asset types is information.

Information assets are found in many different forms: for example in databases and data files, Commission or system documentation, contracts, user manuals, training material, operational or support procedures, guidelines, documents containing important results of the Commission's business, continuity plans, or fallback arrangements.

In addition, there are other assets that are used to store or process information, or which have an impact on the security of the information assets. These other assets include the following:

- Software: such as business applications, package or standard software (database management software, application server software, web server software, etc.), service, maintenance or administration software (backup software, etc.), operating systems, development tools and utilities

- Network: such as medium and support (cable, fibre, etc.), passive and active relay (router, switches, etc.), communication interfaces (WIFI connection devices, etc.), network interconnection devices (firewalls, gateways, proxies, etc.)

- Hardware: such as data processing equipment (fixed or transportable equipment, processing peripherals, etc.), data media (electronic or other media)

- Sites: such as places (building, offices, computer rooms, etc.), essential services (telephone lines and network, power supply, cooling and anti-pollution devices, etc.)

- Personnel and organisation: such as users, system administrators, developers, external personnel (subcontractors, suppliers, manufacturers, etc.), structure of the organisation, project or service organisation

---

[6] An asset is anything that has a value for the Commission: it may be tangible or intangible.

[7] The list of assets is taken from section 3 of the Standard on asset management.

APPENDIX B: GENERIC ATTACK METHODS

This list is taken from [EBIOS Section 4, part 3]. For more details, please consult the detailed explanation of EBIOS. The table also indicates the usual impact category (Availability, Confidentiality or Integrity) and the cause (Accidental or Deliberate). It is recommended to keep the numbering when writing threat scenarios (see section 3.1 Identification of threats) since this facilitates the comparison of risk analyses.

	Impact on			Cause	
Attack method	**A**	**C**	**I**	**Accidental**	**Deliberate**
1 - Physical damage					
01 – FIRE	X		X	X	X
02 - WATER DAMAGE	X		X	X	X
03 - POLLUTION	X		X	X	X
04 - MAJOR ACCIDENT	X		X	X	X
05 - DESTRUCTION OF EQUIPMENT OR MEDIA	X		X	X	X
2 - Natural events					
06 - CLIMATIC PHENOMENON	X		X	X	
07 - SEISMIC PHENOMENON	X		X	X	
08 - VOLCANIC PHENOMENON	X		X	X	
09 - METEOROLOGICAL PHENOMENON	X		X	X	X
10 - FLOOD	X		X	X	
3 - Loss of essential services					
11 - FAILURE OF AIR-CONDITIONING	X			X	X
12 - LOSS OF POWER SUPPLY	X			X	X
13 - FAILURE OF TELECOMMUNICATION EQUIPMENT	X			X	X
4 - Disturbance due to radiation					
14 - ELECTROMAGNETIC RADIATION	X		X	X	X
15 - THERMAL RADIATION	X		X	X	X
16 - ELECTROMAGNETIC PULSES	X		X	X	X
5 - Compromise of information					
17 - INTERCEPTION OF COMPROMISING INTERFERENCE SIGNALS		X			X
18 - REMOTE SPYING	X	X	X		X
19 - EAVESDROPPING		X			X
20 - THEFT OF MEDIA OR DOCUMENTS		X			X
21 - THEFT OF EQUIPMENT	X	X			X
22 - RETRIEVAL OF RECYCLED OR DISCARDED MEDIA		X		X	X
23 - DISCLOSURE		X		X	X
24 - DATA FROM UNTRUSTWORTHY SOURCES	X		X	X	X
25 - TAMPERING WITH HARDWARE		X			X
26 - TAMPERING WITH SOFTWARE	X	X	X	X	X
27 - POSITION DETECTION		X			X
6 - Technical failures					
28 - EQUIPMENT FAILURE	X			X	
29 - EQUIPMENT MALFUNCTION	X			X	
30 - SATURATION OF THE INFORMATION SYSTEM	X			X	X
31 - SOFTWARE MALFUNCTION	X		X	X	
32 - BREACH OF INFORMATION SYSTEM MAINTAINABILITY	X			X	X
7 - Unauthorised actions					
33 - UNAUTHORISED USE OF EQUIPMENT	X	X	X		X
34 - FRAUDULENT COPYING OF SOFTWARE		X			X
35 - USE OF COUNTERFEIT OR COPIED SOFTWARE	X			X	X
36 - CORRUPTION OF DATA		X	X		X
37 - ILLEGAL PROCESSING OF DATA		X			X
8 - Compromise of functions					

	Impact on			Cause	
Attack method	**A**	**C**	**I**	**Accidental**	**Deliberate**
38 - ERROR IN USE	X	X	X	X	
39 - ABUSE OF RIGHTS	X	X	X	X	X
40 - FORGING OF RIGHTS	X	X	X		X
41 - DENIAL OF ACTIONS			X		X
42 - BREACH OF PERSONNEL AVAILABILITY	X			X	X

Humans are potentially dangerous threat sources. The following table[8] presents an overview of possible human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack.

Threat-Source	**Motivation**	**Threat Actions**	**Attack method**
Hacker, cracker	Challenge Ego Rebellion	Hacking Social engineering System intrusion, break-ins Unauthorized system access	14, 19, 30, 33, 36, 40
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer crime (e.g., cyber stalking) Fraudulent act (e.g., replay, impersonation, interception) Information bribery Spoofing System intrusion	17, 19, 23, 24, 33, 34, 36, 40, 41
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/Terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering	1, 2, 3, 4, 5, 11, 12, 13, 14, 19, 25, 26, 30, 33, 36, 40
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)	17, 18, 19, 20, 21, 22, 24, 25, 26, 27, 33, 40
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error, lack of maintenance)	Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access	18, 19, 20, 21, 22, 23, 24, 25, 26, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42

[8] Taken from NIST Special Publication 800-30.

APPENDIX C: GENERIC VULNERABILITIES

This list is taken from [EBIOS Section 4, part 4]. It summarises each vulnerability for every asset type and the attack method that could exploit the vulnerability. This facilitates the creation of attack scenarios. For more details, please consult the detailed explanation of EBIOS.

