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

Brussels 02/09/2011
HR.DS5/GV/ac ARES (2011)1009585
SEC20.10.05/05 - Guidelines

European Commission

Information System Security Policy

C(2006) 3602

GUIDELINES ON ASSET CLASSIFICATION

Version 2 of 02/09/2011

TABLE OF CONTENTS

1. INTRODUCTION

This guidelines document is a complement to the "Standard on Asset Management" and describes how to actually carry out the classification of assets. After a section on general principles, tips and remarks, three classification methods are described.

The first two methods are straightforward since they rely on available information or on actual experience, while the third one is more formal and provides a step by step process. This third method has to be used if the criteria to use the other ones are not met, e.g. if the experience of the assessors is not sufficient.

2. GUIDELINES DOCUMENT OBJECTIVES

- Provide the Commission services with:
  - Consistent methods to carry out a security classification of their assets that are related to information and information systems.
  - A formal process linking the classification results and the following steps leading to the definition of the detailed security requirements.
- Ensure that all important Commission information and related assets receive the appropriate level of protection.

3. SCOPE

All assets that are related to information and information systems. A tentative list of assets associated with information systems is:

- Information assets whatever form it takes: 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 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 interface (WIFI connection devices, etc.), network interconnection devices (firewalls, gateways, proxies, etc.),

- Hardware: such as data processing equipments (transportable equipments, fixed equipments, processing peripherals, etc.), data medium (electronic medium, 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.

4. PRINCIPLES OF CLASSIFICATION

Policy objective 2.2.1: Information and related information systems must be categorised on the basis of their security needs, i.e. levels of confidentiality, integrity and availability, using a systematic process based on their value to the Commission, criticality and sensitivity. These levels, which must be periodically reviewed, allow the need for, priorities for, and degree of security protection to be determined.

4.1. Information and information related assets

All assets associated with information and information systems need to be protected in relation to the value of this information.

Classification (or assessment of security needs) is the process of establishing the business impacts for the Commission of a loss of confidentiality, integrity and availability of its information and of synthesising them in classification levels. The classification process is used to classify all physical and logical assets based on the classification of the information they are storing or processing.

- Classification is first done on **information**, regardless of the means used to store or to process them. When the information results from the aggregation of different information elements, the classification shall be performed taking into account the aggregated set of information elements. Unless it is really necessary, the classification is not done at the detailed level, like records or files, but from information type perspective.
- The classification of software and physical assets is inherited or derived from the classification of the information they are storing or processing.
- When an asset is related to two or more distinct classification levels of information, the classification of this asset must always adopt or be based on the highest classification level.
- When an asset is related to two or more distinct classification levels of information, the classification of this asset must always adopt or be based on the highest classification level.

- There are situations where the same information is held in different databases or systems but one is the master and the other is the copy. Two different examples of such a situation:

  (1) Assume that the copy is the back-up copy to be used to recover the master in case of problem. In the classification process, the confidentiality level will be the same for this information on both master and back-up copy, but the integrity and availability levels could be different for the master database/system and the copy. This requires that the copy and the master are subject to separate classification analysis at least from the integrity and availability perspectives.

  (2) Assume that the master system/database contains confidential information before its release to the copy where it is made public. The confidentiality level for the same information would be different for the two systems and maybe also the integrity and availability levels. So the classification analysis has to allow making the difference. The classification of the information on the master is time-bound or event bound and related to the release for publication.

- Sometimes information elements can have their individual confidentiality level increased when they are together by concatenation or simply being associated for business purposes. One example of this is the originator and recipient addresses of a commercial transaction in a message: the originator and the recipient addresses have no confidential level when separated, but the commercial link given by the message should not be disclosed to the competition.

- In case of interdependent applications A and B where application A is the provider application for the customer application B it can be useful to consider the mutual impacts of their respective classification levels (confidentiality, integrity and availability) in the light of the following:

  – The confidentiality level of the provider application impacts directly the confidentiality level of the customer.

  – The availability and integrity levels of the customer may respectively impact the availability and integrity levels of the provider depending on the need of the customer application to access or not the provider application each time it needs information (not only the first time) to process it.

4.2. Classification levels

As indicated in the standard, the classification levels are based on the examination of information from 3 perspectives: confidentiality, integrity and availability.

Confidentiality level:

– Obtained by assessing the extent of harm to the organisation that would result from unauthorised disclosure of the information asset.

- Four EU classified information confidentiality levels: TOP SECRET UE/EU TOP SECRET, SECRET UE, CONFIDENTIAL UE, and RESTREINT UE.
- Three Unclassified information confidentiality levels: LIMITED HIGH, LIMITED BASIC and PUBLIC.

Integrity level:

- Obtained by assessing the extent of harm to the organisation that would result from corruption or unauthorised modification of the information asset.
- Three integrity levels: MODERATE, CRITICAL and STRATEGIC. To simplify, it is possible to use the terms "Low", "Medium" and "High" respectively.

Availability level:

- Obtained by assessing the final / maximum consequences of a loss of availability of the information asset.
- Three availability categories: MODERATE, CRITICAL and STRATEGIC. To simplify, it is possible to use the terms "Low", "Medium" and "High" respectively.
- It is also possible to assess the time-criticality of the recovery mechanisms that must be applied if the information asset is unavailable, i.e. assessing the maximum period of outage of the asset that is acceptable for the business.

Security marking and designators

Moreover an additional and optional security marking can be attached for information at one of the above confidentiality levels of security (except Public level) identifying the categories of persons or bodies that are the recipients of the information or authorised to access it, like:

- Commission internal: only for use within the Commission.
- Limited: only for use within the European Institutions and Members States.
- Limited DG/Service: only for use within the nominated DG/Service.
- Personal: only to be opened by nominated person.

In addition a "security designator" approved by the Security Directorate may be added to the classification of documents, either to limit the validity of the classification, or when there is a need for limited distribution and special handling in addition to that designated by the security classification.

The approved lists of security markings and designators that may be used at the Commission are given in the "Security Notice 01: The use and application of security designators and markings". (See Security Directorate website)

4.3. Classification preparation: scope and asset analysis

Before proceeding with the classification itself, it is necessary:

- To define the scope of the asset to classify, i.e. the purpose of the asset and the stakeholders who have a vested interest in the asset and will participate in the classification.
- To analyse and understand the asset and to provide a modelling of it, depicting all its components, sub-components and their relationship. The purpose of this modelling is to identify the various information types that are related to this asset and that will eventually determine the overall classification of this asset.

We can take the example of a critical system that is quite complex and contains different types of information used by different functions/applications like for example[1] for training, payroll, holidays, timesheets, promotions or personal identification. These different types of information potentially deserve their own classification. The following steps should be done:

- The first step of the process should be the identification of all functions/applications and a description of the different types of information.
- Then the classification of information for all types and/or functions/applications should be performed; the classification process must be repeated for all of these.
- Even if an information has only one owner, the same information can be used in several functions/applications and then receive different classification levels when considered from different point of views; in this case the highest classification level must be retained.

4.4. Classification approval

Finally the results of the classification have to be signed for acceptance by the System Owner and for information by the LISO and DPO.

4.5. Classification repository

It is useful to foresee a central repository in each Commission service for the results of the classification process (i.e. the completed classifications forms) in order to be used in future assessments as examples of reasoning or as reference for similar classifications. This is not described in this document.

4.6. Information from external party or classification (partly) imposed

In case of information originated from, or owned by an external party with which the Commission has concluded a security or a service level agreement, the Commission must use the classification defined by this external party.

---

[1] Sysper2 system is a good example of such a complex system.

Similarly, if the classification of the asset is partly imposed or known the classification exercise can be faster and the effort focused on the classification parts/steps that are not yet known.

