



idm@F4E UID / VERSION

**29XB3F / 1.1**

VERSION CREATED ON / STATUS

**03 October 2018 / Approved**

EXTERNAL REFERENCE

Quality Document  
**F4E-QA-111 Supplier Risk & Opportunity Management  
Instruction**

The purpose of this Work Instruction is to describe how the suppliers risk register is created, updated and maintained in accordance with the Fusion for Energy (F4E)SOP-22.2 Project Risk and Opportunity Management (29SSKX) and F4E-QA-115 - Supplier Quality Requirements (22F8BJ).

The objective of project risk management is to control and reduce the unknowns of a project regarding its main ...

<i>Approval Process</i>			
	<i>Name</i>	<i>Action</i>	<i>Affiliation</i>
<i>Author</i>	<b>Jover Sanz-Pastor T.</b>	<b>03 October 2018:signed</b>	<b>PM</b>
<i>Co-Authors</i>	<b>Loughran T.</b>	<b>03 October 2018:signed</b>	<b>PM</b>
<i>Reviewers</i>	<b>Creus Oleart E.</b>	<b>11 October 2018:recommended</b>	<b>PM</b>
	<b>Rodrigues D.</b>	<b>03 October 2018:recommended</b>	<b>ADM</b>
<i>Approver</i>	<b>Baker K.</b>	<b>11 October 2018:approved</b>	<b>PM</b>
<i>RO: Popescu Marcel-Stefan (F4E)</i>			
<i>Read Access</i>	<b>LG: F4E_QAO, AD: IDM_Users, GG: IAS Audit on Document Management, project administrator, RO</b>		

Original Document MD5#: 3E9C0E83BD9A5F4759C49A9348964EC8

*Change Log*

**F4E-QA-111 Supplier Risk & Opportunity Management Instruction (29XB3F)**

<i>Version</i>	<i>Latest Status</i>	<i>Issue Date</i>	<i>Description of Change</i>
v0.0	In Work	21 August 2017	
v1.0	In Work	02 October 2018	First Issue
v1.1	Approved	03 October 2018	comments from Diogo and Kevin implemented.



# INSTRUCTION

## Control Page

<b>idm@F4E ref:</b>	<b>F4E_D_29XB3F</b>	<b>Date:</b>	<b>2018.Oct.03</b>
---------------------	---------------------	--------------	--------------------

<b>Document title:</b>	<b>F4E- QA-111 Supplier Risk &amp; Opportunity Management Instruction</b>
------------------------	---

<b>Areas and functions</b>			
Procedure ownership:	Risk and Opportunity Management Function		
Area(s) concerned:	Operational Contracts		
Function(s) concerned:	Supplier Project Manager and Risk Management Responsible Function		
Level	<input checked="" type="checkbox"/> Corporate	<input type="checkbox"/> Department	<input type="checkbox"/> Unit

### Purpose

The purpose of this Work Instruction is to describe how the suppliers risk register is created, updated and maintained in accordance with Fusion for Energy’s procedure for Project Risk & Opportunity Management and [F4E-QA-115 - Supplier Quality Requirements \(22F8BJ\)](#).

The objective of project risk management is to control and reduce the unknowns of a project regarding its main objectives: cost, schedule and output performances. Control is achieved by identification and measure of potential delays and cost overruns through risk management techniques and implementing risk response plans.

### Scope

The scope of this document is dependent upon the quality class selected in [F4E-QA-115 - Supplier Quality Requirements \(22F8BJ\)](#) and is applicable to operational contracts.

If the quality class deems that a risk register is required, then the risk register template provided in Appendix A must be completed by the supplier in accordance with this document.

### Table of Contents

Control Page.....	1
1 Introduction .....	4
2 Responsibilities .....	4
3 Risk Procedure .....	5
3.1 Risk Initiation .....	5
3.1.1 Risk Register.....	6
3.2 Risk Identification .....	6
3.2.1 Risk Identification Workshop.....	6
3.2.2 Risk ID .....	6
3.2.3 Type .....	6
3.2.4 Risk Owner .....	6
3.2.5 Risk Title.....	7
3.2.6 Risk Description .....	7
3.2.7 Risk Status.....	7
3.2.8 Risk Category .....	7
3.2.9 Risk Exposure Dates.....	8
3.3 Assess, Analyse & Evaluate .....	8
3.3.1 Risk Classification Tables (RCT) and Probability Impact Diagram (PID) .....	8