Vulnerability	Asset type	Attack method
Access point allowing unlawful eavesdropping	Network	37
Access privileges to shared information difficult to manage or not managed at all (definition, implementation, monitoring)	Network	23
Access right management functions too complicated to use and capable of producing an error	Hardware	23
Access to back-up equipment not protected	Hardware	20
Access to communication terminal equipment not protected	Physical	19
Access to the tracking system is not protected	Software	41
Accesses to the IS are not secured (gateways, intrusion detection, supervision of security events, etc.)	Organisation	36
Additional hardware items can be fitted for storing, transmitting or corrupting information (e.g. physical keylogger).	Network	25
Additional hardware items can be fitted for storing, transmitting or corrupting information (e.g. physical keylogger).	Hardware	25
Additional software can be added for storing, transmitting or corrupting information (e.g. keylogger)	Network	26
Ageing of cooling pipes	Physical	2
Ageing of the equipment	Hardware	28
Ageing of the equipment	Network	28, 29
Ageing of the medium	Media	28, 29
Ageing of the premises	Physical	1
Analysis of match between needs and equipment capabilities not organised	Organisation	28, 29
Ancillary equipment making it easier to pick up compromising stray signals (electrical cables, pipes, etc.)	Physical	17
Application requiring computing resources not matched by the equipment (e.g. insufficient RAM)	Software	30
Application that is complex to use	Software	38
Applications are not checked before installation	Software	26, 31, 32, 36, 40
Applications can be modified or changed	Software	26
Archives requiring air-conditioning for their preservation	Media	11
Assignment files too complex or unpractical	Software	24, 26, 39, 40, 41
Assignment of user rights is not clearly defined	Organisation	39
Audit functions are not separate from monitoring functions	Organisation	41
Back-up hardware, software or procedures modified without taking old back-ups or archives into account	Media	32
Ceiling or external opening not watertight	Physical	2
Change of the organisation's policy or strategy	Organisation	41
Circulating information in clear text	Network	19
Climatic conditions not taken into account in the construction of the premises	Physical	6
Communication in broadcast mode	Network	19
Complex routing between sub-networks	Network	19, 23
Conditions of use outside operating limits of the equipment	Hardware	6, 9
Configuration of software components not managed or prone to management errors (e.g. application of a UK patch not adapted to a FR version)	Software	31
Conflictual industrial relations	Personnel	1, 2, 3, 5, 24, 26, 42
Conflictual situation	Personnel	26, 36, 40, 41
Connection passwords not sufficiently complex	Software	26, 36, 39, 40, 41
Contract contains no clauses concerning identification and verification of the origin of the software	Organisation	35

Vulnerability	Asset type	Attack method
Correct reflex actions not known if an anomaly is detected	Personnel	26
Credulity	Personnel	24
Difficult industrial relations possibly resulting in transport strikes	Physical	42
Documentation not up to date	Software	31, 32
Earthing of exposed conductive parts does not comply with regulations	Physical	12
Easily dismantled equipment	Hardware	21
Easily removed hard disc	Hardware	20
Easily transported or removable media (e.g. floppy disc, ZIP disc, removable hard disc, tape)	Media	20, 37
Equipment accessible to persons other than its owners (e.g. located in a passage way)	Hardware	5
Equipment accessible to unauthorised persons	Network	5
Equipment allowing data to be recorded on media (floppy disc, ZIP disc, CD/DVD writer)	Hardware	34
Equipment capable of emitting compromising stray radiation	Network	17
Equipment capable of emitting compromising stray radiation	Hardware	17
Equipment freely available to a number of persons	Hardware	21
Equipment maintained remotely via telecommunication equipment	Hardware	13
Equipment or medium sensitive to electromagnetic or thermal radiation	Hardware	14, 15, 16
Equipment requiring air-conditioning in order to operate	Hardware	11
Equipment sensitive to electrical disturbances (voltage drops, overvoltages, transient power-cuts)	Hardware	12
Equipment sensitive to vibrations	Hardware	7
Equipment that can be resold (no marking, used without password)	Hardware	21
Equipment that is complex to use or not user-friendly	Network	38
Equipment that is complex to use or not user-friendly	Hardware	38
Equipment used on self-service basis by a number of persons	Hardware	20
Equipment using flammable materials (e.g. bulk printers producing dust)	Hardware	1
Equipment with a communication interface that can be eavesdropped (infrared, 802.11, Bluetooth, etc.)	Hardware	19
Equipment zoning not taken into account	Network	17
Equipment zoning not taken into account	Hardware	17
Existence of obsolete components in the information-processing infrastructure (development in languages no longer used, etc.)	Personnel	32
Existence of periods or events that cause a very significant increase in use of the system	Software	30
External opening not watertight	Physical	2
Failure to appreciate the importance of qualifying information	Personnel	24
Failure to comply with anti-virus software updating rules	Personnel	26
Failure to comply with development rules	Personnel	32
Failure to comply with instructions	Personnel	38
Failure to comply with quality rules	Personnel	32
Failure to comply with rules concerning the destruction of media containing classified information	Personnel	22
Failure to comply with the IT charter specifying the rules of use	Personnel	33, 34, 35, 36
Failure to follow rules concerning information classification.	Personnel	20, 23
Failure to follow the rules concerning physical protection of transportable equipment	Personnel	21
Failure to follow work procedures	Personnel	31
Failure to observe discretion	Personnel	23
Failure to take into account a specific environment that increases the risks of failure (overheated atmosphere, industrial environment, etc.)	Physical	28, 29
Flaws in the management of access privileges to messaging gateways	Network	19
Fragility of equipment	Hardware	5

Vulnerability	Asset type	Attack method
Fragility of media	Media	5
High political / economic stakes	Organisation	41
Inaccessibility of support media outside the organisation or from a country with a large time difference	Hardware	32
Inadequate awareness of the need to protect sensitive information	Personnel	23
Inappropriate organisation	Organisation	40
Incorrect operating conditions	Hardware	28, 29, 38
Incorrect operating conditions	Network	28, 29
Incorrect sizing (e.g. too much data for the maximum bandwidth)	Network	30
Incorrect sizing of emergency power supply equipment (inverter, batteries, etc.)	Physical	12
Incorrect sizing of emergency resources	Physical	30
Incorrect sizing of operating and maintenance resources	Personnel	31
Incorrect sizing of resources (e.g. insufficient reserve time on a laptop battery).	Hardware	30
Incorrect sizing of resources (e.g. not enough storage or file share space)	Software	30
Incorrect sizing of resources (e.g. too many simultaneous connections)	Software	30
Incorrect sizing of resources (e.g. too many users for the maximum capacity of the directory)	Network	30
Incorrect sizing of resources (e.g. too many users for the number of connections possible and the bandwidth)	Network	30
Incorrect sizing of storage spaces for received messages	Software	30
Incorrect sizing of telecommunication resources, resulting, for example, from daily use of resources intended for the emergency solution.	Network	30
Incorrect use of the messaging service (mailboxes used as storage space)	Software	30
Installation rules not taken into account	Network	17
Installation rules not taken into account	Hardware	17
Insufficient competency	Software	38
Insufficient monitoring of material requirements for developing an application	Personnel	33
Insufficient training in measures and tools for protecting external and internal exchanges	Personnel	19
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	Personnel	30, 31, 32
Interface side effects (compatibility problems between protocols, etc.)	Network	31
Interface with a function that allows eavesdropping	Network	19
Interface with technical characteristics specific to the country (e.g. different telephone connectors between France and the United Kingdom)	Network	29, 38
Lack of awareness of individual responsibilities	Organisation	37
Lack of confidence in the organisation	Personnel	41
Lack of discretion or vigilance	Personnel	27
Lack of information concerning conditions of use of emergency power supply points	Personnel	12
Lack of information concerning laws and regulations applicable to information processing	Organisation	34, 37
Lack of motivation for work involving data keying	Personnel	38
Lack of personnel awareness	Organisation	37
Lack of professionalism	Personnel	38
Lack of responsibility	Software	38
Lack of responsibility	Hardware	38
Lack of training	Personnel	31
Lack of understanding of responsibilities	Personnel	38
Locatable equipment (e.g. triangulation)	Hardware	27
Logical access to equipment allowing eavesdropping software to be installed	Hardware	19
Loss or poor management of original documents (support contracts, licences, etc.)	Media	32
Low awareness of the need to economise the organisation's IT resources (poor use of storage spaces, etc.)	Personnel	30