For example if we assume that we know the critical time or maximum outage acceptable for the business, the availability classification step can be avoided.

Another example is an IT service provider that gets a classification from SLAs agreed with the System Owner or that defines standardized services based on a fixed classification (e.g. a data centre hosting applications whose Integrity <= Critical, Availability<=Critical and Confidentiality <= Limited).

4.7. Classification methods

The rest of the document describes the three methods that are proposed to actually carry out the classification of information and related assets:

- Method 1: Analogy with classification already done.
- Method 2: Using overall definitions from Commission Decision C(2006) 3602 for the unclassified information and with the Commission Decision 2001/844/EC, ECSC, Euratom for the EU classified information.
- Method 3: Formal classification based on a business impact assessment process.

The two first methods are straightforward since they rely on available information or actual experience while the third one is more formal and provides a step by step process. This third method has to be used if the criteria to use the other ones are not met, e.g. if the experience of the assessors is not sufficient.

5. METHOD 1 - ANALOGY WITH CLASSIFICATION ALREADY DONE

Criteria for use: an information valuation has already been made for similar information used in a similar scope: similar stakeholders, similar boundaries and interfaces. If the scope is different, it is recommended to use method 3.

This is the simplest and quickest method.

- Look in existing sources and repositories to see whether information already classified can be used as a reference to support the new classification. For example it is very useful to look into the "comments" cells of the confidentiality, integrity and availability rating forms filled in during previous classifications done with the third method.

- Derive the classification for confidentiality, integrity and availability for the information to classify based on other classification(s) that has (have) already been done.

- Optionally, within the range of outages covered by the availability level, assess a value of the maximum duration of outage that is acceptable to the business. This is the value of the RTO (Recovery Time Objective). The RTO value is recommended to be one of the following: 4 hours, 12 hours, 1 day, 2 days, 1 week, 2 weeks or months.

- Report the resulting classification (including the security markings and/or designators as described in SN01) on a “Classification summary and approval" form (see appendix 6).

- This form must then be signed by the System Owner, the LISO and the DPO.

- Important remark: a classification that is fully imposed by external parties is eligible for this method.

- Remark on asset valuation (impact level): this first method does not directly provide the asset valuation or impact level that is necessary for the risk assessment. A risk assessment is indeed required to be done in some cases after the asset classification by the Implementing rules. Appendix 8 explains how to map impact levels onto the classifications levels defined in this method. The resulting impact levels also need to be reported in the “Classification summary and approval" form.

6. METHOD 2: USING OVERALL DEFINITIONS

Criteria for use: at least one of the people performing the evaluation (system owner, LISO, IRM, other stakeholders) has a real experience in valuation techniques: he has the abstraction abilities to identify the worst case impact potentially caused by all kinds of threat and vulnerability without taking into account any existing or potential security countermeasures. In case of doubt, it is recommended to use method 3.

6.1. Introduction

This method is based on the overall definitions given to levels in the Commission Decisions C(2006)3602 and 2001/844/CE, CECA, Euratom, further detailed in the Implementing Rules and in the Standard on Asset Management. These overall definitions are reported in the three respective tables. It is faster than the formal method but prone to less accuracy in case the assessor(s) is (are) not experienced. But it can be used in many cases.

The "Asset classification summary and approval" form (see appendix 6) must be filled in. At the end, this form must then be signed by the System Owner, the LISO and the DPO.

In case an "EU classified information" status is imposed by external parties for confidentiality for whatever reason, it has to be adopted as such and reported in the "classification summary and approval form". In this case the method will be followed to assess the classification for the non-imposed elements, usually integrity and availability.

6.2. Confidentiality classification

- Use the table below, which gives overall definitions for confidentiality classification, to assess the business consequences in the worst case of a loss of confidentiality. The first 4 categories are the "EU classified information" categories referred to as in the Decision C(2006)3602 and defined in the decision 2001/844/CE.

- Derive the confidentiality classification and report the result (including the security markings and/or designators as described in SN01) on the "Classification summary and approval" form.

CONFIDENDIALITY LEVELS	**Business consequences if unintended or unauthorised disclosure of information related to the asset:**
EU TOP SECRET / TRES SECRET UE	Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of its Member States. The compromise of assets classified EU TOP SECRET would be likely to: – Threaten directly the internal stability of the EU or one of its Member States or one of its Member States or friendly countries – Cause exceptionally grave damage to relations with friendly governments – Lead directly to widespread loss of life – Cause exceptionally grave damage to the operational effectiveness or security of Member States or other contributors' forces, or to the continuing effectiveness of extremely valuable security or intelligence operations – Cause severe long-term damage to the EU or Member States economy.
SECRET UE	Information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States. The compromise of assets classified SECRET UE would be likely to: – Raise international tensions – Seriously damage relations with friendly governments – Threaten life directly or seriously prejudice public order or individual security or liberty – Cause serious damage to the operational effectiveness or security of Member States or other contributors' forces, or to the continuing effectiveness of highly valuable security or intelligence operations – Cause substantial material damage to EU or one of its Member States financial, monetary, economic and commercial interests.
CONFIDENTIEL UE	Information and material the unauthorised disclosure of which would harm the essential interests of the European Union or of one or more of its Member States. The compromise of assets classified CONFIDENTIEL UE would be likely to: – Materially damage diplomatic relations, that is, cause formal protest or other sanctions – Prejudice individual security or liberty – Cause damage to the operational effectiveness or security of Member States or other contributors' forces, or to the effectiveness of valuable security or intelligence operations – Substantially undermine the financial viability of major organisations

	– Impede the investigation or facilitate the commission of serious crime – Work substantially against EU or Member States financial, monetary, economic and commercial interests – Seriously impede the development or operation of major EU policies – Shut down or otherwise substantially disrupt significant EU activities.
RESTREINT UE	Information and material the unauthorised disclosure of which could be disadvantageous to the interests of the EU or of one or more of its Member States. The compromise of assets classified RESTREINT UE would be likely to: – Adversely affect diplomatic relations – Cause substantial distress to individuals – Make it more difficult to maintain the operational effectiveness or security of Member States or other contributors' forces – Cause financial loss or facilitate improper gain or advantage for individuals or companies – Breach proper undertakings to maintain the confidence of information provided by third parties – Breach statutory restrictions on disclosure of information – Prejudice the investigation or facilitate the commission of crime – Disadvantage EU or Member States in commercial or policy negotiations with others – Impede the effective development or operation of EU policies – Undermine the proper management of the EU and its operations.
LIMITED BASIC/ LIMITED HIGH	Information system or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would be prejudicial to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit classification above. An additional marking may be attached for information at this level of security identifying the categories of persons or bodies that are the recipients of the information or authorised to access it. This class may apply to very large user communities (as Commission Internal Information) or to a very limited set of people (as people part of a recruitment panel). As the scope of the definition of Limited of the Decision C(2006)3602 is quite large, the LIMITED category has been broken down into 2 sub-categories which correspond to two levels of prejudice in the following way: **LIMITED BASIC** for information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause moderate prejudice to the Commission, other institutions, Member states or other parties, but not to an extent serious enough to merit EU classification. Cases would include:

	– Moderately affect political or diplomatic relations – Cause local negative publicity to the image or reputation of the Commission or other institutions – Cause embarrassment to individuals – Affect staff morale/productivity – Cause limited financial loss or, moderately facilitate improper gain or advantage for individuals or companies – Moderately affect the effective development or operation of EU policies – Moderately affect the proper management of the EU and its operations. **LIMITED HIGH** for information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause consequential prejudice to the Commission, other institutions, Member states or other parties, but not to an extent serious enough to merit EU classification. Cases would include: – Cause embarrassment to political or diplomatic relations – Cause damage to the image or reputation of the Commission or other institutions in maximum three member states – Cause distress to individuals – Cause consequential reduction in staff morale/productivity – Embarrass EU or Member States in commercial or policy negotiations with others – Cause financial loss or facilitate improper gain or advantage for individuals or companies – Affect the investigation of crime – Breach legal or contractual obligations on confidentiality of information – Affect the development or operation of EU policies – Affect the proper management of the EU and its operations.
PUBLIC	Information system or information whose public disclosure would not damage the interests of the Commission, the other Institutions, the Member States or other parties. Specifically for general release outside the EC.

