**Business Case  
<BPM ANALYSIS NAME>**

**Purpose:**

This document is the template for producing a business case.

The business case describes the justification for one or several initiative(s) (IT or non-IT initiatives) in terms of the value to be added to the business as a result of the initiative outcomes.

Prior submission for the IT requirements analysis, the initial business case should be composed of the core document and 2 annexes: Business Requirements log, and Business Case Methodological Review.

After the IT requirements analysis, the business case should be updated and completed with 2 additional annexes: IT Scenario Feasibility, and IT Financial Cost and Benefits / Scenario.

A business case assists in the determination of strengths and weaknesses of a proposal in a systematic and objective manner. The business case should be designed to be business oriented and measurable.

This document is designed as a tool to assist decision makers and/or business analysts in consideration of implementation issues.

A business case is a major input for the IT Programme Management. At various stages, the business case can be updated. For instance, the initial business case is amended after the IT requirements analysis.

Every business case should demonstrate that considerable thought has been given to the implementation of proposals and to how it will be managed.

Table of contents

[1. Executive Summary 5](#_Toc456677549)

[2. Business Objectives and Expected Benefits 6](#_Toc456677550)

[3. Key Performance Indicators 6](#_Toc456677551)

[4. Potential Business Scenarios 6](#_Toc456677552)

[4.1. List of the possible scenarios 6](#_Toc456677553)

[4.2. Alignment 6](#_Toc456677554)

[4.3. Details - Scenario 1 6](#_Toc456677555)

[4.3.1. Business requirements coverage 6](#_Toc456677556)

[4.3.2. Potential business and organisational impact 6](#_Toc456677557)

[4.3.3. Potential technological impact 6](#_Toc456677558)

[4.3.4. Personal data impact 6](#_Toc456677559)

[4.3.5. Other potential impact 6](#_Toc456677560)

[4.3.6. Benefits and costs analysis 6](#_Toc456677561)

[4.3.7. Risk assessment and mitigation actions 6](#_Toc456677562)

[4.4. Details - Scenario n 6](#_Toc456677563)

[4.4.1. Business requirements coverage 6](#_Toc456677564)

[4.4.2. Potential business and organisational impact 6](#_Toc456677565)

[4.4.3. Potential technological impact 6](#_Toc456677566)

[4.4.4. Personal data impact 6](#_Toc456677567)

[4.4.5. Other potential impact 6](#_Toc456677568)

[4.4.6. Benefits and costs analysis 6](#_Toc456677569)

[4.4.7. Risk assessment and mitigation actions 6](#_Toc456677570)

[5. Justification and Recommendation 6](#_Toc456677571)

[6. Implementation Plan 6](#_Toc456677572)

[6.1. Assumptions, constraints and dependencies 6](#_Toc456677573)

[6.2. Time scale 6](#_Toc456677574)

[7. Modelling assets inventory 6](#_Toc456677575)

[8. ANNEX for Data Protection 6](#_Toc456677576)

[9. ANNEX to assess security needs 6](#_Toc456677577)

[10. ANNEXES for the Initial Business Case 6](#_Toc456677578)

[10.1. Annex - Business Requirements log 6](#_Toc456677579)

[10.2. Annex - Business Case Methodological Review 6](#_Toc456677580)

[11. ANNEXES for IT Requirements Analysis 6](#_Toc456677581)

[11.1. Annex - IT Scenario Feasibility 6](#_Toc456677582)

[11.2. Annex - IT Financial Costs and Benefits / scenario 6](#_Toc456677583)

[12. ANNEX - Document control 6](#_Toc456677584)

[12.1. Circulation 6](#_Toc456677585)

[12.2. Change history 6](#_Toc456677586)

[12.3. Applicable documents 6](#_Toc456677587)

[12.4. Reference documents 6](#_Toc456677588)

[12.5. Glossary 6](#_Toc456677589)

[12.6. Usage conventions 6](#_Toc456677590)

**Click on the Show/Hide  button in the toolbar to display/hide guidance.**

# Executive Summary

This section highlights the key points in the business case, which should include important benefits. Some stakeholders will only read this section, so ensure that all pertinent information is succinctly included here (e.g. context, reasons for the BPM analysis, main results, and implementation scenarios)

# Business Objectives and Expected Benefits

Before an organisation starts analyzing, or optimizing business processes, it should define the business objectives it wants to achieve by modelling the organisation's business objectives hierarchy.