Vulnerability	Asset type	Attack method
Low awareness of the need to protect confidential documents, leading to a lack of vigilance	Personnel	20
Low awareness of the need to protect equipment outside the organisation	Personnel	21, 25
Low awareness of the need to protect information	Personnel	18
Low awareness of the need to protect the confidentiality of information exchanges	Personnel	19
Low awareness of the threat posed by malicious codes	Personnel	26
Low maintenance budget	Personnel	32
Maintenance contract monitoring not organised	Organisation	28
Maintenance fault	Hardware	28
Maintenance fault	Network	28, 29, 32
Maintenance or use of the equipment only possible if network supports are available	Network	32
Managers have no contact with the expertise or technology watch departments	Organisation	17, 24, 25, 26, 33, 37, 39, 40
Manual triggering of the emergency solution	Physical	28, 29
Media accessible to unauthorised persons	Network	5
Media are complex to use or not user-friendly	Media	38
Media available to everyone	Media	20, 33, 37, 41
Media can be used to exchange sensitive information	Media	23
Media or documents sent or present outside the site	Physical	20
Media sent via postal services (external service providers, internal mail service, etc.)	Media	20
Media storage not protected	Media	20
Medium accessible to persons other than its owners	Media	5
Medium and supports capable of emitting compromising stray radiation	Physical	17
Medium and supports whose characteristics allow eavesdropping (e.g. Ethernet, wireless communication systems)	Network	19
Medium and supports with technical characteristics specific to their locality (e.g. different ADSL configuration parameters between France and the United Kingdom)	Network	29, 38
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	Hardware	6, 7, 8, 9, 10
Medium sensitive to storage conditions	Media	3
Medium unsuitable for the life of data to be stored	Media	28, 29
Missions not suited to the personnel	Personnel	40
No access control to information	Organisation	36, 37
No access logging	Network	23
No access monitoring device when equipment is inactive	Software	19
No access rules	Software	33, 36
No accessible support	Software	38
No accessible user support	Software	38
No accessible user support	Hardware	38
No accessible user support	Network	38
No analysis of emergency power level required if equipment is added	Physical	12
No anti-virus check on exchanges	Software	26
No anti-virus filtering system	Software	26
No archive storage measures suitable for the storage periods (ageing of tapes, wear of CD-ROMs)	Media	5
No archiving procedure	Media	42
No audit of physical access control procedures	Hardware	39
No audit of physical access control procedures	Media	40
No audit or supervision of accesses (for example inventory of accesses outside the organisation and types of data flow)	Software	33, 36, 37

Vulnerability	Asset type	Attack method
No audit policy	Software	39, 40, 41
No authentication of equipment connected to the network	Network	19
No authorisation management and monitoring policy imposed at the organisation's sites	Organisation	36, 39
No awareness and training programme for processes relating to continuity of professional activities	Organisation	42
No awareness of the risks of sanction	Organisation	33, 34, 40
No awareness or information concerning copyright law	Organisation	34, 35
No awareness programme concerning risks incurred through downloading software	Software	26
No awareness programme concerning the risks incurred by opening attachments	Software	26
No awareness programme concerning the risks of usurping of identity (misuse of means of authentication such as passwords)	Personnel	24
No awareness programme for protection of equipment	Personnel	1, 2, 3, 5
No backtrack procedure in the event of a modification error	Software	32
No back-up of data contained on the media	Media	1, 2, 4, 5, 20
No back-up of event logs	Software	39, 40, 41
No back-up procedure	Software	36
No back-up redundancy or procedure	Media	36
No cable layout plan	Network	32, 38
No checking (or tracking) of exchanges with the outside	Physical	23
No checking to confirm that emergency resources operate correctly	Physical	28, 29
No clause covering response time for repair and replacement in the event of equipment failure	Organisation	28
No clause covering response time for repair and treatment in the event of malfunction	Organisation	29
No clause or procedures for transfer of knowledge	Organisation	42
No clear identification of water stop cocks	Physical	2
No climate of trust between individuals	Organisation	40
No clock synchronisation procedure	Software	31
No code of conduct	Personnel	33, 40
No confidentiality clause in the contract	Organisation	37
No content monitoring	Software	37
No continuity clause for service provision	Organisation	42
No continuity plan covering the organisation's essential activities	Organisation	28, 29, 31, 32
No contractual clause concerning the definition of communication and exchange procedures	Organisation	41
No contractual clause covering the activity (in the event of shutting down the activity, supplier bankruptcy, etc.)	Organisation	32
No contractual clause covering the quality of service of systems placed under limit conditions (intense demand on the system, input of non-compliant data, input of data corresponding to operating limits)	Organisation	30
No contractual clause relating to electromagnetic compatibility	Organisation	14
No contractual clauses concerning the use of fraudulent copies of software	Organisation	34
No contractual clauses covering compensation for damage in the event of loss of an essential service	Organisation	11, 12, 13
No contractual clauses covering support and call-out conditions	Organisation	31
No contractual clauses covering the maximum acceptable downtime of an essential service	Organisation	11, 12, 13
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	Organisation	17, 18, 19, 20, 21, 22
No contractual clauses guaranteeing cover of the activities if a crisis is declared at a subcontractor or a supplier's site	Organisation	1, 2, 4, 6, 7, 8, 9, 10
No contractual clauses guaranteeing the safety of supplies delivered by a subcontractor or supplier	Organisation	26
No contractual clauses relating to the protection of IT equipment	Organisation	36
No contractual clauses relating to the use of IT equipment	Organisation	33
No contractual clauses setting out the responsibilities of both parties	Organisation	39
No control of access to information stored in the directory	Network	23
No control of access to the site or premises	Physical	1, 2, 5