6.3. Integrity classification

- Use the table below, which gives the overall definitions for integrity classification, to assess the business consequences in the worst case of a loss of integrity.

- Derive the integrity classification and report the result on the "Classification summary and approval" form.

INTEGRITY LEVELS	**Business consequences resulting from loss, corruption or unauthorised modification of information asset**
STRATEGIC	This classification shall apply to information or information systems the loss of integrity of which would be unacceptable to the Commission, to other Institutions, to Member States or to other parties because it might, for example: – Lead to the halting of the Commission's decision-making process – An adverse effect on important negotiations involving catastrophic political damage or financial losses – The undermining of the Treaties or their application.
CRITICAL	This classification shall apply to information or information systems the loss of integrity of which might threaten the position of the Commission with regard to other Institutions, Member States or other parties. Cases would include: – Damage to the image of the Commission or of other Institutions in the eyes of the Member States or the public – Very serious prejudice to legal or natural persons – Budget overrun or substantial financial losses with very serious adverse consequences for the Commission's finances.
MODERATE	This classification shall apply to information or information systems the loss of integrity of which might threaten[2] the internal working of the Commission. Cases would include: – Non-application of the Commission’s Rules of Procedure with limited or no outside impact – Threat to the achievement of the objectives of an action plan – Appearance of significant organisational and operational problems within the Commission without any outside impact

6.4. Availability classification

- Use the table below, which gives the overall definitions for availability classification, to assess the business consequences in the worst case of a loss of availability.
- Derive the availability classification.
- Optionally, within the range of outages covered by the availability level, assess a value of the maximum duration of outage that is acceptable to the business. This is the value of the RTO (Recovery Time Objective). The RTO value is recommended to be one of the following: 4 hours, 12 hours, 1 day, 2 days, 1 week, 2 weeks or months.

---

[2] At the maximum, so that "no impact" is also classified as MODERATE.

- Report the result (availability classification and optional RTO) on the "Classification summary and approval" form (see appendix 6).

AVAILABILITY LEVELS	**Final/maximum business consequences of a loss of availability of the information asset:**
STRATEGIC	This classification shall apply to information or information systems the loss of availability of which would be unacceptable to the Commission, to other Institutions, to Member States or to other parties because it might, for example: – Lead to the halting of the Commission's decision-making process – An adverse effect on important negotiations involving catastrophic political damage or financial losses – The undermining of the Treaties or their application.
CRITICAL	This classification shall apply to information or information systems the loss of availability of which might threaten the position of the Commission with regard to other Institutions, Member States or other parties. Cases would include: – Damage to the image of the Commission or of other Institutions in the eyes of the Member States or the public – Very serious prejudice to legal or natural persons – Budget overrun or substantial financial losses with very serious adverse consequences for the Commission's finances.
MODERATE	This classification shall apply to information or information systems the loss of availability of which might threaten[3] the internal working of the Commission. Cases would include: – Non-application of the Commission’s Rules of Procedure with limited or no outside impact – Threat to the achievement of the objectives of an action plan – Appearance of significant organisational and operational problems within the Commission without any outside impact

6.5. Remark on asset valuation (impact level):

This second method does not directly provide the asset valuation or impact level that is necessary for the risk assessment. A risk assessment is indeed required to be done in some cases after the asset classification by the Implementing rules. Appendix 8 explains how to map impact levels onto the classifications levels defined in this method. The resulting impacts levels also need to be reported in the “Classification summary and approval" form.

---

[3] At the maximum, so that "no impact" is also classified as MODERATE.

7. METHOD 3: FORMAL CLASSIFICATION BASED ON BUSINESS IMPACT ASSESSMENT

7.1. Principles

This method has to be used when neither of the two simple methods is satisfactory, either because the asset looks too sensitive at a first glance, or because the asset is more complex and needs more careful attention. It provides the Directorates-General with a step by step Business Impact Assessment (B.I.A.) process to identify the classification levels. It consists in determining the possible business impacts resulting from incidents for each of the confidentiality, integrity and availability categories.

The classification consists in scoring the business impact of some situations occurring based on a worst case scenario that ignores any countermeasures already in place.

- It is important to understand that the purpose of the classification is to determine the business value of an information asset and that this value is inherent to the information asset itself.
- This value does not depend at all on how the information asset is protected, but it is actually just the opposite: this value is used to decide on the level of protection and countermeasures.

So, as the classification boils down to the determination of a business value, it is a business decision pertaining to the System Owner, who must have enough knowledge and skills to take such a decision.

According to good business practices, it is recommended that a B.I.A. based classification is conducted in a workshop meeting facilitated by a staff member trained and skilled for it. This staff member could be the LISO or his representative as this will ensure consistency in classifying information assets. This meeting should gather a good representation of the stakeholders with a vested interest in this asset, but the final decision rests with the system owner.

In order to help the assessors during their classification exercises appendix 7 provides threat examples potentially leading to losses of confidentiality, integrity and/or availability. This should help them figure out possible scenarios leading to (a) security incident(s) and, hence, be convinced of the likelihood of security breaches impacting information assets.

7.2. Classification tools

7.2.1. Rating levels

The confidentiality, integrity and availability ratings are worst case ratings of the business impact or damage resulting from situations causing loss of them. The following ratings or impact levels will be used to measure this impact.

Rating/Impact level	**Significance**
1	Low (negligible or no damage)
2	Medium (moderate damage)
3	High (consequential damage)
4	Very High (significant damage)
5	Major (from serious to exceptionally grave damage)

7.2.2. Classification forms

Seven forms are available to perform and support the classification process. These forms are described in the following sections and given in the appendices: A copy of the Excel file is embedded in appendix 1 containing most of these forms.

- Business impacts definition table (appendix 1)
- Business impact levels reference table (appendix 2)
- Confidentiality rating and classification form (appendix 3)
- Integrity rating and classification form (appendix 4)
- Availability rating and classification form (appendix 5)
- Classification summary and approval form (appendix 6)
- Example of threats scenarios (appendix 7)

7.2.3. Business impacts definition table

The Business impacts definition table has to be used by the classification exercise participants to help in **identifying business impacts relevant to the Commission.** The business impact types are related to the business of the Commission and their categories are mapped on the Risk management framework published by the DG BUDG.

The Business impacts definition table, which is given in appendix 1, contains 2 columns.

The first column defines 15 types of business impacts grouped in the following 4 main categories:

- External environment, which contains 5 impact types (e.g. Damage to Commission's partner)
- Planning, Process and systems, which contains 5 impact types (e.g. Unforeseen costs)
- People related, which contains 3 impact types (e.g. Damage staff morale/productivity, abuse of personal data)

- Legality and regularity aspects, which contains 2 impact types (Penalties and legal liabilities)

For each business impact type listed in the first column, the second column provides examples of business impacts identified as relevant and/or specific to the Commission. This gives an indication on the kind of impacts that are expected in the related category. It is important to know that they are business impacts examples and that the list of examples does not pretend to be exhaustive. During a classification exercise other business impacts that are not in the list for a particular impact type are likely to be identified.