3.3.2	Current and Residual Impact Assessment .....	9
3.3.3	Current Impact Assessment.....	9
3.3.4	Technical Flag .....	9
3.4	Risk Response Plans .....	9
3.4.1	Risk Treatment.....	9
3.4.2	Response Action .....	10
3.4.3	Risk Response Owner .....	10
3.4.4	Action Initiation / Completion Date.....	10
3.4.5	Action Status.....	11
3.4.6	Multiple Response Actions .....	11
3.5	Implement Responses .....	11
3.5.1	Risk Reviews.....	11
3.5.2	Risk Register.....	11
3.5.3	Risk Related Issue Management.....	12
4	Communicate and Report .....	12
5	Monitor, Review and Continuous Improvement .....	12
5.1	Audits.....	12
5.1.1	Risk Register Comments .....	13
5.2	Closing of risks .....	13
5.3	Change Control .....	13
5.4	Feedback.....	13
5.5	Project Completion .....	13
6	Appendix A – Risk Register.....	14
7	Appendix B – Risk Categories .....	15
7.1	Requirement/ Scope Definition .....	15
7.2	Design .....	15
7.3	Stakeholder/ Regulatory/Environmental.....	15
7.4	Safety/ Security/Quality .....	16
7.5	Supply Chain/ Supplier Capability.....	16
7.6	Technology/ Information Technology .....	17
7.7	Fabrication/ Manufacture.....	17
7.8	Construction Strategy/ Construction.....	17
7.9	Interface/ Integration/ Assembly .....	18
7.10	Testing/ Operations .....	18

## Reference Documents

- [1] [F4E-QA-115 - Supplier Quality Requirements \(22F8BJ\)](#)  
[2] [Supplier Risk Register \(22HPB6\)](#)

## Roles and Definitions

<b>F4E</b>	Fusion for Energy
<b>NCR</b>	Nonconformity Report
<b>SWOT</b>	Strengths, Weaknesses, Opportunities and Threats
<b>SMART</b>	Specific, Measurable, Achievable, Realistic and Timely
<b>Risk</b>	The definition of a risk encompasses both “threat’s” and “opportunities” and is defined as an uncertain event or set of circumstances that, should it occur, will have an effect either positive or negative on the achievement of one or more of the project’s objectives.
<b>Threat</b>	A threat is an event or set of circumstances that, should it occur, would have an adverse effect on the achievement of one or more of the project’s objectives.
<b>Opportunities</b>	Opportunities are the opposite of threats; they would have a positive effect on the achievement of the project objectives.
<b>Issue</b>	An issue is an event or concern that has occurred or is taking place and needs to be addressed.
<b>Uncertainty</b>	Uncertainty describes a state of incomplete knowledge about a proposition or the range of possible outcomes from a known event. For example, a project may know they need an external approval but may be uncertain over the possible duration of the approval process.

## 1 Introduction

- a) All projects have risks (threats and opportunities) that could affect them in terms of impacting time, cost or reputation. It is therefore of paramount importance to identify and understand the risks and the potential effect they could have on the supplier's scope of work and the wider F4E programme as a whole.
- b) This document describes the scope and level of risk management activities that must be applied by all F4E suppliers and its subcontracts. This work instruction also describes the interfaces and prescribed tools that are central to the delivery of risk management activities by the supplier.
- c) The supplier is deemed to have a working knowledge of risk management and have the capability to comply with early warning contract clauses (if applicable). Risk reviews will form an integral part of the regular and routine supplier performance reviews and part of the suppliers Progress Report as requested in [QA-115 - Supplier Quality Requirements \(22F8BJ\)](#).
- d) For the avoidance of doubt, the Supplier's Risk Register (Appendix A) is intended by the parties to be used to assist with practical matters affecting the management of the Project. The risks contained within the Supplier's Risk Register must not have any contractual effect and do not form part of the Contract.
- e) The Contract requires that F4E and the Supplier work in close collaboration to meet agreed objectives for health, safety, quality, schedule, cost and risk management. As a direct result of this approach F4E developed this work instruction to ensure efficient and consistent risk management activities are implemented between the parties. Requiring F4E and the Supplier to integrate some of their workflow processes to ensure both parties benefit from this integrated approach.

## 2 Responsibilities

- a) The Supplier shall nominate a person from within the Supplier's organisation who is responsible for Risk Management and will be the main point of contact for risk & opportunity management.
- b) In the scope of this document, that person is:
  - The owner of the Risk Register provided in Appendix A.
  - Responsible for the implementation of risk management activities in line with this work instruction;
  - Responsible for the day-to-day management of the Risks identified in the risk register;
  - Responsible for providing updated information on Risks and Risk Response Plans and ensuring that the risk register is accurate and up-to-date;
  - Responsible for following up implementation of risk response action plans;
  - Ensure key decisions and information is captured in the risk register;
  - Responsible for the preparation of reports;
  - Allow for F4E to review and comment on the risk levels for any identified risk before and after the development of a mitigation plan for the risk.
- c) The Supplier's Project Manager is responsible for day-to-day management of the Supplier's risk programme including the following:
  - Overall responsibility for the risk management process;
  - Provision and allocation of resources to support risk management activities;
  - Explain and enable implementation of the risk responses.
- d) The objective is to have a collaborative approach between the Supplier and F4E to anticipate risks and to maximise the effect of mitigation strategies.

### 3 Risk Procedure

To ensure a consistent approach across F4E for Risk Management, a common process has been adopted based on industry best practice and ISO31000, see below in Figure 3.1.