Expected benefits are derived from the business objectives. Business objectives are to be achieved by promoting benefits and implementing new business processes and related initiatives.

Describe the benefits that the outcomes of the initiative will deliver expressed in measurable terms. Benefits should be both qualitative and quantitative.

Relevant objectives or benefits can be assigned to the KPIs for evaluating their achievement (see chapter 3).

You can additionally insert here your objective/benefit diagram(s).

| **Business Objective** | | | | **Benefit (Detailed Business Objective)** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°** | **Name** | **P/S[[1]](#footnote-1)** | **Description** | **N°** | **Name** | **Type\*** | **Related KPIs N°** |
| [BO-01] |  |  |  |  |  |  |  |
| [BO-02] |  |  |  |  |  |  |  |
| ... |  |  |  |  |  |  |  |
| [BO-n] |  |  |  |  |  |  |  |

**\*Benefit Types:**

• **DM:** Direct Monetary benefits (measurable);

• **DNM:** Direct Non-Monetary benefits (measurable);

• **IN:** INdirect benefits (not measurable).

# Key Performance Indicators

List the key performance indicators against which the new / modified business processes will be assessed. The **"To-be" KPI** could be described within the "To-be" map (in the ARIS BPM analysis space).

A KPI is an indicator or a benchmark for measuring a degree of objective accomplishment.

Where possible, key performance indicators should include both quantitative (e.g. achieving a numerical target) and qualitative (e.g. level of end user satisfaction) indicators. They should cover both effectiveness of the business process in achieving the desired objectives and efficiency. Most importantly, KPI should be objective, realistic, attainable, and measurable.

For each indicator, it is advisable to identify the points of measurement and the information needed, how it will be collected, frequency of reporting, validity and reliability. It should contain an actual value and a target value.

Metrics: Explain the way the KPI is calculated. In case several metrics are possible, compare, evaluate and recommend the best one, justifying your choice

| **KPI N°** | **KPI Name** | **Metrics (Point of measurement)** | **Actual Value** | **Target Value** | **Related business process or activity** |
| --- | --- | --- | --- | --- | --- |
| [KPI-01] |  |  |  |  |  |
| [KPI-02] |  |  |  |  |  |
| ... |  |  |  |  |  |
| [KPI-n] |  |  |  |  |  |

# Potential Business Scenarios

A scenario describes a way to implement one initiative. Several scenarios are possible for each initiative. The ultimate purpose of this chapter is to provide a founded recommendation for one viable scenario, and to get a decision.

It is important to include the status quo option ("as-is" or "do nothing" scenario) as it will act as the baseline for quantifying the other scenarios.

The advantages and disadvantages of each scenario should be fully explored and evaluated in terms of their costs and risks

## List of the possible scenarios

Identify; describe every possible scenario that can address the business need. Include the status quo scenario.

In the following tables, the ID identifies a scenario.

| **ID** | **Title** | **Description (high level)** |
| --- | --- | --- |
| **SC-01** |  |  |
| **SC-02** |  |  |
| **...** |  |  |
| **SC-n** |  |  |

## Alignment

Describe how the scenario supports the organisation's current business objectives.

| **ID** | **Alignment with business objectives / benefits** |
| --- | --- |
| **SC-01** |  |
| **SC-02** |  |
| **...** |  |
| **SC-n** |  |

## Details - Scenario 1

This section presents the financial and non-financial impacts of the scenario. List the positive and negative non-financial impacts: organisational, technological, regulatory and others. Then list all the costs elements.