Vulnerability	Asset type	Attack method
No control of access to the site or premises or possibility of intrusion via indirect access routes.	Physical	19, 20, 21
No control of access to the site or premises or possibility of intrusion via indirect access routes.	Physical	26
No correctly sized redundant equipment	Physical	11
No crisis management organisation	Organisation	1, 2, 4
No data protection rules	Hardware	36
No decision to resize when significant increases in the use of IT resources are observed.	Personnel	30
No definition of privileges limiting the possibility of installing software on workstations	Organisation	35
No definition of responsibilities	Organisation	41
No definition of the right to know	Organisation	39
No diagnostic function to prevent equipment failures	Software	28, 29
No disciplinary procedures	Organisation	41
No document base for rules and procedures	Organisation	42
No double checking of critical processes	Organisation	38
No effective and operational virus shield	Software	23
No emergency procedure	Software	32
No emergency service close to the organisation	Organisation	4, 6, 7, 8, 9, 10
No emergency situation management procedures	Personnel	4
No encryption system	Software	37
No equipment inventory	Hardware	20, 21
No equipment verification procedure before purchase or after maintenance work.	Organisation	17
No event logging	Software	39, 40, 41
No explicit documentation on the application systems	Software	38
No failure reporting (volumes, cost of incidents, downtime)	Organisation	28
No filter to protect the system against saturation	Software	30
No filtering and logging on communication relays between networks	Network	23
No filtering system	Network	23
No fire partitions	Physical	1
No fire-fighting organisation (description of roles and responsibilities)	Organisation	1
No formalisation of responsibilities known by everyone	Personnel	38
No global policy for fighting against malicious code	Organisation	26
No global policy for managing and archiving tracks and other elements of proof	Organisation	41
No guarantee of the organisation's durability	Organisation	32
No guarantee that water detectors are operating correctly	Organisation	2
No hierarchical organisation or reporting procedure	Organisation	41
No history recording persons entering and leaving	Physical	41
No identification of security needs for a project	Organisation	18, 19, 20, 21
No identification of sensitive assets	Organisation	18, 19, 20, 21, 22, 23, 25, 26
No identification of the system protection levels	Software	37
No implementation of basic security rules applicable to the operating system and software	Software	26, 36
No implementation of incident monitoring to foresee failures or saturation (trend charts)	Personnel	28, 29, 30
No incident monitoring to foresee failures or saturation (trend charts)	Organisation	29, 30, 31
No incident monitoring to foresee malfunctions (trend charts)	Personnel	31
No individual commitment to protect confidential documents	Personnel	20
No information concerning the division of responsibility and means of guaranteeing the legitimacy of a request.	Organisation	24
No information or awareness concerning residual data on media	Personnel	22
No information protection policy	Organisation	17, 18, 20, 23
No information protection policy applicable to recycling and discarding	Organisation	22
No information protection policy imposed at the organisation's sites	Organisation	36, 37

Vulnerability	Asset type	Attack method
No installation standard for sites belonging to the organisation	Organisation	1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13
No instructions (warning, prevention, reaction, etc.)	Organisation	8, 9, 10, 11, 12, 13
No instructions aimed at eliminating risk-inducing behaviour in the use of information resource	Organisation	31
No instructions concerning the use of IT equipment	Organisation	33, 36
No instructions for avoiding the use of IT resources in a manner that leads to saturation of storage spaces or processing resources.	Organisation	30
No instructions given to internal or external personnel working on the premises	Personnel	1, 2, 5, 6, 7
No instructions relating to incidents (detection, action, etc.)	Organisation	30, 31, 32, 37
No insurance cover for serious damage	Organisation	1, 2, 4, 5
No internal support tool	Software	32
No inventory of media used	Media	20
No IT charter specifying the rules of use	Personnel	33, 34, 35, 36
No labelling of cables or cable layout plan	Physical	38
No labelling of media	Media	38
No licence monitoring policy imposed at the organisation's sites	Organisation	34
No licence monitoring policy imposed at the organisation's sites	Organisation	35
No limits on the size of attachments	Software	30
No logging of entry to the site	Physical	33, 34, 35, 36
No maintenance of air-conditioning equipment	Physical	1, 2, 3, 11
No maintenance of termination and distribution equipment	Network	13
No maintenance procedure	Software	31, 32
No maintenance procedure	Network	31
No management of access authorisation	Software	37
No management of emergency equipment inspection reports	Organisation	1, 2
No management of information access privileges (possibility of corrupting public data, etc.)	Software	23
No management of licences or registration and activation measures	Software	33, 34, 35
No management of profile privileges (administrators, users, guest, etc.)	Software	34
No management of profile privileges (administrators, users, guest, etc.)	Hardware	34
No management of the equipment assets	Personnel	33
No management of write rights in shared storage spaces.	Software	30
No management support for application of the security policy	Personnel	18, 19, 20, 21, 22, 23, 24, 27, 34, 35, 36, 39, 40, 41
No maximum response time for support guarantees	Network	32
No means of checking the safety of media when they enter the organisation	Media	26
No means of destroying the media	Media	22
No means of encryption	Media	37
No means of guaranteeing the authenticity of codes	Personnel	24
No means of guaranteeing the authenticity of developments	Personnel	26
No means of guaranteeing the source of equipment	Hardware	24
No means of guaranteeing the source of supplies	Organisation	24
No means of identifying the sensitivity of information contained on the media	Media	37
No means of protecting and monitoring data integrity	Media	36
No means of protecting and monitoring data integrity	Software	36
No means of ventilation or air-conditioning during excessive summer heat	Physical	6
No measure to avoid negligence when information is sent	Network	23
No measures for checking developments	Organisation	26
No measures for protecting code integrity during the design, installation and operation phases	Organisation	26
No measures to make communication lines and equipment secure	Physical	33, 36
No mechanism for monitoring actions, logs and alerts	Organisation	41

Vulnerability	Asset type	Attack method
No monitoring of application of the security policy	Organisation	17, 18, 19, 20, 21, 22, 24, 25, 26, 36
No monitoring of critical processes by the parent organisation	Organisation	38
No monitoring of data integrity	Software	36
No monitoring of installation and maintenance procedures (configuration and parameter setting records)	Software	32
No monitoring of maintenance and support contracts with suppliers	Organisation	28, 32
No monitoring of maintenance contracts	Organisation	1, 3
No monitoring of product certification	Organisation	35
No monitoring of product origin	Organisation	35
No monitoring of sensitive assets	Organisation	20, 22, 23, 25, 26
No monitoring procedure	Organisation	33, 34, 40
No mutual checking of codes	Organisation	41
No network partitioning	Network	40
No one responsible for the protection of personal data and information	Organisation	37
No operating procedure	Physical	38
No operational qualification procedures	Organisation	25, 29
No organisation for management of security incidents	Organisation	20, 21
No organisation for protecting documentation and system maintenance resources	Organisation	32
No partitioning of communication networks	Network	19, 23, 30, 36
No partitioning of equipment	Hardware	40
No passing up of information for a centralised failure analysis	Personnel	28, 29
No passing up of information for a centralised malfunction analysis	Software	31
No personal commitment to protect confidentiality	Organisation	23
No personnel protection team	Organisation	42
No physical and logical protection	Network	39
No physical and logical protection (partitioning, etc.)	Network	36, 40
No physical protection	Hardware	37, 39, 40
No policy for authorising access to information	Organisation	36
No policy for checking the correct sizing of the equipment of the information processing infrastructure, including the emergency equipment	Organisation	30
No policy for partitioning user environments to avoid unintentional assignment of rights to modify the system and application	Organisation	31
No policy for protecting the workstations	Organisation	26
No policy for storing and analysing activity tracks	Organisation	24, 26
No precautions taken at the installation phase for fire risks specific to the equipment housed.	Physical	1
No prevention and detection of viruses and other malicious programmes	Organisation	36
No procedure and means for destruction	Media	37
No procedure and means of verifying the origin of the software (code signature, binary signature, etc.)	Personnel	35
No procedure for access to classified information	Organisation	41
No procedure for assessing products	Personnel	35
No procedure for checking work carried out by external personnel on the organisation's equipment	Organisation	25, 26
No procedure for passing up information in the event of detection	Organisation	40
No procedure for personnel authorisation	Organisation	40
No procedure for testing incoming goods and confirming their compliance with the specifications	Software	38
No procedure or system for authorising personnel to modify data	Software	36
No procedures for checking authorisation of personnel entering the site or premises	Physical	33, 34, 35, 36, 39, 40
No procedures for checking external floppy disks	Organisation	36
No procedures for checking the identity of all persons entering the premises or zones	Physical	33, 34, 35, 36
No procedures for system configuration management	Organisation	32
No procedures for transfer of knowledge	Organisation	42
No procedures for validating hardware components when they are delivered or returned	Organisation	25