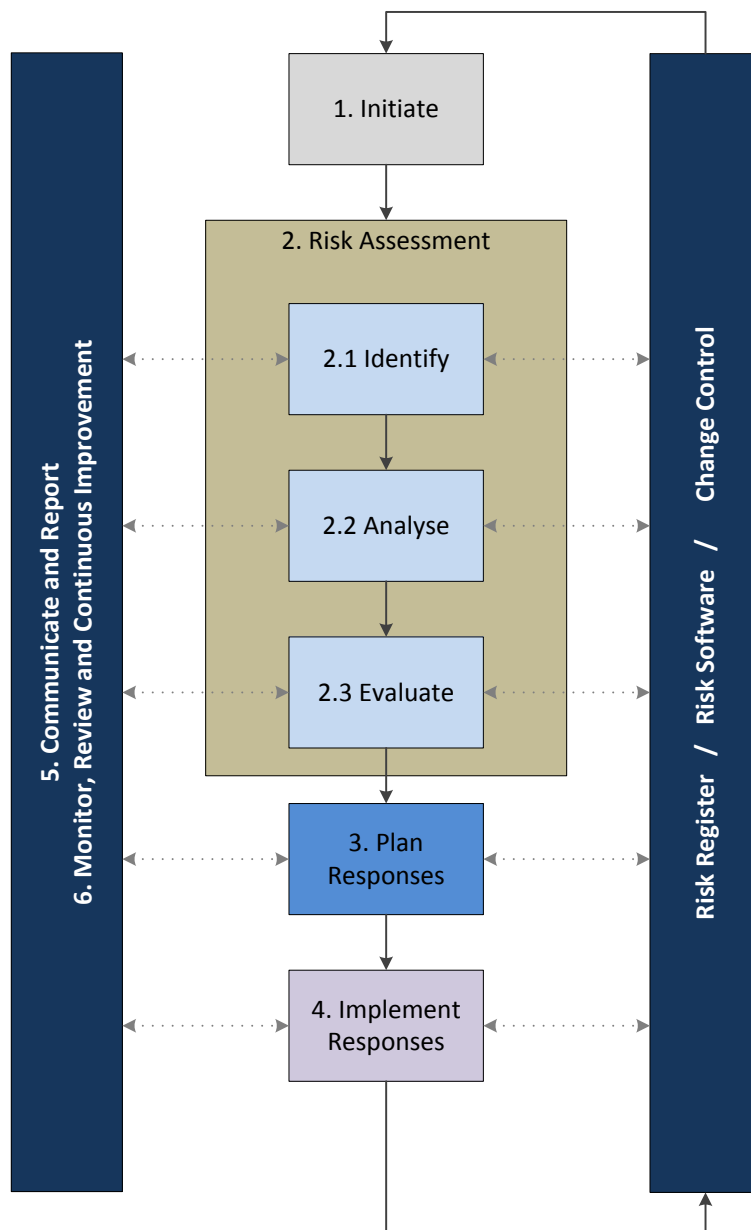


Figure 3.1 – Risk Procedure

#### 3.1 Risk Initiation

- a) As part of the “kick-off meeting” the project will:
- Give a brief on the project to the Supplier;
  - Agree a strategy for the successful delivery of the project;
  - Finalise and confirm the practical methods for communications and submittals, future meetings and exchange contact details of Supplier Personnel and F4E Personnel responsible for each function.
- b) Participation by functional heads of both parties is required at the kick-off meeting to deliver or accept any specific instructions and guidance. The person in charge of Risk Management from the supplier’s

side will be required to attend the kick-off meeting so the requirements for risk management can be discussed and formally agreed.

### 3.1.1 Risk Register

- a) Risks must be captured and recorded on the Supplier Risk Register (Appendix A) and updated in accordance with this work instruction.
- b) From time to time specific instructions may be published by F4E for risks to be updated in a certain way for example the introduction of a new flag to escalate risks; these instructions will be discussed with the Supplier's Project Manager before implementation.

## 3.2 Risk Identification

### 3.2.1 Risk Identification Workshop

- a) The first step is to identify the potential risks (threats and opportunities) to ensure the successful completion of the project this is typically achieved by holding a joint risk identification workshop. A risk workshop should be held for each task order, major changes or when major NCR's are raised.
- b) There are a wide range of techniques that a Risk Manager can use during the risk identification workshop e.g.; questionnaires, brainstorming, checklists, SWOT analysis, and review of risk registers and lessons learned from previous or similar projects.
- c) The person in charge of Risk Management from the supplier organisation, in conjunction with F4E will decide the most appropriate technique to be used during the risk identification workshop. The process of identifying risks is a continuous activity that will take place throughout the project lifecycle.
- d) A risk can be raised by any person involved in the project, once the risk is identified; it is described in detail including the cause(s) and effect of the risk (as detailed in Section 3.2.5 and 3.2.6).

### 3.2.2 Risk ID

- a) Once a risk has been identified it will be captured in the supplier risk register (Appendix A).
- b) Each risk (Threats and Opportunities) will then be assigned a unique number or code to enable the risk to be easily identified. Note: the number or code cannot be reused even if the risk is cancelled.

### 3.2.3 Type

- a) The risk will then be assigned via a drop down box in the risk register as either "Threat" or "Opportunity".
- c) The risk register calculates threats and opportunities separately from each other; so changing the type determines what risk treatment strategy can be selected.