The overall structure of the documents described in the following sections is exactly the same as the Business impacts definition table and mapped on the contents of the first column. In a nutshell they are based on the same business impact types and main categories.

7.2.4. Business impact levels reference table

The Business impact levels reference table has to be used to **help determine the ratings during the assessment of the confidentiality, integrity and availability impact values**. The Business impacts levels reference table, which is given in appendix 2, contains 7 columns.

The first column is the same as the first column of the Business impacts definition table and provides the 15 impact types grouped in the same four categories.

For each impact type of the first column, the second column, which is named "evaluation criteria", provides recommended or proposed measurement types for the rating. For example the Impact type "Damage to commission's partner" can be assessed in two ways:

- either qualitatively by the "extent of damage",
- or quantitatively by the estimation of the financial impact proposed as a percentage of a budget. This budget can be the total budget of a particular DG or DG’s programme. This total budget will be determined during the classification.
- the choice between the two depends on the specific business impact that is identified and the information available about it.

For each business impact type of the first column and the evaluation criteria of the second column, the five following columns provide a value or range of values for each impact levels 1 to 5. The proposed value is quantitative or qualitative depending on the measure. Considering the same example "Damage to commission's partner", if the impact identified by the system owner is "Damage the continuing effectiveness of security or intelligence operations" and his qualitative assessment of the damage is "Significant", the table proposes a rating or impact level of 4.

7.2.5. Customization of the business impact levels reference table:

Due to the differences in business and budget in different DG's and programmes within DG's, a same cause can have very different levels of business impact. So it is maybe useful to adapt the Business impact levels reference table to the reality of the DG and /or programme.

It is recommended to do this customization carefully in order to keep the essence of this method. So, before using the customized table for actual rating in a DG or a programme within a DG, it should be formally approved by the DG director general or the programme responsible after consulting HR.DS.

The percentages of total budget or range of percentages given can be different from DG to DG, and within a DG from programme to programme. The percentages given in the table are proposals that can be customised. It is then advised to review the reference table DG-wise or programme-wise and to get an agreement on the percentages that have to be used consistently for the classification exercises in the particular DG or programme.

Another way to customize the financial impact is to replace the percentage by the calculated values using the actual budget to be considered. For example if the total budget of 1000 million Euros for a programme is used, the impact level 2 (medium) will be from 100 KEuros to 1 million Euros.

Similarly, this reference table could also be customised in the "extent of delay" measurement criteria for the "degraded service" and "impaired political decision/execution" impact types.

7.3. Classification steps

7.3.1. Classification steps overview

After the classification preparation phase (see section 5.3) consisting in analysing the asset and identifying various stakeholders the classification participants need to be provided with the information and documentation necessary to understand the process.

The classification itself consists in the following steps:

- Confidentiality rating and classification: assessment of the business impact and resulting confidentiality classification using the confidentiality rating and classification form (appendix 3).

- Integrity rating and classification: assessment of the business impact and resulting integrity classification using the integrity rating and classification form (appendix 4).

- Availability rating and classification: assessment of the business and resulting availability classification impact using the availability rating and classification form (appendix 5).

- Summary and approval of the ratings and classification: reporting the above ratings and classifications on the Classification summary and approval form (appendix 6) and sign them off.

These steps are described in the following sections together with, and using the various forms provided in the appendices.

7.3.2. Step 1: Confidentiality rating and classification

Confidentiality rating (impacts)

The confidentiality rating is the assessment of the business **impact** of a loss of confidentiality for each of the business impact types. This will be done by filling in a blank Confidentiality rating and classification form given in appendix 3 with the support of the two tables described above: the Business impacts definition table and the Business impact levels reference table.

The first column of the confidentiality rating and classification form contains the same impact types grouped into the same four categories as the first column of the Business impacts definition table. The additional rows that are below the "summary of ratings" heading are dedicated to the summary of ratings and the mapping to the resulting confidentiality level.

The following five columns are dedicated to get the rating corresponding to the business impact type of the first column.

It consists in providing a rating for the business consequences (worst case) of unintended or unauthorised disclosure of information for each of the Business impact types corresponding to a row in the table unless the impact type is not relevant for the asset being classified. This means that, for <u>all rows</u> of the table corresponding to an impact type relevant to the asset, <u>one cell</u> corresponding to an impact level value must be ticked. If the impact type is not relevant, the corresponding row will be left blank.

For example consider that we are figuring out if the unintended or unauthorized disclosure of information X could have a business consequence of the type "Damage to Commission's partner":

- We look into the Business impacts definition table and we try to figure out if any of the examples given for this type is or are relevant.
- After discussing various scenarios in their worst case, we realise that the most serious damage in this example would be "Damage member states financial, monetary and commercial interests".
- Then we use the Business impact levels reference table at the same row "Damage to Commission's partner" and look if we can assess the impact with numbers (financial impact) or only with qualifiers (extent of damage). We agree that it is possible to assess with numbers.
- So we proceed with the assessment and we get to the agreement (from key stakeholders) that the most likely impact value if we consider the worst

case would be in the region of 4% of the total budget considered for this classification. We see that it corresponds to a level of 4 or Very High.

- Finally we report this rating by ticking the cell which is at the intersection of the row "Damage to Commission's partner" and the column 4 or Very High.

The last column named "comments" can be used to refer to the reasoning behind the rating of the same row. If there is not enough room in the cell, it could be a number referencing a longer explanation in a companion document. It is strongly recommended to document the reasons for the ratings, especially for 4 and 5 ratings. Such reasoning is very useful during future classifications using whatever method and more specifically method 1.

Finally when all the impact types relevant for the asset being classified have been considered and all the ratings reported it is time to summarize the confidentiality rating in the row below summary of ratings. As the summary has to indicate the **highest damage** assessed in the rows above, we just need to tick the cell that corresponds to the highest rating in the rows above. This is the quickest way of proceeding.

However, in some rare cases there is some hesitation between two ratings in the summary due to the spread of the ratings above or because there is no clear agreement on the highest rating in the rows above. Then the System Owner has the final decision and could perfectly decide on the rating just below the highest rating in the rows above. The comment cell beside can be used to document this final decision.

Determination of the confidentiality classification

This actual classification has to be derived directly from the summary of ratings defined just above and using the row "Mapping from ratings to classification levels" in the following way:

- If the summary of ratings is 1, the mapping gives Public
- If the summary of ratings is 2, the mapping gives LIMITED BASIC
- If the summary of ratings is 3, the mapping gives LIMITED HIGH.
- If the summary of ratings is 4, the mapping gives RESTREINT UE.
- If the summary of ratings is 5, the mapping allows choosing between CONFIDENTIAL UE, SECRET UE or TRES SECRET UE. The participants of the classification exercise have to reach a consensus on which one of the three to choose based on the nature and usage of the assets (paper or information). In case of disagreement the system owner has the final word on the choice.

Then the final classification can be reported in the last row by erasing the classification levels that have not been chosen.

7.3.3. Step 2: Integrity rating and classification

Integrity rating (impacts)

The integrity rating is the assessment of the Business **impact** resulting from loss, corruption or unauthorised modification of information asset for each of the business impact types. This will be done by filling in a blank Integrity rating and classification form given in appendix 4 with the support of the two tables described above: the Business impacts definition table and the Business impact levels reference table.

The first column of the integrity rating and classification form contains the same impact types grouped into the same four categories as the first column of the Business impacts definition table. The additional rows that are below the "Summary of ratings" heading are dedicated to the summary of ratings and the mapping to the resulting integrity level.

The following five columns are dedicated to get the ratings corresponding to the business impact type of the first column.

It consists in providing a rating for the business consequences (worst case) of accidental or unauthorised corruption of information for each of the Business impact types corresponding to a row in the table unless the impact type is not relevant for the asset being classified. This means that, for all rows of the table corresponding to an impact type relevant to the asset, one cell corresponding to an impact level value must be ticked. If the impact type is not relevant, the corresponding row will be left blank.