### Business requirements coverage

Identify the business requirements covered by this scenario. Refer to the deliverable "Business Requirements log (BREQ)"

### Potential business and organisational impact

### Potential technological impact

### Personal data impact

The processing of personal data[[2]](#footnote-2) is subject to specific requirements enshrined in Regulation EC n°45/2001. Therefore, any impact on personal data shall be identified as soon as possible.

**Annex 8 shall be filled in if at least one of the here below boxes has been ticked** whilst contact shall be made with the Data Protection Service of the Institution by the Business Owner (MOA).

|  |
| --- |
| **What categories of personal data will be processed?** |
| Administrative data (name, email, phone numbers, function, personnel number ...)  Data related to criminal convictions (criminal records)  Evaluation data (cv, annual staff reports, …)  Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership  Data concerning health or sex life  Financial data (bank account, ...)  Profiling data (consumption habits, use of technical log files, GPS coordinates, …) - *Please specify*:  Biometric data (hand-written signature, fingerprints, …) - *Please specify*:  Other - *Please specify*: |

### Other potential impact

### Benefits and costs analysis

List all the cost elements related to the scenario and produce initial estimates of the costs.

Typical business case *costs* include equipment (purchase and maintenance) and labour (training and operation).

If the costs and the benefits can be quantified, you can conduct a cost-benefit analysis by which you weigh expected costs against expected benefits to determine the best (or most profitable) course of action

The cost and financial analysis can be completed within the next version of the business case.

### Risk assessment and mitigation actions

Identify the risks and conduct a risk assessment for the scenario, along with the development of a risk response.

The business case must identify all material risks associated with the scenario, an indication as to who is positioned to bear those risks, and a proposed means to manage risk.

Each scenario will invariably involve some element of risk and uncertainty. Risk encompasses a range of factors, which may result in a scenario failing to deliver the expected outputs and/or outcomes at the estimated cost and time.

Both risk and uncertainty are rarely able to be removed, but can usually be managed. The risks should be assessed in detail and strategies developed to reduce or manage them for the preferred option.

Where appropriate mitigation actions can be devised to manage the risks, they should be documented and included in the business case.

To assist in identifying the various risks inherent in a scenario, the following categories of risk should be considered:

Change in law/policy, commercial, commissioning, completion/construction, contractual, demand, economic, environmental, financial, implementation, investment planning, management, obsolescence, operations, organisational, political, private sector, regulatory/technological, residual value, and upgrade.

These risks need to be assessed for the business case on an ongoing and routine basis during initiative execution (including the degree of risk sensitivity associated with assumptions used). A risk management planning process should also be covered.

|  |  |
| --- | --- |
| **Risk** | **Mitigation action** |
|  |  |
|  |  |

## Details - Scenario n

This section presents the financial and non-financial impacts of the scenario. List the positive and negative non-financial impacts: organisational, technological, regulatory and others. Then list all the costs elements.

### Business requirements coverage

Identify the business requirements covered by this scenario. Refer to the deliverable "Business Requirements log (BREQ)"

### Potential business and organisational impact

### Potential technological impact

### Personal data[[3]](#footnote-3) impact

The processing of personal data is subject to specific requirements enshrined in Regulation EC n°45/2001. Therefore, any impact on personal data shall be identified as soon as possible.

**Annex 8 shall be filled in if at least one of the here below boxes has been ticked** whilst contact shall be made with the Data Protection Service of the Institution by the Business Owner (MOA).

|  |
| --- |
| **What categories of personal data will be processed?** |
| Administrative data (name, email, phone numbers, function, personnel number ...)  Data related to criminal convictions (criminal records)  Evaluation data (cv, annual staff reports, …)  Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership  Data concerning health or sex life  Financial data (bank account, ...)  Profiling data (consumption habits, use of technical log files , GPS coordinates, …) - *Please specify*:  Biometric data (hand-written signature, fingerprints, …) - *Please specify*:  Other - *Please specify*: |

### Other potential impact

### Benefits and costs analysis

List all the cost elements related to the scenario and produce initial estimates of the costs.