### 3.2.4 Risk Owner

- a) It is essential that ownership is clearly allocated to one appropriate person. The risk owner must have the power to act in control of the risk and must report action taken through the relevant channels. The risk owners are a named individual from of the project team and can be from either F4E or the supplier organisation.
- b) In the case where the risk management ownership is "shared" between F4E and the Supplier, the risk can be split into two risks to describe precisely which portion of the risk must be managed by the Supplier and which portion will be managed by F4E. The Supplier and F4E may also adopt a collaborative risk management strategy.
- c) Risk owners are nominated at the beginning of the risk assessment. They may be, but do not have to be, the individual who identified the risk.



- d) The Risk Owner does not need to be a named person; but must contain the organisation they represent and their role, i.e. F4E – Role. The role must be fully described in the comments section of the risk register (Section 5.1.1)
- e) In the scope of this document the risk owner is responsible for the following:
- Responsible for the accuracy of the risk description;
  - Responsible for ensuring the assessment of the risk is accurate and up-to-date;
  - Responsible for the implementation of the risk response plans and actions;
  - Responsible for the reporting of risk information and attending meeting as required;
  - Accountable to the Supplier’s Project Manager

### 3.2.5 Risk Title

This should be a short sentence which encompasses the risk description, such as a newspaper headline, short and concise that grabs the reader’s attention.

### 3.2.6 Risk Description

- a) It is recommended that all risks are structured and written in such a way that they are clear and unambiguous and identify the cause, the event and the consequence as detailed below:

*As a result of / Due to <definite cause(s)>, there is a risk that / of <uncertain event> may occur, leading to / resulting in <effect on an objective(s)>*

- a) It is very important that the risk cause and effects are fully captured, as it helps focus the risk response plans that need to be put into place to help manage the risk. If cause and effects are not defined or are incorrect then the risk response plans could be ineffective.

### 3.2.7 Risk Status

- a) When a risk is first identified it will have a proposed status, once an accountable risk owner has been agreed and the risk has been populated it will be set to open.
- b) Once “Open” risks are ready to be closed, they will be assigned one of the following closure statuses:
- Closed (Managed): When risk mitigation actions were successfully carried out and the risk has passed its trigger dates and did not occur.
  - Closed (Impacted): When the risk has occurred and impacted the project.
  - Closed (Rejected): When the risk is reviewed and determined to be not valid this could be because the risk has expired or merged with another risk etc.

**Note:** When a risk has been closed impacted, F4E will confirm if a NCR must be raised by the supplier in accordance with the in [QA-115 - Supplier Quality Requirements \(22F8BJ\)](#) “Deviation and Nonconformity Management” Section.

### 3.2.8 Risk Category

This is a drop down box within the risk register that allows the user to select the most appropriate risk category. The risk categories are detailed in Appendix B of this document and in a separate tab contained within the Excel risk register.

**Note:** If more than one risk category applies, select the most appropriate.

### 3.2.9 Risk Exposure Dates

- a) Ideally risks (threats and opportunities) will be associated with an activity in the project schedule, so when the activity is complete the risk can be closed. When risks are linked to activities it will take the early start and latest completion dates from those activities this provides the project the risk exposure dates. This also provides the project with a list of risk that need to be managed now and what risks are on the horizon.
- b) *Risk Start Date:* This is the date that the threat or opportunity can occur from.
- c) *Risk Expiry Date:* This is the date that the threat or opportunity can no longer occur.

### 3.3 Assess, Analyse & Evaluate

- a) Each risk is individually assessed to determine the risk probability and impact during the risk evaluation phase. Risks will be initially assessed for current (pre-mitigation) status. The residual (post mitigation) status can only be assessed once the mitigation plans and responses have been identified (Section 3.4).
- b) Typically, this step may be re-visited several times as the knowledge and understanding of the risk improves as the risk management process evolves.
- c) When a risk is newly identified, a first assessment will be undertaken before any response plan is prepared. The assessment then takes place regularly to evaluate the residual importance of the response plan.

#### 3.3.1 Risk Classification Tables (RCT) and Probability Impact Diagram (PID)

- a) Contained within the Risk Register Template (Appendix A) are pre-determined Risk Classification Tables (RCT) and Probability Impact Diagram (PID) (Figure 3.3.1).
- b) The risk score is determined by plotting the probability of the risk against the highest of the impact bands (cost and schedule) of the risk, then plotting to two together onto the PID. This is completed automatically in the risk register template (Appendix A).