For example consider that we are figuring out if errors in, or deliberate manipulation of information X could have a business impact of the type "Loss of management control":

- We look into the Business impacts definition table and we try to figure out if any of the examples given for this type is or are relevant.
- After discussing various scenarios in their worst case, we realise that the most serious damage in this example would be "Impaired decision making".
- Then we use the Business impact levels reference table at the same row "Loss of management control" and look if we can assess the impact with numbers (financial impact) or only with qualifiers (extent of problem). We decide that it is possible to assess with qualifiers.
- So we proceed with the assessment and we get to the agreement (from key stakeholders) that the most likely impact value if we consider the worst case would be "Impede important executions" (significant). We see that it corresponds to a level of 4 or Very High.
- Finally we report this rating by ticking the cell which is the intersection of the row "Loss of management control" and the column 4 or Very High.

The last column named "comments" can be used to refer to the reasoning behind the rating of the same row. If there is not enough room in the cell, it could be a number referencing a longer explanation in a companion document. It is strongly recommended to document the reasons for the ratings, especially for 4 and 5 ratings. Such reasoning is very useful during future classifications using whatever method and more specifically method 1.

Finally, when all the impact types have been considered and all the ratings reported, it is time to summarize the integrity rating in the row below the summary of ratings. As the summary has to indicate the **highest damage** assessed in the rows above, we just need to tick the cell that corresponds to the highest rating in the rows above. This is the quickest way of proceeding.

However, in some rare cases there is some hesitation between two ratings in the summary due to the spread of the ratings above or because there is no clear agreement on the highest rating in the rows above. Then the System Owner has the final decision and could perfectly decide on the rating just below the highest rating in the rows above. The comment cell beside can be used to document this final decision.

Determination of the integrity classification

This actual classification has to be derived directly from the summary of ratings defined just above and using the row "Mapping from ratings to classification levels" in the following way:

- If the summary of ratings is 1 or 2, the mapping gives Moderate
- If the summary of ratings is 3 or 4, the mapping gives Critical
- If the summary of ratings is 5, the mapping gives Strategic

Then the final classification can be reported in the last row by erasing the classification levels that have not been chosen.

7.3.4. Step 3: Availability rating and classification

Availability rating (impacts)

The availability rating is the assessment of the business **impact** of a specific outage of the system and loss of availability of information for each of business impact types. This will be done by filling in a blank Availability rating and classification form given in appendix 5 with the support of the two tables described above: the Business impacts definition table and the Business impact levels reference table.

The first column of the availability rating and classification table contains the same impact types grouped into the same four categories as the first column of the Business impacts definition table. There are four additional rows described further in the section:

- The first one dedicated to the summary of ratings for each column.
- The second one is dedicated to the maximum rating of all columns.
- The third one is used to derive the resulting availability classification.
- The fourth one is an optional line dedicated to the overall assessment of the RTO (Recovery Time Objective).

The following five columns are dedicated to get the ratings corresponding to the business impact type of the first column.

It consists in providing a rating of the business consequences (worst case) of the information or related assets being unavailable for each of the Business impact types corresponding to a row in the table unless the impact type for the asset being classified is not relevant and for each of the different duration of outage/unavailability (4 hours, 12 hours, 2 days, 1 week, 2 weeks) in the row:

- This means that you have to write a number (impact level value) between 1 and 5 in <u>each cell of a row</u> corresponding to an impact type, unless the impact type is not relevant for this classification.
- The impact level value will increase with the duration of outage from left to right in the table.
- So this means that only the value 1 can be found to the left of a cell where level value 1 is identified and the value 5 to the right of a cell where level 5 is identified.

For example consider that we are figuring out if a prolonged outage of the system Y with information X could have a business consequence of the type "Damage to image or reputation":

- We look into the Business impacts definition table and we try to figure out if any of the examples given for this type is or are relevant to this situation.
- After discussing various scenarios in their worst case, we realise that the most serious damage in this example would be "Damage to reputation".
- Then we use the Business impact levels reference table at the same row "Damage to image or reputation " and look if we can assess the impact with numbers (financial impact) or only with qualifiers (extent of negative publicity). We decide that it is possible to assess with qualifiers.
- So we proceed with the assessment for each duration of outage and we get to the agreement that the most likely impact value if we consider the worst case would be the following for each duration of outage:
    - 4 hours: the impact is assessed as "negligible", which corresponds to a level of 1 or Low.

  - 12 hours: the impact is assessed as "local negative publicity", which corresponds to a level of 2 or Medium.
  - 2 days: the impact is still assessed as "local negative publicity", which corresponds to a level of 2 or Medium.
  - 1 week: the impact is assessed as "Consequential", which corresponds to a level of 3 or High.
  - 2 weeks: the impact is assessed as "Significant", which corresponds to a level of 4 or Very High.
- Finally we report these ratings by writing the values into the cells that are at the intersection of the row "Damage to image or reputation" and respectively each of the column 4 hours, 12 hours, 2 days, 1 week and 2 weeks. This will give in our example: 1 for 4 hours, 2 for 12 hours, 2 for 2 days, 3 for 1 week and 4 for 2 weeks.

The main difference with the ratings for confidentiality and integrity is that we have to give a rating for each cell in a row corresponding to an impact type relevant for this classification.

The last column named "Comments" can be used to refer to the reasoning behind the ratings of the same row. If there is not enough room in the cell, it could be a number referencing a longer explanation in a companion document. It is strongly recommended to document the reasons for the ratings, especially for 4 and 5 ratings. Such reasoning is very useful during future classifications using whatever method and more specifically method 1.

When all the impact types have been considered and all the ratings reported it is time to summarize the availability ratings in the row identified by "The summary of ratings for each column would…"

- There is the same difference as above compared to the confidentiality and integrity ratings. All the cells of the summary row must be filled in. We need to proceed column by column.
- As the summary has to indicate the highest damage assessed in the rows above, we just need to report in a cell of the summary of rating row the highest rating in all the cells of the column above.
- In our example, we assume to have filled in all the lines and by following the instructions just above we assume that we get the following sequence of values from left to right: 1, 2, 2, 3 and 4 respectively for outages of 4 hours, 12 hours, 2 days, 1 week and 2 weeks.

Then, it is possible to fill in the row "Maximum rating for all columns" with the highest rating of the ratings just filled in the row above. . Normally it is the rating under the last column (2 weeks). In our example this would give a maximum rating of "4".

Finally it is possible to derive the Resulting Availability classification from the maximum rating as indicated in the "Legend for resulting availability":

- Moderate if the maximum rating is 1 or 2.
- Critical if the maximum rating is 3 or 4.
- Strategic if the maximum rating is 5.

In our example, the resulting availability classification would be "critical".

Optional - Assessment of Recovery Time Objective

Optionally, it is possible to assess of the Recovery Time Objective for recovering the information and hence related assets, i.e. the timescale beyond which an outage of the information and related assets is unacceptable to the business. It is recommended to proceed as follows:

- The System Owner (or designated owner of the asset) has first to define the level of harm that is unacceptable for the business: in our example he considers that the level of harm that is unacceptable for the business is "Significant or limited to 5 EU countries ".

- Then the identified "level of harm that is unacceptable for the business" has to be mapped to its corresponding impact level in the table of appendix 2 (Business impact levels reference table level 1 to 5). In our example this unacceptable level of harm "Significant or limited to 5 EU countries" corresponds to impact level 4 or "Very High" in the Business Impact Reference Table.