Vulnerability	Asset type	Attack method
from maintenance		
No process for managing the continuity of the organisation's professional activities	Organisation	42
No process for managing the continuity of the project team's professional activities	Organisation	42
No product certification	Personnel	35
No protection against electrical disturbances	Hardware	28, 29
No protection against lightning	Physical	9
No protection against rising water levels	Physical	10
No protection against spam	Software	30
No protection against the use of advanced privileges	Software	19
No protection against the use of advanced privileges	Software	26
No protection and audit of access to sensitive information	Organisation	37
No protection and classification of information	Personnel	36, 37
No protection measures (read only, etc.)	Software	38
No protection of access to equipment	Physical	17
No protection of equipment against theft (anti-theft cable)	Hardware	20
No protection of logs containing activity tracks	Software	19
No protection of media	Media	40
No protection of spaces dedicated to information exchange or sharing	Organisation	40
No provisions for monitoring and sanctioning	Organisation	37, 39
No qualification of developments in a context representative of operation	Software	30
No Quality Assurance Manual	Organisation	32
No quick response instructions to protect equipment in the event of water damage or fire	Organisation	28
No regulation defining rights	Organisation	39
No report for maintenance operations	Software	31, 32
No reporting on malfunctions	Organisation	29
No restriction on software entry points	Software	36
No revision of air-conditioning needs when premises are modified or equipment is added.	Physical	11
No robust access control system	Network	36, 40
No robust access control system	Hardware	39
No rules and procedures for personnel authorisation	Organisation	40
No rules covering conditions of use of information processing infrastructures (ban on smoking, drinks and food in rooms housing IT equipment)	Organisation	28
No rules covering the operating environment of information processing infrastructures (temperature, humidity, etc.)	Organisation	29
No rules for checking equipment entering/leaving the organisation	Organisation	21
No rules for protecting the confidentiality of information that can be used to locate a personnel member (ticket requests, entry/exit records, etc.)	Organisation	27
No rules for protecting the exchange of confidential information	Organisation	18, 19
No rules for the use and storage of hardware and information media (protection conditions during transport, smoking ban, etc.)	Organisation	5
No rules imposing the use of standards	Organisation	17, 29, 30, 31
No screen saver when equipment is inactive	Software	18
No security policy for protecting the information processing infrastructure in the organisation's sites	Organisation	18, 19, 20, 21, 24, 25, 26, 27
No security policy for protecting the information processing infrastructure in the organisation's sites	Organisation	32, 33
No security rules for developments	Personnel	31
No site inspection by emergency services (fire-fighting services)	Organisation	1
No sizing of the automatic fire extinction system, or incorrect sizing or inadequacy of this system.	Physical	1
No standard or norm	Personnel	32
No storage of activity tracks	Software	24
No storage of processing tracks	Software	31, 32
No strict routing between sub-networks	Network	23

Vulnerability	Asset type	Attack method
No structure allowing identification of a person to be guaranteed within the organisation or a project	Organisation	24
No structure responsible for defining, implementing and monitoring access privileges to information	Organisation	23
No subject in the internal regulations dealing with responsibilities for information systems security	Organisation	37
No substitute organisation for sensitive functions	Organisation	42
No substitutes for strategic personnel	Organisation	42
No substitution equipment	Hardware	1, 2, 4, 5, 21
No sump	Physical	2
No supervision tool	Software	38
No sure means of identification	Software	24
No systematic qualification procedure before installation or updating	Software	31
No test of reaction and information procedures in the event of an accident	Personnel	1, 2, 3, 6, 7, 8, 9
No tracking and auditing system	Hardware	41
No training in the use and maintenance of new software	Personnel	31, 32, 38
No training on the equipment or software used	Organisation	38
No training plan concerning security issues	Organisation	36
No training plan for maintenance of new systems	Organisation	32
No training to explain the conditions controlling the lawful use of information	Personnel	37
No updated display of information for calling the emergency services	Organisation	1, 2, 4
No up-to-date labelling and diagram of the architecture	Network	38
No use of norms or standards relating to information system development	Organisation	32
No user documentation for existing applications	Personnel	38
No validation of keyed data entries	Software	38
No verification of approved shared access	Software	23
No vigilance when a maintenance agent works on a workstation or server	Personnel	25
No warning, reaction or information instructions in the event of water damage (no identification of stop cocks, etc.)	Organisation	2
No water stop cock	Physical	2
Non-intuitive software	Software	38
Non-upgradable hardware	Hardware	32
Non-upgradable software	Software	32
Obsolete hardware	Hardware	32, 36
Obsolete hardware	Network	32
Obsolete medium	Media	32
Obsolete software	Software	32
Obtaining an advantage	Personnel	33, 34, 39, 40, 41
Obtaining an advantage through disclosing information	Personnel	20
Obtaining an advantage through disrupting the information system	Personnel	26, 30
Obtaining an advantage through misinforming	Personnel	24, 25
Obtaining an advantage through picking up information	Personnel	19
Obtaining an advantage through selling equipment	Personnel	21
Operating faults on the internal telephone network	Network	13
Operating problem already encountered on the telecommunication service supply	Network	13
Operator or maintainer with extended privileges	Personnel	26
Original media	Media	1, 2, 4, 5, 20
Password for accessing support software changed rarely or not at all	Software	19
Password for accessing the system or application changed rarely or not at all	Software	18, 19
Penalty or sanction clause out of proportion or not suited to the context	Organisation	41
Personnel categories with higher access privileges	Personnel	39