RISKS					PROBABILITY	OPORTUNITIES				
Very Low (1)	LOW (2)	MEDIUM (3)	HIGH (4)	VERY HIGH (5)		VERY HIGH (5)	HIGH (4)	MEDIUM (3)	LOW (2)	Very Low (1)
5	20	45	80	125	Probability of occurrence > 80%	125	80	45	20	5
4	16	36	64	100	Probability of occurrence > 50% but <=80%	100	64	36	16	4
3	12	27	48	75	Probability of occurrence > 30% but <=50%	75	48	27	12	3
2	8	18	32	50	Probability of occurrence > 10% but <=30%	50	32	18	8	2
1	4	9	16	25	Probability of occurrence <=10%	25	16	9	4	1
07. <=0.5M€	06. >0.5M k€ <=1M€	05. >1M€ <=2M€	04. >2 M€ <=5M€	03. >5 M€	COST IMPACT 3. From 10 M€ to 50M€	03. >5 M€	04. >2 M€ <=5M€	05. >1M€ <=2M€	06. >0.5M k€ <=1M€	07. <=0.5M€
08. <=50k€	07. >50 k€ <=500 k€	06. >0.5M k€ <=1M€	05. >1M€ <=2M€	04. >2M€	COST IMPACT 3. Less than 10 M€	04. >2M€	05. >1M€ <=2M€	06. >0.5M k€ <=1M€	07. >50 k€ <=500 k€	08. <=50k€
IMPACT < 1 week	1 week ≤ IMPACT < 3 months	3 month ≤ IMPACT < 6 months	6 months ≤ IMPACT < 1 year	IMPACT ≥ 1 year	SCHEDULE IMPACT	IMPACT ≥ 1 year	6 months ≤ IMPACT < 1 year	3 month ≤ IMPACT < 6 months	1 week ≤ IMPACT < 3 months	IMPACT < 1 week

Figure 3.3.1 - RCT / PID

#### 3.3.1.1 Probability (Likelihood)

The determination of probability is to be completed by suitably trained and experienced personnel. This analysis will also include assessments from other stakeholders and to obtain a balanced point of view.

### 3.3.1.2 Impact (Cost and Schedule)

It is advisable that input from the Project Estimator and the Project Planner is sought when assessing the risk impacts to avoid double accounting of the risks, and to gain an appreciation of the potential impact to the project schedule.

### 3.3.2 Current and Residual Impact Assessment

- a) The Likelihood, Cost and Schedule impacts are drop down boxes. As described in Section 3.3.1 the risk register has a per-determined RCT and PID.
- b) The probability and schedule impacts are the same regardless of the value of the project. However, the Cost impact scale can be adjusted to the needs of the project by selecting the bands available in the “The Cost Impact Scale” in the header of the risk register.
- c) The Risk Register has three cost impact scales to select from.
  - Less than 10 million Euros
  - Between 10 million and 50 million Euros and
- d) Once one is selected the available options drop down box in cost impact will change automatically. But if the risk register is complete and the cost impact scale is changed after this the cost impact bands will need to be re-assessed as this *is not updated automatically*.

### 3.3.3 Current Impact Assessment

- a) The Current status takes into account the following action status:
  - Actions Complete
  - Actions In-progress
- b) The residual assessment score/level can only change from the current assessment if proposed actions have been raised.

### 3.3.4 Technical Flag

- a) In addition to assessing the cost and schedule impacts; due to the technical complexity of the ITER Machine risks are also assessed against the technical criteria to provide an alternative view of the risks. The one of the following symbols are selected:
  - - Minimal or no consequence to technical performance;
  - ★ Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program;
  - ✓ Moderate reduction in technical performance or supportability with limited impact on program objectives;
  - ● Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success;
  - ⊗ Severe degradation in technical performance; Cannot meet baseline or key technical/supportability threshold; will jeopardize program success.

## 3.4 Risk Response Plans

Once the risks (threats and opportunities) have been assessed the next step is to prepare specific management responses against the identified risks for the purpose of removing, or reducing the threats and to maximise opportunities.

### 3.4.1 Risk Treatment

- a) Before generating a detailed risk response, the strategic approach to be taken should be considered. The potential strategies fall into four categories which are discussed below:
  - Threats: Reduce, Avoid, Transfer, or Accept

- Opportunities: Enhance, Exploit, Facilitate or Reject

#### 3.4.1.1 Reduce / Enhance

- Mitigation/ Enhancement plans are the responsibility of the risk owner, plans need to be resourced, implemented, monitored, adjusted, and reported on.
- Every risk and opportunity must be allocated an owner who is responsible for ensuring that the agreed actions are implemented.

#### 3.4.1.2 Avoid/ Exploit

Avoiding or exploiting involves adopting a different approach and so removing the threat or realising the opportunity e.g. changing the scope of the project, changing the project requirements or objectives to enable the risk to be avoided or the opportunity to be realised.

#### 3.4.1.3 Transfer / Facilitate

- The main reason for transferring a threat is if another party may be more capable of effectively addressing the threat.
- For opportunity this involves sharing the opportunity so that everyone is incentivised to work collaboratively to maximise the opportunity.

#### 3.4.1.4 Accept/ Reject

- In some cases, it may be appropriate to accept the threat either when the threat is assessed as very low, or when it is not cost-effective or possible to reduce the threat further by mitigation or transfer.
- Similarly, for opportunity, when it is not cost-effective to treat them any further they are rejected.

#### 3.4.2 Response Action

- Reducing or enhancing actions involves creating a response plans; the plans should:
  - Be 'SMART'.
  - Provide a baseline against which progress can be monitored
  - Enable informed decisions to be made on whether to invest in the threat response.
  - Address the probability of occurrence and the direct causes or consequence of the threat/opportunity.

#### 3.4.3 Risk Response Owner

- The Risk Owner is responsible for ensuring that the appropriate person has been appointed to manage the risk response.
- The Risk Response Owner is accountable for the implementation and progress of the risk response actions assigned to them.
- The Risk Response Owner does not need to be a named person; but must contain the organisation they represent and their role, i.e. F4E – Role. The role must be fully described in the comments section of the risk register (Section 5.1.1).

#### 3.4.4 Action Initiation / Completion Date

- Ideally Risk Response Actions will be associated with an activity in the project schedule, so when the activity is complete the action can be closed.
- Action Initiation Start Date: This is the date that the action is expected to start. This will enable open actions to be monitored and progressed.

- c) Action Completion Date: This is the date that action MUST be complete by i.e. not a soft target date (aim or hopeful date); but the date action must be completed by as it would have programme repercussions.

### 3.4.5 Action Status

- a) Each action will be assigned its own status from:

- Proposed New action identified and is under consideration to be implemented;
- In-Progress Action is currently on-going;
- Complete Action was successfully implemented;
- Delete Action is no longer valid and has been closed without being implemented.

### 3.4.6 Multiple Response Actions

If multiple response actions have been identified, then they should be added to the risk register in the following format (Figure 3.4.6):

Risk Response					
Treatment	Response Actions	Action Owner	Initiation Date for each action	Completion Date for each action	Status
Reducing	1. Hold integrated meetings with IO for an improved interface management, including progress meetings with component designers (e.g. design & integration reviews)	1. F4E - (PTM)	1. 01/01/17	1. 31/12/19	1. In-Progress
	2. Project Strategy is to defer the manufacturing of items until the interfaces and boundaries are frozen.	2. F4E - (TPO)	2. 01/08/17	2. 30/04/19	2. In-Progress
	3. (FB) If the risk occurs then the project will challenge the configuration changes and raise a PCR.	3. F4E - (PTM)	3. 01/01/17	3. 30/04/19	3. Sanctioned

Figure 3.4.6 - Multiple Response Actions

## 3.5 Implement Responses

The aim of the Implement Response step is to ensure that risk management process has been implemented effectively by undertaking regular risk review and that planned risk response actions are be monitored.

### 3.5.1 Risk Reviews

The person in charge of Risk Management from the suppliers are responsible for ensuring that regular risk reviews are carried out on the project (generally within a minimum interval of three months and monthly for the more significant risks) and for ensuring that the information captured within the risk register remains accurate.

### 3.5.2 Risk Register

- a) Risks will develop throughout the life of the project; this new information must be captured and recorded on the risk register. The implementation step ensures that the risks held within the risk register are reviewed in accordance with this work instruction and that new risks are being identified and captured as well as ensuring that existing risks are being mitigated and where appropriate closed.

- b) It is the Supplier's Project Manager responsibility to review the risk register and ensure that the following is being carried out:
- Ensure that appropriate progress is being made against the risk responses, with particular attention to risks with a medium or high impact
  - Determine where risk response actions have been carried out, has this affected the probability of the risk or the severity of the impact(s)
  - Establish if any risks have occurred and therefore are subject to closure and/or implementation of fall-back plans
  - Highlight any adverse trends

### 3.5.3 Risk Related Issue Management

When a risk occurs and impacts on one or more of the projects objectives it is classified as an issue. Once the Issue has been realised, the Supplier's Project Manager shall inform F4E and formally capture the impacts of the issue in a systematic and auditable manner.

## 4 Communicate and Report

- a) The Supplier shall be responsible for monitoring the risks related to the project and for providing F4E with a copy of the latest Supplier's Risk Register.
- b) If a Risk is reviewed and no changes are made to the risk; then the notes cell within the risk register must be updated with the following:
- Date of the risk review.
  - Name and role of the reviewer(s)
  - Comment "Risk was reviewed and agreed with no changes"
- c) Risk reporting at the Supplier's level will consist of:
- Providing risk information when requested;
  - Updated Risk Register (including a narrative on the changes);
  - Risk item status in each criticality level;
  - Identification of new risk items;
  - Closed risk items from previous months;
  - Risks or issues requiring significant attention.
  - Custom/unique risk reports maybe requested by F4E. These reports will be discussed with the Supplier's Project Manager for agreement.
- d) The Risk Register must be updated and submitted as part of the Progress Report for discussion during the Progress Meeting between F4E and the supplier. The Supplier's Risk Register is to be completed to take into account the updates identified by both Parties and stored by the supplier in CTS on a quarterly basis as a deliverable.

## 5 Monitor, Review and Continuous Improvement

This step encompasses all aspects of the risk management process to verify that the Risk Management processes and procedures are being implemented correctly. As a result, the Risk Management activities will be more robust and will offer added business benefits to both F4E and the supplier.

### 5.1 Audits

As part of the projects overall contract governance specific risk management audit may be undertaken to ensure process and procedural compliance.

### 5.1.1 Risk Register Comments

- a) As the risk register progresses it is important to record key decisions and information for audit purposes.
- b) The Person responsible for managing risk within the Supplier's organisation shall ensure that the Comments is updated with the following as a minimum:
  - The date the review took place
  - Named reviewers
  - Short summary that describes the outcome of the review. (Note: If the risk was agreed with no changes then this still needs to be captured in the comments cell)
  - The comments box must also describe the abbreviations used to describe the Risk Owner and Risk Response Owner.

### 5.2 Closing of risks

- a) As the project progresses risks (threats and opportunities) will be closed either because the probability or consequence of the risk is reduced to acceptable level or risk has passed.
- b) Risks that are highlighted to be closed must be proposed by the Supplier and validated by F4E during the Progress meeting in a collaborative approach.

### 5.3 Change Control

- a) During the life of the project, F4E may raise a change to the project scope in accordance with the contract requirements.
- b) Changes may have a considerable impact on the risk register; therefore, an assessment of the change is required. If the change is deemed to have a major impact on the risk register, a risk workshop can be requested by the Supplier's Project Manager.
- c) Where a defect or nonconformity has occurred the supplier shall raise a NCR in accordance with [QA-115 - Supplier Quality Requirements \(22F8BJ\)](#) "Deviation and Nonconformity Management" Section.

### 5.4 Feedback


Feedback is a vital part of the risk management process, as the project progresses, the supplier and F4E will gather valuable information which will be used to improve the risk management process and can inform other projects of best practice methods to be used.

### 5.5 Project Completion

- a) When the project is in its final few weeks, a risk review will be held to review the remaining risks. The aim of the review is to close the remaining risks.
- b) The last progress meeting of the contract will review the project risk register and agree the risks to be transferred to the next phase and to identify risks for lessons learnt.

## 6 Appendix A – Risk Register

The Risk Register is illustrated below and can be accessed via this hyperlink [Supplier Risk Register \(22HPB6\)](#)

 <b>RISK REGISTER</b>															Document Reference No:											
															Issue Date:											
															Revision Number:											
F4E / Supply Chain Risk Register: Supply Chain																										
CONTRACT REF NUMBER:																										
COST IMPACT SCALE: Between 10M and 50M Euros																										
PROJECT TITLE:																										
PROJECT TEAM:																										
PROJECT MANAGER:																										
Risk ID	Threat/ Opportunity	Risk Owner	Risk Category	Status	Risk Description			Current Impact Assessment				Risk Response					Target Impact Assessment				Technical Flag	Comments				
					Risk Title	(*As a result of...)	(*There is a risk that...)	(*Resulting in...)	Start date	Finish date	Likelihood	Cost Impact (€k)	Schedule (days)	Risk Score and Level	Treatment	Response Actions	Action Owner	Initiation Date for each action	Completion Date for each action	Status			Likelihood	Cost Impact (€k)	Schedule (days)	Risk Score and Level



## 7 Appendix B – Risk Categories

### 7.1 Requirement/ Scope Definition

#### *Requirements*

- Are the functions or Requirements undefined, incomplete or unclear? If so what is the concern?
- Insufficient Requirements analysis performed? If so why is this a concern?
- Are there any unstable Requirements? If so what is the concern?
- Are the Requirements difficult to trace? If so what is the concern?
- Is there actual or potential non-compliant or invalidated Requirements?

#### *Scope Definition*

- Is the Scope clearly defined and understood
- Are the parties clear on what they are delivering/providing
- Are there any gaps between Requirement and Scope
- Is the Requirement for the System/Sub System clear
- Is there any ambiguity in understanding between parties

### 7.2 Design

#### *Design Complexity*

- Are there any complex design features that present a particular cause for concern?
- Is the Design compromised by a need to complete for the PA or other milestone?
- Is there potential for incompatibility between designs?
- Are there numerous or unclear bases of assumptions?

#### *Design Maturity*

- Are aspects of the Design unresolved due to unclear requirements and scope?
- Inadequate or conflicting design documentation?
- Are there any known or potential errors or omissions in the Design?

#### *Design Development*

- Is the design still being developed...particularly relevant as it nears PA signature?
- Is there potential for the design to advance and not be effectively communicated?
- Is the change process capturing Design changes and are these and effectively communicated?

#### *Design Integration*

- Is the design effectively communicated? If No what are the concerns...?
- Are there any known or potential unstable or not frozen interfaces?
- Are there any known or potential design integration issues?

### 7.3 Stakeholder/ Regulatory/Environmental

#### *Stakeholder*

- What are the key Stakeholders concerns? Do these present a cause for concern?
- Are there any particular Stakeholders concerns that are currently causing problems?
- Are there any likely Stakeholder concerns that will cause problems in the future?

#### *Regulatory*

- Are there any particular French Regulation concerns that are currently causing problems?
- Are there any likely French Regulator concerns that will cause problems in the future?

#### ***Environmental***

- Is an Archaeological Review required? What are the concerns?
- Is an Environmental assessment required? What are the concerns?
- Any Environmental Permits or licenses required? What are the concerns?
- Are there any known or potential Environmental concerns?
- Potential for releases or additional releases?
- Undefined disposal methods?

### **7.4 Safety/ Security/Quality**

#### ***Safety***

- Does the system or subsystem have:
  - Hazardous material involved?
  - Significant contamination potential?
  - New design basis accidents or other unreviewed safety questions?
  - Safety class or safety significant systems (or other non-nuclear equivalent) involved?
  - Is the French Regulators approval or safety basis documentation requirements a cause for concern. Is it likely to take longer than planned?

#### ***Security***

- Are there any security related issues with any aspect of the system that are currently/or are envisaged that will cause problems?

#### ***Quality***

- Is precision work required and if so are there any perceived difficulties?
- Does the supplier community have the required skill?
- Are QA standards well-defined?
- Are QA processes understood?
- Change without careful analysis and integration into the design?
- Lack of information transfer in-between design, manufacturing, and assembly teams?
- Lack of (or limited) tests for budget or schedule reasons?
- Out of tolerance deviations from / during manufacturing?
- Is rework expected due to nature of project tolerances?

### **7.5 Supply Chain/ Supplier Capability**

#### ***Supply Chain***

- Is there sufficient depth in the supply chain to ensure competition?
- Is there potential for unavailability of qualified vendors or subcontractor?
- Does the supply chain have sufficient spare capacity to undertake the work?
- Is the supply chain sufficiently qualified, experienced and possesses the necessary skills to perform and deliver the work?
- Does the supplier have the requisite experience, skills to ensure the supply chain delivers?

#### ***Supplier Capability***

- Is there potential for the unavailability of facilities?
- Does the supplier community have the required skill?
- Are there any uncertainties associated with the supplier process?
- Are there any uncertainties associated with the supplier stability?
- Are there any known or potential difficulties with the availability of materials or parts?

## 7.6 Technology/ Information Technology

### *Technology*

- Does R&D support the technology development? If not what is the main concern?
- Is there any unknown or unclear technology in any part of the system that is a cause for concern?
- Is there a requirement for a new application of an existing technology that is or will present a problem?
- Is there modernized /advanced technology in an existing application?
- Is there potential for technology under development that will not perform as expected (specific items)?
- Is there a requirement for new technology that is presenting a cause for concern?
- Is there potential for new technologies not to be properly developed by the R&D programme
- Is there potential that integration of the technology into the ITER system fails?
- Is there potential that technology no longer supported?
- Is Industry in place?

### *Information Technology*

- Are there any known or potential problems associated with IT or Software?
- Is there potential for incompatibility (Hardware/Software) across systems?

## 7.7 Fabrication/ Manufacture

- Are there any problems/potential problems associated with the fabrication capabilities within the supply chain?
- Are design documents inadequate to develop manufacturing plans or control specifications?
- Is the system for manufacturing management inadequate to control the quality, cost, and schedule?
- Manufacturing plans are late or insufficient to manage the fabrication of components
- Manufacturing processes cannot produce components that meet the design criteria
- The system for disposition of non-conformances is inadequate to meet the schedule
- The systems engineering function is inadequate to integrate the component/system tolerances and specifications
- Is there a risk to fabrication and assembly from the effects of cumulative tolerances
- Is there potential for machinery failure in fabrication phase?
- Demands on the QA/QC system will delay the manufacturing schedule

## 7.8 Construction Strategy/ Construction

### *Construction Strategy*

- Are there any known difficulties with the construction strategy?

**Construction**

- Site ground conditions are not as expected?
- Is the Building design not adequately integrated with systems to be installed?
- Is there a risk of equipment & component degradation during shipping and storage?
- Is there a risk of availability of lay down space?
- Are there any conflicts between buildings and plant installation?
- Is there any maintenance issues to equipment & components in storage?
- Are there conflicts between Supplier working areas?
- Is there potential for site safety systems and management will be ineffective in ensuring worker safety?

**7.9 Interface/ Integration/ Assembly****Interfaces**

- Are there any unstable or not frozen interfaces?
- Are multiple project interfaces involved and do these present a concern?
- Are all interfaces for this system understood and documented?
- Is there potential for insufficient systems integration?
- Do other adjacent Systems understand clearly this System requirements?

**Integration**

- Are there any known or potential integration issues?
- Is the integration of buildings and systems clear?
- Is the integration of system to system understood?
- Is the integration of system to building understood?

**Assembly**

- Is the Assembly schedule inadequately defined?
- Is the Assembly multi shift working pattern unachievable?
- Is the Assembly unable proceed due to unavailability of Buildings?
- Is the Assembly unable to proceed due to the unavailability of Plant & Equipment?
- Is there potential for difficulties to arise during Assembly phase
- Is there potential for re-work to occur during Assembly phase due to for example incompatibilities of components or systems?
- Is there a risk of Assembled plant tolerances being exceeded?
- Is there is a risk of Assembly unable to proceed due to incompatibility issues i.e. the affects of compounded tolerances?

**7.10 Testing/ Operations****Testing**

- Are there any problems foreseen in the Testing phase?
- Operations
- Are there any problems foreseen in the Operations phase?
- Is there potential for major component/equipment failure in Operations phase (list specific systems)?

- Difficulties envisaged due to multiple suppliers will have unplanned conflicts working in the same area?
- Difficulties envisaged from multi-shift commissioning work that will not be achievable?
- Is planning immaturity within Operations a potential problem?
- Is there a potential problem due to maintenance routines not being adequately defined?
- Insufficient spare parts will be available?

***Other***

- Free Category - enter here any other risk that does not comfortably fit into the above