- Then, the Summary of ratings that has just been established in the Availability rating form has to be analysed to identify in which column (duration of outage) the value of impact becomes equal to the identified impact level that is unacceptable to the business; in our example (sequence of values from left to right: 1, 2, 2, 3 and 4 respectively for outages of 4 hours, 12 hours, 2 days, 1 week and 2 weeks), the impact level 4 identifies the duration of outage that corresponds to that level of unacceptable harm and, hence, the duration when the impact level becomes 4 is 2 weeks.

- The recovery time objective (RTO) that corresponds to the level of outage unacceptable for the business has to be lower than, or equal to the duration of outage identified above as when the impact level becomes equal to the unacceptable to the business; in our example 2 weeks is the duration of outage when the impact level becomes 4, so that the stakeholders have to choose an RTO that is lower than, or equal to 2 weeks.

- In the light of the information above, the various participants have to agree on an RTO value that is recommended to be one of the following: 4 hours, 12 hours, 1 day, 2 days, 1 week, 2 weeks or months; in our example the participants get to the agreement endorsed by the system owner that the RTO is 2 weeks.

7.3.5. Step 4: Summary and approval of the ratings and classification

Classification summary and approval form

Report the summary ratings and classification for confidentiality, integrity and availability determined in the three preceding sections on a blank "Classification summary and approval form" given in annex 6, as described in the following sections.

Confidentiality results:

- In the Confidentiality table under the "Resulting security classification" heading, report the confidentiality classification level that has been defined in the last row of the "Confidentiality rating and classification form": delete the non-chosen classification levels in the text string "Public/ LIMITED BASIC/LIMITED HIGH/RESTREINT UE/CONFIDENTIEL UE/SECRET UE/TRES SECRET UE" pre-written in the cell.
- If required by the participants and approved by the System owner, add the marking and/or security designator in the same box.
- In the second row, report the summary of ratings that has also been defined in the last row of the "Confidentiality rating and classification from": this can be done by highlighting the defined rating value in one of the five boxes or deleting the useless ones.

Integrity results:

- In the Integrity table under the "Resulting security classification" heading, report the integrity classification level that was defined in the last row of the "Integrity rating and classification form": delete the non-chosen classification levels in the text string "Moderate/Critical/Strategic" pre-written in the cell.
- In the second row, report the summary of ratings that has also been defined in the last row of the "Integrity rating and classification form": this can be done by highlighting the defined rating value in one of the five boxes or deleting the useless ones.

Availability results and Recovery Time Objective:

- In the availability table under the "Resulting security classification" heading, report the availability classification level that has been defined in the row "Resulting Availability classification" of the "Availability rating and classification form": delete the non-chosen classifications levels in the text string "Moderate/ Critical/ Strategic" pre-written in the cell of the first row.

- In the second row report the Recovery Time Objective that has been defined in the same "Availability rating and classification form".
- In the last box of the table, report the summary of ratings that has also been defined in the "Summary of rating for each column…" of the "availability rating and classification form". This can be done by highlighting the defined rating values in one of the five boxes or deleting the useless ones. This has to be done for each of duration of outage (4 hours, 12 hours, 2 days, 1 week, and 2 weeks).

Approval of the results

The box in upper part of the form has to be filled in with the description of the asset resulting from the classification preparation and analysis of the asset (see section 5.4). This box has also to be filled in with the asset location, the service provider hosting the asset (e.g. DG, DG DIGIT or external provider) and the names of the System Owner, the LISO and the DPO.

The System Owner has to sign-off the classification results in the lower part of the sheet. The LISO and the DPO need to sign for information.

8. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006.

Implementing rules of Commission Decision C(2006) 3602

International standard ISO/IEC 27001

International standard ISO/IEC 27002

Framework for Business Continuity Management in the Commission {Sec(2006) 898 and 899}

Security Notice 01: The use and application of security designators and markings (See Security Directorate website)

Towards an effective and coherent risk management in the Commission services SEC(2005)1327

Decision 2001/844/EC, CECA, Euratom 29/11/2001

9. SUPPORTING STANDARDS AND GUIDELINES

Standard on asset management

Standard on risk management

10. APPENDIX 1: BUSINESS IMPACTS DEFINITION TABLE

Business impacts definition table	
Business impact types	**Examples of types of business impacts**
External environment	
Damage to political relations	Intervention at political level (Council, Parliament) about EC's performance Problems in diplomatic relations Problems with friendly / unfriendly government
Impaired political decision/execution	Political decisions and priorities delayed or not taken Aid, subsidies, grants, programs delayed, not executed or missed
Damage to Commission's partner	Damage to Commission partner (member states companies, citizens, contractors, consultants) Damage the operational effectiveness or security of Members states or other contributors force Damage the continuing effectiveness of security or intelligence operations Damage member states financial, monetary and commercial interests Damage the financial viability of major organisations
Damage to image or reputation	Damage to reputation (eg due to disclosure of confidential information, compromised info, info not available) Damage to image (due to disclosure of confidential information, compromised info, info not available)
Damage to public order	Cause protest, demonstration or prejudice public, locally or more widespread due to delayed or not executed EC decisions or policies
Planning, processes and systems	
Impaired management control	Impaired decision making Jeopardise the realisation of major policy objectives Impede the development or operation of major EU policies Cause problems on important negotiations involving political damage or financial losses Process management failure Implementation of policies affected by non-reliability of available information Implementation of policies affected by delays in receiving the data
Degraded service	Degraded service provided (for internal customers or external partners) Cause problems to EU management, activities or operations Delayed deliveries (project)
Unforeseen or additional costs	Recovery costs, uninsured losses, increased insurance, Cost to detect the cause of the harm and to repair it
Loss of tangible assets	Material loss or theft Fraud, theft of money, lost interest Loss of EU funds caused by fraud
Budget overrun	Could also lead to Intervention at political level (Council, Parliament) about EC's performance
People related	
Health and safety	Injury or loss of life of staff, suppliers, contractors and others employed by the EC (directly or indirectly)
Damage staff morale/productivity	Distress (=anger, frustration, disappointment, embarrassment or concern) Prejudice individual security or liberty Reduction in staff morale/productivity (reduce efficiency, lost time, job losses)
Abuse of personal data	Prejudice security, liberty, finances or fair treatment due to unauthorised disclosure, unlawful processing or transfer to third country with inadequate level of data protection.
Legality and regularity aspects	
Impede law/rules enforcement	Facilitating commission of a crime, prejudice the investigation of a crime Impede the procedure of selection, fair assessment of readiness of candidates or fair evaluation of experts,
Legal liability and penalties	Civil suit or criminal offence resulting in damage/penalty Result in the infringement of laws, regulations and contractual obligations Claims against the commission due to disclosure of confidential information

Table 1: Integrity rating and classification form; Excel file available in appendix 9