Vulnerability	Asset type	Attack method
Personnel living a long way from the premises	Physical	42
Personnel not aware of the risk of sanction	Personnel	33, 34, 35, 36, 37
Personnel not used to keying	Personnel	38
Personnel receive no communication or information concerning authorisation procedures	Organisation	40
Personnel susceptible to enticement	Personnel	19, 20, 21, 22, 23, 24, 25, 26, 36
Physical access to communication support or equipment allowing eavesdropping equipment to be installed	Network	19
Physical or logical access to a relay allowing eavesdropping equipment to be installed	Network	19
Pirated programmes can be installed	Software	26
Political / economic conflict between the organisation's home country and its host country	Organisation	42
Polluted atmosphere (hangar, workshop, etc.)	Physical	3
Poor equipment reliability	Hardware	28, 29
Poor equipment reliability	Network	28, 29
Poor management of pilot releases and configurations	Network	31
Poor medium reliability	Network	28, 29
Poor storage conditions	Media	28, 29
Possibilities of destruction caused by an external event (collisions, attacks)	Physical	4
Possibility of adding an eavesdropping programme such as a Trojan horse	Software	19
Possibility of adding software derivations	Network	26
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	Software	37, 39, 40, 41
Possibility of circuit derivation	Network	25
Possibility of corrupting a communication	Network	24
Possibility of creating or modifying system commands	Software	26
Possibility of deleting, modifying or installing new programmes	Software	26
Possibility of eavesdropping on exchanges with application servers	Network	19
Possibility of eavesdropping on exchanges with authentication servers	Network	19
Possibility of incompatibility between equipment items	Hardware	29
Possibility of incompatibility between resources	Network	29
Possibility of incompatibility between the media and other components	Network	29
Possibility of incorrect configuration, installation or modification of relays	Network	29, 30, 31
Possibility of incorrect configuration, installation or modification of the operating system	Software	29, 30, 31
Possibility of installing a backdoor or Trojan horse in the operating system	Software	33, 37
Possibility of installing an eavesdropping device on messaging gateways	Network	19
Possibility of installing correction programmes, updates, patches, hot fixes, etc.	Software	24, 26
Possibility of interfering with data transmitted via the communication media	Network	36
Possibility of introducing eavesdropping software on client terminals	Network	19
Possibility of modifying or corrupting the software	Software	26
Possibility of picking up transmissions outside the site	Physical	19
Possibility of remote administration of the system using non-encrypted administration tools	Network	26, 36, 39, 40, 41
Possibility of remote system administration	Software	26, 36, 39, 40, 41
Possibility of remote system administration from any station	Software	26, 36, 39, 40, 41
Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	Hardware	38
Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	Hardware	42
Possibility of subjecting the relays to an excessive number of requests or intense interference (e.g. denial of service attacks such as smurfing, SYN flood etc.)	Network	30
Possibility of subjecting the system to an unlimited number of requests	Software	30, 31

Vulnerability	Asset type	Attack method
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	Software	39, 40, 41
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow)	Software	31, 40
Possibility of the systems operating with illegally copied or counterfeit operating systems	Software	35
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	Organisation	33, 40, 41
Possibility of usurping the directory function	Network	24
Possible existence of hidden functions introduced during the design and development phase	Software	26
Possible harm to personnel using the equipment (wireless transmission, emanations, etc.)	Network	42
Possible side effects after updating a software component	Software	31
Presence of a communication network with the outside allowing exchange of information	Network	23
Presence of a device allowing remote modification or installation of applications	Software	26
Presence of a fire extinction system using water	Physical	2
Presence of an opening onto a public right-of-way (window)	Physical	1
Presence of discarded media in public places	Physical	22
Presence of discarded media outside the site	Physical	22
Presence of observation point outside the site	Physical	18
Presence of protocol that has no authentication function	Software	26, 40
Presence of residual data unknown to the user of reallocated or discarded equipment	Hardware	22
Presence of residual data used by the software	Software	22, 23
Presence of shared directory for storing information	Hardware	23
Printer present in passage way	Hardware	20
Procedures for managing access privileges too heavy to operate	Software	23
Programmes or system files can be deleted or modified	Software	26
Proprietary operating system distributions can be easily copied	Software	34
Protocol not allowing safe authentication of the sender of a communication	Network	24
Proximity of a source of electromagnetic or thermal radiation	Physical	14, 15, 16
Proximity of industrial activity or potentially hazardous site	Physical	4
Proximity of pollution sources (noise, smoke, vapour, etc.)	Physical	3
Public access close to the buildings	Physical	17
Public access to the gateway	Network	30
Requirements defined for a project without taking into account special situations that put the system under limit conditions.	Software	30
Resource sharing makes it easy for unauthorised persons to use the system	Software	33, 36, 39, 40, 41
Resources can be used without tracking	Network	23, 24, 26, 39
Responsibilities for information systems security not dealt with in the internal regulations	Organisation	33, 34, 35, 36, 39, 40, 41
Responsibility of each person not known	Personnel	41
Rights assigned without legitimate need	Personnel	33, 40
Risk of electromagnetic or thermal radiation not taken into account in the design	Physical	14, 15, 16
Risks arising from the proximity of an electromagnetic source not taken into account	Hardware	14, 15, 16
Room situated close to a public right-of-way	Physical	17
Rooms containing acid-based batteries are not specifically designed and physically isolated from the equipment to which they are connected	Physical	12
Rooms in which explosion/implosion risks have not been taken into account	Physical	4
Screen observable from outside	Physical	18
Security responsibilities concerning the classification of information are not formalised or known by everyone	Organisation	20, 23

Vulnerability	Asset type	Attack method
Seismic conditions not taken into account in the construction of the buildings	Physical	7, 8
Sensitive documents read in public places (documents observed by external persons, etc.)	Media	18
Shared use of connection identifier	Software	33
Single copy of licence contracts	Software	1, 2, 3, 4, 5
Single internally-developed applications	Software	1, 2, 3, 4, 5, 20
Site in which extreme weather phenomena occur periodically (storm, hurricane, cyclone, etc.)	Physical	9
Site listed as volcano-prone	Physical	8
Site located in flood-prone area	Physical	2, 10
Social problems	Personnel	42
Software can be easily copied	Software	34, 35
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	Software	37, 39, 40, 41
Software incompatibility (e.g. side effect of message-filtering anti-virus software, etc.)	Software	31
Software not adequately tested before acceptance (test data set does not cover all the operating conditions - intense demand on the system, input of non-conforming data, input of data corresponding to operating limits)	Organisation	31
Software not adequately tested before acceptance, especially concerning limit values	Organisation	25
Software retrieval from a non-authenticated source	Software	24, 26
Software that is complex to use	Software	38
Some highly sensitive operations can be performed by a single person	Personnel	38, 39, 40
Specialised personnel accommodated in remote rooms	Physical	42
Specific hardware	Hardware	32
Specific hardware	Network	32
Specific software	Software	32
Standard interface allowing information exchanges (e.g. Bluetooth interface accepting all communications by default)	Network	23
System depending on a chilled water or power supplier	Physical	11
System maintained or operated via the network	Network	32
System not adequately sized to meet the needs	Physical	11
Technical characteristics can be modified (e.g. MAC address of an Ethernet card)	Network	40
Technical rooms too cramped	Physical	38
Technology chosen without guarantee of continuity	Personnel	32
TEMPEST zoning not carried out	Physical	17
Tempting equipment (trading value, technology, strategic)	Hardware	20, 21, 37
Tempting or popular operating system	Software	34
Tempting or popular software	Software	34, 35
Terminal communication equipment with no emergency power supply	Hardware	12
The access system allows software downloads	Software	34, 35
The access system allows software storage	Software	34, 35
The access system does not log tracks of its operation	Software	41
The computing equipment is not homogenous	Organisation	31
The equipment allows system resources to be used from outside	Network	33
The equipment can be accessed and used by everyone	Hardware	41
The equipment can be accessed by everyone	Network	33
The equipment can be booted from any peripheral (e.g. floppy disc, CD-ROM)	Hardware	26, 36
The equipment can be used for purposes other than those intended	Software	33
The equipment can be used for purposes other than those intended (development of software for use outside the organisation, etc.)	Hardware	33
The equipment is connected to external networks	Network	33, 40
The floor or wall coverings are not anti-static	Physical	12
The interfaces are connected to external networks	Network	40