Typical business case *costs* include equipment (purchase and maintenance) and labour (training and operation).

If the costs and the benefits can be quantified, you can conduct a cost-benefit analysis by which you weigh expected costs against expected benefits to determine the best (or most profitable) course of action

The cost and financial analysis can be completed within the next version of the business case.

### Risk assessment and mitigation actions

Identify the risks and conduct a risk assessment for the scenario, along with the development of a risk response.

The business case must identify all material risks associated with the scenario, an indication as to who is positioned to bear those risks, and a proposed means to manage risk.

Each scenario will invariably involve some element of risk and uncertainty. Risk encompasses a range of factors, which may result in a scenario failing to deliver the expected outputs and/or outcomes at the estimated cost and time.

Both risk and uncertainty are rarely able to be removed, but can usually be managed. The risks should be assessed in detail and strategies developed to reduce or manage them for the preferred option.

Where appropriate mitigation actions can be devised to manage the risks, they should be documented and included in the business case.

To assist in identifying the various risks inherent in a scenario, the following categories of risk should be considered:

Change in law/policy, commercial, commissioning, completion/construction, contractual, demand, economic, environmental, financial, implementation, investment planning, management, obsolescence, operations, organisational, political, private sector, regulatory/technological, residual value, and upgrade.

These risks need to be assessed for the business case on an ongoing and routine basis during initiative execution (including the degree of risk sensitivity associated with assumptions used). A risk management planning process should also be covered.

|  |  |
| --- | --- |
| **Risk** | **Mitigation action** |
|  |  |
|  |  |

# Justification and Recommendation

Built upon the detailed analysis of scenarios (chapter 4 Potential BPM Analysis scenarios), identify the preferred scenario. The recommendation is based on the net benefits of the viable scenario over all others.

| **Scenarios Findings** | | |
| --- | --- | --- |
| **Scenario** | **Screening summary**  (Baseline / Viable / Discounted) | **Rationale**  (Reasons for inclusion or exclusion) |
| **SC-01: Status Quo** |  |  |
| **SC-02: ...** |  |  |
| **...** |  |  |
| **SC-n: ...** |  |  |

# Implementation Plan

Once the analysis has been completed and the recommended scenario has been identified, the next step involves outlining how the initiative will be implemented. (Major expected deliverables, timing constraints, interdependencies with other initiatives …)

## Assumptions, constraints and dependencies

List and describe all the assumptions, constraints, and dependencies associated with the ability to address the main requirements

|  |  |
| --- | --- |
| **Type**  **(A, C, D)** | **Description** |
| **Assumptions** | |
| A |  |
| A |  |
| **Constraints** | |
| C |  |
| C |  |
| **Dependencies** | |
| D |  |
| D |  |

## Time scale

This section provides information about the period over which the initiative should run, and the period over which the benefits should be realized. This information is subsequently used to help timing decisions when planning (IT programme plan, IT project plan)

# Modelling assets inventory

For each scenario, you can complete this form referring to the To-be map.

List all entity types identified within the data map. An entity type in an application is a logical group of permanent data as seen from the perspective of the user. It is a group of data that an experienced user considers as a significant and useful unit or object. An equivalent to this kind of logical group of data is an object type in data modelling.

An internal entity type meets the following criteria:

* It is used by the application to be counted.
* It is maintained by the application to be counted.

An external entity type meets the following criteria:

* It is used by the application to be counted.
* It is not maintained by the application to be counted.
* It is maintained by a different application (excluded from count).
* It is directly available to the application to be counted.

|  |  |
| --- | --- |
| **Useful information for the workload estimation survey** | |
| Scenario number | [SC-n] |
| End-user(s) |  |
| Type of change *(New development / Enhancement)* | New development  Enhancement |
| Data modelling is available *(Yes/No)* | Yes  No |
| If data modelling is available:   * For a new application: precise number of new Main Entity Type; * For an existing application: precise number of added, changed and deleted Main Entity Type(s). | Total Main Entity Type(s): XX  Including External Main Entity Type(s): XX  Internal:  External: |
| Number of required form(s) | XX forms are required: |
| Number of required report(s) | XX reports are required: |

# ANNEX for Data Protection

Please be aware that this annex is a work in progress that may be completed and/or modified, depending on the phase of the project.