11. APPENDIX 2: BUSINESS IMPACT LEVELS REFERENCE TABLE

BUSINESS IMPACT LEVELS REFERENCE TABLE						
Business impact types	**Evaluation criteria**	**Impact levels**				
		1 Low	**2 Medium**	**3 High**	**4 Very High**	**5 Major**
External environment						
Damage to political relations	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave; raise tension or formal protest
Impaired political decision/execution	Extent of delay (time) or	One week or negligible delay	One month or moderate delay	Three to five months or consequential delay	Six months or significant delay	From one year or serious delay to exceptionally grave delay, or abandoned execution
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
Damage to Commission's partner	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
Damage to image or reputation	Extent of negative publicity	Negligible or no damage	Moderate/ local negative publicity	Consequential or limited to 3 EU countries	Significant or limited to 5 EU countries	More than serious, Europe wide or worldwide negative publ.
Damage to public order	Extent of damage	Negligible or no protest	Limited or very localised protest	Consequential, region wide protest, lightly injured people	Demonstrations national effects or injured people	Threaten stability, widespread effects/ individual or loss of life
Planning, processes and systems						
Impaired management control	Extent of problem	Negligible or no damage	Moderate	Consequential, affect executions	Significant or impede important executions	From serious to exceptionally grave, or from disrupt to abort critical execution(s)
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
Degraded service	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave
	Extent of delay (% of total expected time)	One day or negligible delay (1%)	One week or moderate delay (<10%)	One month or consequential delay (<25%)	Two months or significant delay (<50%)	More than one year or serious delay (>50%) or abort project/delivery
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
Unforeseen or additional costs	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
Loss of tangible assets	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
Budget overrun	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave
People related						
Health and safety	Number of incidents & extent of harm	No injuries	Minor injury(ies)	More than minor injury(ies)	Life of individual(s) threatened	From death of one individual to widespread loss of life
Damage staff morale/productivity	Extent of loss of morale	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to complete loss
Abuse of personal data	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave
Legality and regularity aspects						
Impede law/rules enforcement	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave
Legal liability and penalties	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 2%	2% to 5%	More than 5%
	Extent of damage	Negligible or no damage	Moderate	Consequential	Significant, adversely affect	From serious to exceptionally grave

Table 2: Business impact levels reference table; Excel file available in appendix 9

12. APPENDIX 3: CONFIDENTIALITY RATING AND CLASSIFICATION FORM

Business Impact Assessment						
CONFIDENTIALITY RATING AND CLASSIFICATION						
Business impact types	**Business impact levels**					**Comments**
Business consequences of unintended or unauthorized **disclosure** of information (worst case)	**1** Low	**2** Medium	**3** High	**4** Very High	**5** Major	
External environment						
Damage to political relations						
Impaired political decision/execution						
Damage to Commission's partner						
Damage to image or reputation						
Damage to public order						
Planning, processes and systems						
Impaired management control						
Degraded service						
Unforeseen or additional costs						
Loss of tangible assets						
Budget overrun						
People related						
Health and safety						
Damage staff morale/productivity						
Abuse of personal data						
Legality and regularity aspects						
Impede law/rules enforcement						
Legal liability and penalties						
Summary of ratings	**1**	**2**	**3**	**4**	**5**	
The summary of rating would normally be at least as high as the highest rating assessed above						
Mapping from ratings to classification levels	Public	Limited Basic	Limited High	Restreint	Confidentiel or Secret Tres Secret	
Resulting Confidentiality classification	**Public / Limited Basic/ Limited High / RESTREINT UE / CONFIDENTIEL UE/ SECRET UE / TRES SECRET UE**					

Table 3: Confidentiality rating and classification table; Excel file available in appendix 9

13. Appendix 4: Integrity rating and classification form

Business Impact Assessment						
INTEGRITY RATING AND CLASSIFICATION						
Business impact types	**Business impact levels**					**Comments**
Business consequences of errors in information or of deliberate manipulation of information to perpetrate or conceal a fraud (worst case)	**1** Low	**2** Medium	**3** High	**4** Very High	**5** Major	
External environment						
Damage to political relations						
Impaired political decision/execution						
Damage to Commission's partner						
Damage to image or reputation						
Damage to public order						
Planning, processes and systems						
Impaired management control						
Degraded service						
Unforeseen or additional costs						
Loss of tangible assets						
Budget overrun						
People related						
Health and safety						
Damage staff morale/productivity						
Abuse of personal data						
Legality and regularity aspects						
Impede law/rules enforcement						
Legal liability and penalties						
Summary of ratings	**1**	**2**	**3**	**4**	**5**	
The summary of rating would normally be at least as high as the highest rating assessed above						
Mapping from ratings to integrity levels	Moderate	Moderate	Critical	Critical	Strategic	
Resulting Integrity classification	**Moderate / Critical / Strategic**					

Table 4: Integrity rating and classification table; Excel file available in appendix 9

14. APPENDIX 5: AVAILABILITY RATING AND CLASSIFICATION FORM

Business Impact Assessment						
AVAILABILITY RATING AND CLASSIFICATION						
Business impact types Business consequences of a prolonged outage of the system (worst case)	**Business impact levels**					**Comments**
	1=low, 2=medium, 3=high, 4= very high, 5=major					
	Duration of outage					
	4 hours	**12 hours**	**2 days**	**1 week**	**2 weeks**	
External environment						
Damage to political relations						
Impaired political decision/execution						
Damage to Commission's partner						
Damage to image or reputation						
Damage to public order						
Planning, processes and systems						
Impaired management control						
Degraded service						
Unforeseen or additional costs						
Loss of tangible assets						
Budget overrun						
People related						
Health and safety						
Damage staff morale/productivity						
Abuse of personal data						
Legality and regularity aspects						
Impede law/rules enforcement						
Legal liability and penalties						
Summary of ratings	**4 hours**	**12 hours**	**2 days**	**1 week**	**2 weeks**	
The summary of rating for each column would normally be at least as high as the highest rating assessed in the column above						
Maximum rating of all columns	**1 / 2 / 3 / 4 / 5**					Legend for resulting availability Moderate if maximum rating is 1 or 2
Resulting Availability classification	**Moderate / Critical / Strategic**					Critical if maximum rating is 3 or 4 Strategic is maximum rating is 5
Assessment of Recovery Time Objective (Optional)	**RTO =**			Timescale beyond which the system outage is unacceptable for the business of the EC or to an EC function it supports?		

Table 5: Availability rating and classification table; Excel file available in appendix 9

15. APPENDIX 6: CLASSIFICATION SUMMARY AND APPROVAL FORM

Classification summary and approval form

Description of the asset:	
Asset location	
Service provider name	
System Owner name:	
LISO name:	
DPO name:	

RESULTING SECURITY CLASSIFICATION

CONFIDENTIALITY:

Classification	**Public/ LIMITED BASIC/ LIMITED HIGH/ RESTREINT UE/ CONFIDENTIEL UE/ SECRET UE/ TRES SECRET UE**				
BIA Rating (optional)	1	2	3	4	5

INTEGRITY:

Classification	**Moderate/Critical/Strategic**				
BIA Rating (optional)	1	2	3	4	5

AVAILABILITY:

Classification	**Moderate/Critical/Strategic**
RTO (Optional)	

BIA Rating (optional)					
4 hours	1	2	3	4	5
12 hours	1	2	3	4	5
2 days	1	2	3	4	5
1 week	1	2	3	4	5
2 weeks	1	2	3	4	5

I agree with and approve the business impact analysis ratings for confidentiality, integrity and availability and their resulting security classifications			
Signature of the System Owner:		Date:	
I agree to have been informed of, and understand the business impact analysis ratings for confidentiality, integrity and availability and their resulting security classifications			
Signature of the LISO:		Date:	
Signature of the DPO:		Date:	

Table 6: Classification summary and approval form; Excel file available in appendix 9

16. APPENDIX 7: EXAMPLES OF THREAT SCENARIOS

16.1. Introduction to this appendix

The third classification method is based on a business impact assessment of a loss of classification, integrity and availability subsequent to an incident. This impact is considered in the worst case and without considering any countermeasures.

In order to help the assessors during their classification exercises this appendix provides threat examples that could lead to one or all of theses losses. This should help them figure out possible scenarios leading to (a) security incident(s).

Each of the next sections is dedicated to threat examples leading to one type of incident. For example the next section is dedicated to threat examples potentially leading to loss of confidentiality.

But it is important to understand that a single threat could lead to more than one type of security incident. For example a single threat could lead to loss of both confidentiality and integrity and, then, this threat example is described both in the section on confidentiality and in the section on integrity.