Vulnerability	Asset type	Attack method
The interfaces can be accessed by everyone	Network	40
The low voltage panel is not accessible	Physical	12
The medium / low voltage transformer substation is not installed on the site (with controlled supplier access)	Physical	12
The medium allows system resources to be used from outside	Network	41
The messaging system allows automatic message transmission	Software	26, 30
The messaging system allows software updates to be installed (e.g. patches, anti-virus updates, etc.)	Software	26
The messaging system can be accessed from Internet	Software	40
The network allows the system resources to be modified or adjusted	Network	26, 36, 40, 41
The network makes it easy for unauthorised persons to use the resources	Network	26, 36, 40, 41
The notion of right is not defined for the personnel	Personnel	39
The operating system allows a session to be opened without password	Software	40, 41
The operating system allows access to data (data base, etc.)	Software	36
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	Software	39, 40, 41
The operating system can be used to make anonymous connections	Software	39, 41
The operating system does not log system records or events	Software	39, 41
The operating system is not checked before installation	Software	36
The operating system logs can be modified by anyone	Software	39, 40, 41
The organisation is under-sized	Organisation	42
The organisation's activity is impaired by its industrial relations	Organisation	42
The organisation's financial or technological continuity is not secure	Organisation	42
The origin of applications is not checked before installation	Software	34, 35
The password base of the operating system is decipherable	Software	39, 40, 41
The passwords entered for access to the operating system are decipherable	Software	39, 40, 41
The principle of least privilege is not applied	Software	39
The principle of least privilege is not applied	Network	39
The protocol does not allow certain identification of the sender	Network	41
The relays can be accessed by everyone	Network	41
The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	Network	24, 40
The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	Network	40
The remote maintenance link is permanently activated	Software	26, 36, 40, 41
The security policy does not include reminding all personnel of their obligations and responsibilities in civil, criminal and regulatory matters.	Organisation	35
The security policy is not applied	Organisation	17, 18, 19, 20, 23, 33, 34, 40
The security policy is not applied especially in relation to processing of personal information	Organisation	37
The security responsibilities concerning authorisation management are not formalised.	Organisation	18, 19
The security responsibilities concerning authorisation management are not formalised.	Organisation	40
The SNMP layer is activated	Software	26, 36, 40, 41
The software allows access to data (content of hard disc, data base, etc.)	Software	36
The supports and medium are connected to external networks	Network	40
The supports and medium can be accessed by everyone and are active by default (e.g. RJ45 connectors intermingled)	Network	41
The system allows access to data that cannot be authenticated (e.g. hoax)	Network	24
The system allows asynchronous operation of certain parts or commands of the operating system (e.g. JavaScript components exploring the hard disc content)	Software	26, 36
The system allows asynchronous operation of certain parts or commands of the operating system to be exploited (e.g. automatic opening of attachments)	Software	26, 36
The system allows attachments to be exchanged	Network	23
The system allows hostile software such as Trojan horses, viruses, worms, logic bombs, etc. to be introduced	Software	36
The system allows information to be sent and received without authentication of the senders or recipients	Software	24

Vulnerability	Asset type	Attack method
The system allows information to be stored or modified without authentication of the authors	Software	24
The system allows relaying	Software	24
The system allows remote deleting, modifying or installing of programmes	Software	36
The system can be accessed by everyone	Software	33, 39, 40, 41
The system can be used by all personnel	Network	23
The system can be used for purposes other than those intended	Network	33
The system has no means of preserving the activity history	Software	24
The system does not allow the author of a modification to be identified	Software	24
The system does not allow the person issuing a request to be identified	Software	24
The system is connected to external networks	Network	23, 33, 37, 41
The system makes it easy to disclose information to the outside	Software	23, 37
Unavailability arising from a competition factor	Personnel	42
Unavailability caused by absenteeism	Personnel	42
Unavailability caused by illness	Personnel	42
Unavailability caused by third parties (physical aggression, hostage taking, etc.)	Personnel	42
Unfamiliarity with emergency procedures if an anomaly is detected	Personnel	26
Unfamiliarity with security measures	Personnel	1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 18, 24, 26, 27, 33, 34, 35, 36, 37
Unfamiliarity with the instructions for using the equipment	Personnel	28, 29
Unfavourable industrial relations	Organisation	42
Unfavourable work conditions	Personnel	38
Unfavourable work environment (rooms too small, lack of storage areas, etc.)	Physical	38
Unidentified underground equipment	Network	5
Unnecessary use of resources	Software	30
Unprotected access to rooms housing production equipment or distribution equipment for essential services	Physical	2, 3
Unprotected access to water and power supply equipment	Physical	11
Unprotected physical access to rooms housing electrical power supply and distribution equipment	Physical	12, 13
Unwanted persistence of data on media	Media	30
Use of a distribution list that includes a large part of the personnel	Software	26
Use of a non-standard system	Software	32
Use of a standard operating system on which logical attacks have already been carried out	Software	26
Use of an obsolete system	Software	32
Use of an obsolete version of the messaging server	Software	26, 31, 32, 40
Use of an obsolete version of the operating system or applications	Software	31, 32, 39, 40, 41
Use of easily-observed passwords to access the system or application (shape on keyboard, short password)	Software	18
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	Physical	21, 25
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	Physical	26
Use of non-evaluated software	Software	26
Use of shared storage space	Software	26
Use of software or developments outside the organisation's norms and standards	Personnel	32
Use of software without a guarantee of its source	Personnel	26
Use of the internal distribution list accessible to everyone	Software	30
User grant rights are not controlled.	Organisation	39
Users lack competency	Personnel	38
Users poorly trained or not trained at all	Personnel	38
Viral epidemic in the locality	Organisation	42
Water pipe close to equipment	Physical	2

Vulnerability	Asset type	Attack method
Wiring laid on the floor	Physical	2
Zone observable from a passage way	Physical	18
Zone with opening onto a public right-of-way	Physical	18

APPENDIX D: RISK CALCULATION BASED ON LIKELIHOOD OF ATTACK METHOD

1) Valuation scale for likelihood of attack method

The use of a vulnerability valuation scale representing the likelihood of attack method to exploit a vulnerability is suggested. The following five-level valuation scale may be used, which is based on EBIOS.

Valuation scale for likelihood of attack method		
	Likelihood	**Description**
1	Very Low	Totally improbable or unfeasible
2	Low	Needing very considerable means and/or a very high level of knowledge in the field concerned
3	Medium	Needing some degree of expertise and/or specific equipment
4	High	Possible using standard means and/or basic knowledge
5	Very High	Certain or possible for anyone

2) Ranking attack scenarios by measures of risk

The proposed approach is based on [BS7799-3 C.5.4] and is known as "*Ranking of incidents by measures of risk*". This method relates the factors of impact (asset value or classification) and the likelihood of an attack scenario succeeding (threats and vulnerabilities coming together to cause a particular attack, taking into account any existing or planned measures).

The practical way of doing this is to describe a specific attack scenario. In the best case, this scenario is based on the description of the threat agent (natural, human or environmental), the cause of the threat (accidental or deliberate), the attack method used by the threat agent and the security criteria (availability, integrity, confidentiality) affected.

For example, a scenario could be "Theft of media or documents containing confidential information by a visitor because the premises are easy to enter during working hours (site of the office)" or "Loss of means of telecommunication because of an accidental malfunction of external networks".

The first step for each scenario is to take the classification of the assets impacted by the scenario. This classification is defined on a scale from 1 to 5 as described in section 7 of the Guidelines on Asset Classification (column B in the table below). Similar assets may be grouped together, but the highest impact must always be recorded.

The second step is to evaluate the likelihood of the attack scenario on a predefined scale, e.g. 1 (very low likelihood) to 5 (very high likelihood) of each scenario (column C in the table below using the valuation scale of attack method given in section 1 of this appendix). This is the likelihood of the vulnerability being exploited by the attack method (as computed in section 4), possibly modified by the existing or planned security measures, taking into account their actual efficiency level (as identified in section 4.2).

If a threat involves the exploitation of several vulnerabilities, the calculation must either (1) take the lowest possibility level of the vulnerabilities if the threat can only materialise by exploiting all the vulnerabilities, or (2) take the highest possibility level of the vulnerabilities if the threat can occur by exploiting just one of the vulnerabilities.

There is no formal method to compute the likelihood but the idea is to compare the likelihood of each scenario on a scale ranging from 1 to 5.

The third step is to calculate the measure of risk by multiplying B by C. Finally the scenarios can be ranked in order of their exposure factor.

The resulting list of attack scenario can be sorted in decreasing order of measure of risk. This list is a communication tool that should receive considerable attention.

It provides the most explicit possible expression of the risk to which the information system is exposed.

Criteria (Confidentiality, Integrity or Availability)				
Scenario	**Asset value (B)**	**Likelihood of the attack scenario (C)**	**Measure of risk**	**Rank**
Scenario A	5	2	10	2
Scenario B	2	4	8	3
Scenario C	3	5	15	1
Scenario D	1	3	3	5
Scenario E	4	1	4	4

APPENDIX E: RISK CALCULATION BASED ON THREAT LIKELIHOOD AND VULNERABILITY LEVEL

1) Valuation scale for likelihood of threat occurrence

This valuation scale represents the likelihood of threat occurrence. It is suggested to use the same following five-level valuation scale as in Appendix D, as described below. The frequency of occurrence may be customised as appropriate for the system being assessed.

Valuation scale for threat occurrence likelihood		
	Likelihood	**Description**
1	Very Low	Less than 1 per 5 years
2	Low	Less than 1 per year
3	Medium	Between 1 and 4 per year (1 and 4 included)
4	High	More than 4 per year
5	Very High	More than 12 per year

2) Valuation scale for level of vulnerability to a threat

A five-level valuation scale may be used representing the level of vulnerability to a threat as shown in the table below. The percentage of vulnerability may be customised as appropriate for the system being assessed.

Valuation scale for vulnerability level		
	Level	**Description**
1	Very Low	Less than 10% or nearly impossible
2	Low	More than 10% or vulnerable with very considerable means and/or a very high level of knowledge in the field concerned
3	Medium	More than 40 % or vulnerable with some degree of expertise and/or specific equipment
4	High	More than 60 %, vulnerable using standard means and/or basic knowledge
5	Very High	More than 90% or possible for anyone

3) Risk calculation

Instead of having a single number as in Appendix D that represents the likelihood of the attack, it is possible to assess separately the threat likelihood and the level of vulnerability to a threat.

In this case the measure of risk is given by the following formula:

Risk = Threat * Vulnerability * Impact

The **Threat** figure represents the likelihood that a threat agent performs an attack to exploit a weakness of the system. For these examples it is proposed to have a scale from 1 (very low) to 5 (very high) as detailed in the table of section 1 of this annex.

The **Vulnerability** figure represents the degree of a weakness of the system, so the degree of vulnerability to be exploited by a threat. For these examples it is proposed to have a scale from 1 (very low) to 5 (very high) as detailed in the table of section 2 of this annex.

The **Impact** figure represents the level of damage caused by the exploitation of a weakness by a threat. It is proposed to rate it on a scale from 1 to 5 like in the example of annex D.

The **Risk** will then be the product of the three estimated values, as indicated in the table below (Impact in column I; threat likelihood in column T and level of vulnerability in column V). This risk value (column R) can then be used to prioritise the treatment.

Criteria (Confidentiality, Integrity or Availability)					
Scenario	**Asset value or Impact (I)**	**Threat likelihood (T)**	**Level of vulnerability (V)**	**Measure of risk (R)**	**Rank**
Scenario A	5	2	3	30	2
Scenario B	2	4	2	16	3
Scenario C	3	5	3	45	1
Scenario D	1	3	2	6	5
Scenario E	4	1	1	4	4

APPENDIX F: RISK SCENARIO REPORT

For each security criterion (confidentiality, integrity and availability) the following table should be made to summarise the results of the risk assessment. This will allow the selection of the adequate security measures.

The threat list and the vulnerability list are useful when security measures must be selected. This table is based on the approach described in Appendix D.

Criteria (Confidentiality, Integrity or Availability)				
Scenario	**Rank**	**Threat list**	**Vulnerability list**	**Measure of Risk**
Scenario C	1	T2	V10	15
Scenario A	2	T3,T25	V82	10
Scenario B	3	T5	V1,V15	8
Scenario E	4	T33	V36,V33	4
Scenario D	5	T34	V4	3