At the initial Business Case stage, it may be only considered as a basis to further discuss the characteristic of the processing with the Data Protection Service.

If the personal data coverage is different per scenario, please complete different questionnaire per scenario.

|  |  |  |
| --- | --- | --- |
| **ID** | **Question** | **Answer** |
| **Impact on personal data** | | |
| I1 | Are personal data directly provided by data subjects or collected via another source (e.g. CODICT)? | from the data subject  other source of collection |
| I2 | Is the processing solely based on the consent of Data subjects[[4]](#footnote-4) (without any legal basis)? | Yes  No |
| I3 | Are personal data handled by an external provider? If yes, please understand in the questions below external provider as defined in the processor's definition[[5]](#footnote-5) | Yes  No |
| I4 | Are disclosures of personal data to entities established outside the EU planned? | Yes  No |
| **Risk assessment** | | |
| R1 | Are access rights foreseen and given according to criticality (e.g. need-to-know …)? | Yes  No  *Please specify (BREQ reference):* |
| R2 | What would be the magnitude of harm to data subjects if personal data were disclosed either intentionally or unintentionally to non-authorized third persons? | low  medium  high  critical  *Please explain why*: |
| R3 | Can data subjects easily access their personal data and notably if handled by a processor5? | Yes  No |
| R4 | Can data subjects easily rectify their personal data and notably if handled by a processor5? | Yes  No |
| R5 | How will consistency of the processing be ensured across the various storage locations? |  |
| **Mitigation actions** | | |
| A1 | Verification of the necessity of collecting personal data (making sure that no other less intrusive way exists) | Remaining work  Done  Other: |
| A2 | Making contact with the Data Protection Service and notifying the processing operation to it | Remaining work  Done  Other: |
| A3 | Definition of a proportionate data retention period and associated procedures of deletion and regular checks of personal data accuracy | Remaining work  Done  Other: |
| A4 | Planning a functionality enabling to manage the deletion of personal data by the end of the retention period | Remaining work  Done  Other: |
| A5 | Verification of the competence of the foreseen recipients as well as of the necessity of the foreseen transfers to those recipients | Remaining work  Done  Other: |
| A6 | Physical reminder (e.g. disclaimer) to recipients that personal data transferred cannot be used for other purposes than the one for which they have been transferred | Remaining work  Done  Other: |
| A7 | Design of appropriate physical and logical security measures | Remaining work  Done  Other: |
| A8 | Information of data subjects through a privacy statement describing the processing operation | Remaining work  Done  Other: |
| A9 | Ensure that data subjects can easily exercise their rights of access and rectification by contacting the data controller[[6]](#footnote-6) | Remaining work  Done  Other: |
| A10 | If the processing operation is voluntary and thus based on consent, plan friendly opt-in and opt-out functionalities | Remaining work  Done  Other: |
| A11 | In case a processor is entrusted with the processing on behalf of the data controller, a detailed data protection clause shall be inserted within the contract, defining its rights and obligations and the fact it may only use personal data upon and according to data controller's instructions and is subject to regulation 45/2001 | Remaining work  Done  Other: |
| **Follow-up actions** | | |
| A12 | Performance of regular updates of the data protection documentation (notification to the Data Protection Service, privacy statement) | Remaining work  Planned  Other: |

# ANNEX to assess security needs

The purpose of this annex is to identify security needs that relate business processes and scenarios to the Information Systems at hand. **The Annex itself is located in the BREQ file/log.**

This form has to be filled in together with the Cassandre team. Please, contact the Centre d'assurances et d'analyses de risques at [CASSANDRE@europarl.europa.eu](mailto:CASSANDRE@europarl.europa.eu). The follow-up and additional queries are under the responsibility of the Risk manager and the Cassandre programme management.

Each requirement within the BREQ Log must be assessed according to the three following axes:

**1. AVAILABILITY:** **what is the maximum unavailability time for the Information System?**

* What would be the impact on the Parliament if the unavailability time of the Information System would be longer?
* Is the information System supporting the EP sessions?
  + Critical the week before the session
  + Critical during the session (when MEPs are there only?)
  + Critical on Fridays after the session
  + Other
* Is the Information System availability need higher only in certain periods of the year?
  + At the end of the year
  + Nights
  + Weekends
  + Other
* What are the Information System's Recovery time objective (RTO) i.e. the time lost from normal business process functioning and the Recovery point objective (RPO). i.e. the data lost or not backed up during that period of time?
* If the Information System is not available, what will be the workaround?

If a high level of availability is needed, the design of the application must be in line with requirements from the Operation Unit (e.g. application should be stateless...).

**2. INTEGRITY:** **what are the integrity needs of the Information System?**

* What would be, in the worst case scenario, the possible impact on the Parliament if a breach of integrity occurs?
* Are business measures already foreseen?

**3. CONFIDENTIALITY: What are the confidentialities needs of the information System?**

* What would be, in the worst case scenario, the possible impact on the Parliament if the information is disclosed?

Levels 2, 3 and 4 relate to classified data: no system exists today at the EP that can handle this information. Handling these data will be more constraining (e.g. no transfer via e-mail, stand-alone PC with no access to network or internet, when necessary only manual handling...).

**Classified Information Unit is in charge of classified information.   
Information Systems with a confidentiality level equal or higher than 2 will be transferred to the responsibility of this Unit, after an initial assessment within DG ITEC.**

Availability

|  |  |
| --- | --- |
| **Level** | **Data maximum unavailability** |
| 0 | More than 3 days |
| 1 | Between 1 day and 3 days |
| 2 | Between 4 hours and 1 day |
| 3 | Between a few minutes and 4 hours |
| 4 | Less than a few minutes |

Integrity

|  |  |
| --- | --- |
| **Level** | **Data integrity** |
| 1 | Could be disadvantageous to the Parliament |
| 2 | Could be disadvantageous to the interests of the Parliament |
| 3 | Could harm the essential interests of the Parliament |
| 4 | Could seriously harm the essential interests of the Parliament |

Confidentiality

|  |  |
| --- | --- |
| **Level** | **Data confidentiality** |
| 0 | Public |
| 1 | Other confidential information |
| 2 | RESTREINT UE / EU RESTRICTED |
| 3 | CONFIDENTIEL UE / EU CONFIDENTIAL |
| 4 | SECRET UE / EU SECRET |

**Notes**

* This maximum level of unavailability cannot be guaranteed today by the standard IT platform: alternative processes/tools need to be studied (e.g. back-up application, implementation of a parallel business process, etc.).
* See Bureau decision of 15 April 2013 "Rules governing the treatment of confidential Information by the European Parliament".
* The security needs and relevant BREQ shall be used for the planning of tests for Information Systems. If you are a Project Manager in charge of the implementation, please contact the test coordinator at Reception Testing Service when using the planning documents [MTP](http://www.evol2wiki.ep.parl.union.eu/wiki/display/testcell/Master+Test+Plan) and TAS.

# ANNEXES for the Initial Business Case

## Annex - Business Requirements log

Refer to or insert your Business Requirements log.

## Annex - Business Case Methodological Review

Business Case Methodological Review completed by the BPM Expert from ITEC-BPM Service and answered by the Business Owner-MOA (supported by the Business Analyst).

The Business Case Methodological Review table is to facilitate the collect of all remarks, comments and modifications proposed during the methodological review of the initial Business Case. Its objectives are to ease the validation process, and to keep track of all the remarks and decisions.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Initials of the reviewer** | **Chapter, paragraph, etc.** | **Remark** | **Answer** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |

# ANNEXES for IT Requirements Analysis

## Annex - IT Scenario Feasibility

Refer to or insert the document provided by ITEC-CONCEPT Unit

## Annex - IT Financial Costs and Benefits / scenario

Refer to or insert the document provided by ITEC-CONCEPT Unit

# ANNEX - Document control

## Circulation

| **DG or Company** | **Role** | **Name/Initials** | | **ERICA[[7]](#footnote-7) code** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Change history

| **Version number[[8]](#footnote-8)** | **Status[[9]](#footnote-9)** | **Date** | **Initials** | **Summary of changes** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Applicable documents

Applicable documents are standards, specimen plans which need to be applied and whose application is verifiable.

| **N°** | **Document name** | **Description[[10]](#footnote-10)** |
| --- | --- | --- |
| [1] | "Charter Scope and Management Plan - CSMP" | Deliverable of the BPM analysis (insert reference) |
| [2] | "As-is" map | Deliverable of the BPM analysis (insert reference) |
| [3] | Business Process Analysis (BPA) report | Deliverable of the BPM analysis (insert reference) |
| [4] | "To-be" map | Deliverable of the BPM analysis (insert reference) |
| [5] | Business glossary | Deliverable of the BPM analysis (insert reference) |
|  |  |  |

## Reference documents

Reference documents are a help or a support but are not directly applicable (e.g. software reference manuals, sample files from outside firms, meeting papers).

| **N°** | **Document name** | **Description** |
| --- | --- | --- |
| [1] | Guide - Benefit Realisation Management | Available on [STANDARDS website](http://www.ismsnet.ep.parl.union.eu/ispnet/cms/Accueil/preconisations/P_Methodologie/PPO4EP), section "Vos indispensables" |
| [2] |  |  |

## Glossary

| **Abbreviation** | **Description** |
| --- | --- |
| **BA** | Business Analyst |
| **BC** | Business Case |
| **BO** | Business Objective |
| **BPA** | Business Process Analysis |
| **BPM** | Business Process Management |
| **BPOw** | Business Process Owner |
| **BREQ** | Business Requirements |
| **EP** | European Parliament |
| **KPI** | Key Performance Indicator |
| **MTP** | Master Test Plan |
| **TAS** | Test plan for Application Security [A3], performed since 2016 in the dedicated TAS-Labo (isolated infrastructure) |

## Usage conventions

Where a chapter or section is not considered to be applicable, put ‘**NOT APPLICABLE**’. Feel free to insert new sections (chapter, paragraph) as needed.

**Click on the Show/Hide  button in the toolbar to display/hide guidance.**

Guidance displayed.

1. P: Primary, S: Secondary. [↑](#footnote-ref-1)
2. Personal data means any information related to an identified or identifiable natural person (the data subject). An identifiable person can be identified directly or indirectly by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity [↑](#footnote-ref-2)
3. Personal data means any information related to an identified or identifiable natural person (the data subject). An identifiable person can be identified directly or indirectly by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity [↑](#footnote-ref-3)
4. Data subjects are the natural persons whose personal data are processed. [↑](#footnote-ref-4)
5. Processor means here external provider - intra-muros or extra-muros- (e.g. service provider having won a EP tender) [↑](#footnote-ref-5)
6. The Data controller is the entity determining the purposes and means of the processing of personal data (e.g. Unit, Directorate or Directorate-General). [↑](#footnote-ref-6)
7. **E**: Examination **R**: Responsible, **A**: Approval, **C**: Contribution, **I**: Informed [↑](#footnote-ref-7)
8. Naming convention: Procedure 'Program & Project naming convention' ([STANDARDS website](http://www.ismsnet.ep.parl.union.eu/ispnet/cms/Accueil/preconisations/P_Methodologie)) [↑](#footnote-ref-8)
9. Status: Draft, Final, Approved [↑](#footnote-ref-9)
10. Description: Note, summary, link, etc. [↑](#footnote-ref-10)