16.2. Threat scenarios targeting confidentiality

- **Disclosure of information:** release of information of a confidential or sensitive nature to people to whom it should not be released.
    - This disclosure could be accidental or intentional. Intentional could be perpetrated by people masquerading the legitimate user, by brute force, theft or any other cause.
    - The disclosure could be either unauthorised or premature. Some information is sensitive before some date and, if prematurely disclosed, can have a negative impact on the image of the EC or a specific EC Service.
    - The disclosure could be to insiders (e.g. EC staff or equivalent) or outsiders (e.g. public, or people external to a DG, programme or project) or to service providers (e.g. CSP). Depending on the information, the impact will be different depending on whether the information is disclosed to insiders or outsiders (disclosure to outsiders is usually more serious).
- **Threats potentially causing disclosure**
    - Unauthorised use of an application or systems in order to get sensitive information. Use of unauthorised software the functionality of which has not been tested or is not known with potential impact on the confidentiality of information.
    - Communication interception or manipulation in order to get information of a confidential nature.

  - Communication interception in order to monitor the traffic, e.g. to know destination of information which could be confidential information

  - External attacks to hack into systems or unauthorized access or intrusion into system or network using a computer device, software tools or malicious code in order to get information.

  - Accidental mis-routing of information to people not entitled to see it.

  - System, network or application failure allowing information to be disclosed to people not entitled to see it. For example software bug or system failure leading to incorrect running of the application.

  - Errors by operators or users that allow information to be disclosed: mis-configuration, passwords disclosed, bad passwords that can be easily guessed, insufficient user awareness of the information classification being dealt with, unattended workstations.

  - Staff shortage leading to excessive need for outside contractors that have not been screened carefully enough.

  - Theft of computers equipment containing sensitive information (e.g. laptops, PC components, PDAs).

  - Errors during hardware or software maintenance leading to unauthorised access to sensitive information.

  - Embedding of malicious code, or changing existing code in order to get confidential information

16.3. Threat scenarios targeting integrity

- **Loss of integrity:** any accidental or deliberate alteration of information or software that prevents the system or service of providing the intended service with the correct information and with the intended security.

- **Threats potentially causing loss of integrity**

  - Alteration of data: intentional modification, insertion or deletion of data, whether by authorised users or not, that compromises the integrity of information produced, processed, controlled or stored by the information processing systems.

  - Alteration of software: intentional modification, insertion or deletion of operating system or application system programs, whether by an authorised user or not, that compromises the integrity of information, programs, the system or resources controlled by the computer systems.

  - Vandalism: malicious and motiveless defacement of property. For example hack into a web site to change the front page.

  - Fraud: a deliberate unauthorised manipulation of hardware, software or information with the intent of financial gain.

  - Communications manipulation in order to modify the data in transit, e.g. payload, routing information, signatures, originator information, security information, control information. Another possibility is the insertion of false messages.

  - Software errors or system, network or application failure: any extraneous or erroneous data in the operating system or applications programs resulting in processing errors or data output errors; improper editing routines for data entry functions or for external feeds; software bug. Programs errors are considered large scale errors compared to the typing errors that are small scale errors.

  - Accidental mis-routing of messages or information.

  - Errors during hardware or software maintenance causing inappropriate alteration of data, configuration data, software or hardware. It could happen if lack of appropriate change control process (including testing) or if lack of appropriate version control process.

  - Replay of transactions or messages for example leading to duplication of payments or orders.

  - Staff shortage leading to excessive need for outsiders with a lack of awareness or competences (hence prone to errors of many types). This can also cause overloaded staff also prone to more errors.

  - Insertion or embedding of malicious code leading to loss of integrity of data, software, storage or databases.

  - External attacks to hack into systems or unauthorized access or intrusion into system or network using a computer device, software tools of malicious code in order to modify/delete information, access rights or other security information.

  - Technical failure of network distribution, network management service host, network interfaces or network services causing non-delivery or alteration of information or software.

  - Repudiation: alteration of originator or recipient that allows dishonestly claiming repudiation of origin or reception respectively.

16.4. Threat scenarios targeting availability

- **Loss of availability:** disruption of services, systems or operations such that authorised users or operators cannot access applications, information and systems. It is possible to have a complete destruction of the above elements leading to very long term or definite unavailability.

- **Threats potentially causing loss of availability**

  - Masquerading of user identity, either by insiders, or outsiders or service providers, in order to make the service, system, information or network not accessible by the user: e.g. changing access rights, erase disk, stop service.

- Unauthorised use of computer systems or program. For example running personal programs such as games or other non approved programs that make the system and applications fail or erase information.
- Vandalism: malicious and motiveless destruction of property.
- Communications infiltration in order to make the service unavailable or overloaded by excessive useless and damaging traffic.
- Operator/user errors: accidental, improper, or otherwise ill-chosen act by an employee that results in processing delays, equipment damage, software destruction or lost data.
- Software errors or system, network or application failure.
- Technical failure of host, storage device, print facilities, network distribution component, network management host, network interface and network services.
- Errors during hardware or software maintenance causing inappropriate alteration or destruction of data, configuration data, software or hardware. It could happen if lack of appropriate change control process (including testing) or if lack of appropriate version control process.
- Staff shortage leading to excessive need for outsiders with a lack of awareness or competences (hence prone to errors of many types). This can also cause overloaded staff also prone to serious errors making services, systems or information unavailable.
- Insertion or embedding of malicious code that lead to serious corruption or destruction of data, software, storage or databases making them unavailable.
- External attacks to hack into systems or unauthorized access or intrusion into system or network using a computer device, software tools of malicious code in order to delete, modify or corrupt information, software or storage devices.
- Other causes of loss of availability are: power failure (short or long) or air conditioning failure.
- Some other threats can lead to the complete destruction or equivalent like fire, water damage, natural disasters, theft by insiders/outsiders, wilful damage by insiders/outsiders or military action/terrorism.
- A denial of service (DoS) attack is an attempt to prevent legitimate users from using a service. This is usually done by consuming all of a resource used to provide the service. The resource targeted is typically one of the following: CPU, operating memory, bandwidth, disk space.

17. APPENDIX 8: MAPPING IMPACT LEVELS TO CLASSIFICATION LEVELS.

Confidentiality Level	Integrity level	Availability level	Impact Level
Public	Moderate	Moderate	**1**
LIMITED BASIC			**2**
LIMITED HIGH	Critical	Critical	**3**
RESTREINT UE			**4**
CONFIDENTIAL UE, SECRET UE or TRES SECRET UE	Strategic	Strategic	**5**

17.1. Confidentiality mapping

The correspondence is straightforward from the classification level (first column) to the (fourth column).

17.2. Integrity mapping

- In case the integrity level is Moderate, the assessors have the choice between 2 levels of impact: 1 or 2. If there is no consensus on the impact level to choose, the last word on the decision is with the system owner.
- In case the integrity level is Critical, the assessors have the choice between 2 levels of impact: 3 or 4. If there is no consensus on the impact level to choose, the last word on the decision is with the system owner.
- In case the integrity level is Strategic, the corresponding level of impact is 5.

17.3. Availability mapping

- In case the availability level is Moderate, the assessors have the choice between 2 levels of impact: 1 or 2. If there is no consensus on the impact level to choose, the last word on the decision is with the system owner.
- In case the availability level is Critical, the assessors have the choice between 2 levels of impact: 3 or 4. If there is no consensus on the impact level to choose, the last word on the decision is with the system owner.
- In case the availability level is Strategic, the corresponding level of impact is 5.

18. APPENDIX 9: TABLES IN EXCEL FORMAT

The BIA templates embedded as bitmaps in this documents are also available in Excel format. Please refer to the embedded Excel file below.

Business_Impact_An
alysis_Tables_v17_31

: