

**Efficiency as a Service**


Plugging a new energy model

Guidelines of risk mitigation

Deliverable: D3.5

Please note that this document is a draft of the final version of “Guidelines of risk mitigation” which will be published in 2022. The EaaS team invites all readers who have questions, comments and recommendations on the content of this document to provide these to info@eaas-initiative.org. The EaaS team could include these in the final version as appropriate.





Contributing authors (alphabetical order)

Mira Tayah, AGORIA

Carlos Ballesteros, ANESE

Javier Martínez Belotto, ANESE

Daniel Navarrete, ANESE

Arno Nijrolder, InnoEnergy

Dimitris Karamitsos, Stiftung BASE

Daniel Magallon, Stiftung BASE

Christophe Rynikiewicz, Stiftung BASE

Text Editor:

Dimitris Karamitsos, Senior Energy Efficiency Business Developer Specialist,
Stiftung BASE.

December, 2021

* The present document reflects only the authors' view and the CINEA or the European Commission are not responsible for any use that may be made of the information it contains.



Executive Summary

Efficiency as a Service (EaaS) is a pay-per-service model to decrease energy consumption from equipment in cities around the world, by making more efficient technologies more accessible to customers. Instead of selling the equipment delivering the service, solution providers shift to selling the outcome generated by the equipment. Examples include cooling, heating, lighting, compressed air, etc. The payment for such services may be based on a pay-per-use scheme, which means that solution providers need to determine the price charges per unit of service delivered, but also all the risks that may occur while implementing such a model.

For this purpose and as part of the Efficiency as a Service initiative, an evaluation of the risks potentially occurring in such projects was completed. These were studied for each stakeholder active on EaaS projects: the provider, the financial partner and the client.

In addition, the report includes existing solutions available to manage risks occurring in EaaS projects. Indeed, due to the complexity of risks occurring in some energy efficiency infrastructure projects, it is recommended for the reader to view the included state-of-the-art studies hereby, in order to attain a holistic view of potential risks occurring in such projects and how to potentially mitigate them.

Therefore, please note that this document provides the basics to evaluate the risks within EaaS projects. Adopters are encouraged to compare, incorporate and/or integrate their proper internal risk tools as well.



Table of Contents

| | |
|--|-----------|
| Executive Summary | 2 |
| 1. Introduction | 5 |
| 2. Risks | 5 |
| 2.1 Project development phases | 5 |
| 2.2 Risk associated with the different stakeholders of the project | 6 |
| 2.2.1 For the EaaS Provider | 6 |
| 2.2.2 For the EaaS Client | 9 |
| 2.2.3 For the EaaS Financier | 9 |
| 2.2.4 EaaS project risks: key aspects | 10 |
| 2.3 Risk analysis heatmap on the business | 13 |
| 3. Existing risk analysis tools | 15 |
| 3.1 QualitEE | 15 |
| 3.2 EEFIG tools | 15 |
| 3.3 LAUNCH protocol | 15 |
| 3.4 International Energy Efficiency Financing Protocol (IEEFP) | 16 |
| 4. Possible mitigation actions | 16 |
| 4.1 National guarantee systems (financial) | 16 |
| 4.2 Insurance products (financial) | 17 |
| 4.3 IEEFP Mitigation strategies | 17 |
| 4.4 Other (financial and non-financial) | 17 |
| 4.4.1 SLA agreements | 17 |
| 4.4.2 EaaS assistance | 18 |
| 5. Conclusion and disclaimer | 18 |
| 6. Annex: List of key stakeholders interviewed | 18 |



List of tables

| | |
|---|----|
| Table 1: Risks with EaaS projects | 14 |
| Table 2: Scale of risks for EaaS projects | 14 |

List of figures

| | |
|---|----|
| Figure 1: Core phases of EaaS Projects | 6 |
| Figure 2: Risk heat map for the customer | 14 |
| Figure 3: Risk heat map for the solution provider | 15 |
| Figure 4: Risk heat map for the financier | 15 |
| Figure 5: PF4EE instrument | 18 |



1. Introduction

The objective of this report is to identify internal and external risks related with the servitisation and the capitalisation strategy and describe the general guidelines for risk mitigation for the servitisation projects supported via the Efficiency as a service (EaaS) business model.

We detail the perceived risk for the SME, the providers and financial entities regarding the performance of the servitisation contracts.

The process will be tested with different stakeholders proposing servitisation of energy efficient equipment during the activities conducted under the other activities of work packages 6,7 and 8 within the EaaS initiative, consisting of building a pipeline of projects in Belgium, The Netherlands and Spain.

2. Risks

The core risks relevant to the implementation of Efficiency as a Service (EaaS) are identified in this section. In the next chapters and in Table 1 in section 2.2.4, each of these risks are explained and evaluated with regards to the implications of implementation on each party in a business transaction within the context of EaaS. Table 1 considers and evaluates the parties bearing the risk under a business-as-usual “Efficiency as a Service” transaction, the amount of risk borne by each party under such a contract, and the party best-positioned to bear the risk in question. Each risk is also categorised within the respective phase of the project it might occur. These phases are shown in Figure 1 and described in section 2.1.



2.1 Project development phases

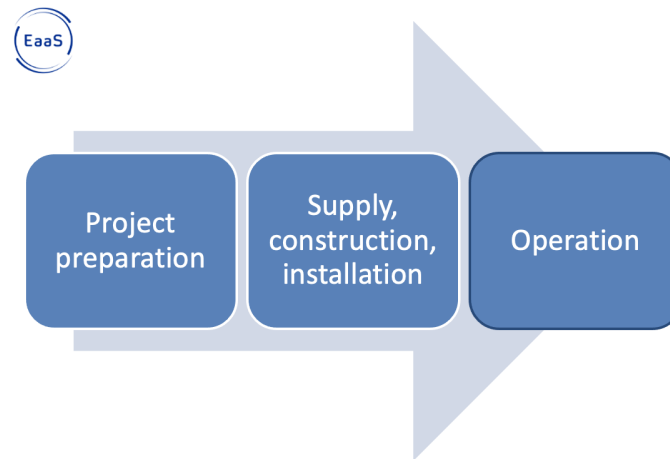


Figure 1: Core phases of EaaS Projects

Phase 1 - Project preparation phase:

At this stage the technology provider selects the right solution to be provided to the end-customer, prepares the offering and evaluates the proper financing partner to onboard.

Phase 2 - Supply, Construction, Installation phase:

The solution has been selected, the financing partner as well and the contracts between the stakeholders have been signed. The solution provider starts to ship/ transport and implement the systems which will be providing the services to the end-customer.

Phase 3 - Operation phase:

The solution provider keeps ownership of the equipment, maintains them, and runs their operation to the end-customer who pays for the service received. The investor(s) (if present) also receives the returns of the project, as contractually agreed.

2.2 Risk associated with the different stakeholders of the project

2.2.1 For the EaaS Provider

The risks of EaaS associated to the solution provider can be summarised as:

a) Technology risk:

- i) Performance risks: These can link to higher operation costs related to utility costs. Since prices per utilisation are contractually agreed upfront, risks associated with performance efficiency are transferred to the solution provider.
 - ii) Hardware system malfunction: any hardware malfunction or parts requiring replacement earlier than expected is at the cost of the solution provider. Furthermore, while the system is not operational the customer does not pay for the service and additional penalty fees could apply. The EaaS provider's liability with regards to the impact hardware malfunctions may have on the customers' end-products will depend on the contractual agreements between the two parties.
 - iii) Manufacturing risks: The solution provider is fully responsible and directly exposed to any manufacturing risks (either subcontracted or not). Solutions placed on site must be operational as contractually predicted for the solution provider to meet expectations and revenue estimations.
 - iv) Software system malfunction: any software malfunction may lead to inaccuracies in system operations and hence performance risks. Solution output quality is at the expense of the solution provider.
 - v) Meter reading malfunction: This can be associated with ii) iii) and iv) above - however any system consumption meter mal-reading jeopardises the services as either the solution provider or the customer is overcharged for the service. However, we consider this a solution provider risks as it is their responsibility to ensure the good functioning of this equipment.
- b) Construction and completion risks: the solution provider entails the full risk within the construction phase. Any delay also impacts any delay in revenue from the customer and potential penalties as well.
- c) Tech provider operation risks (supply chain, service team): risks associated with the replacement of parts during operation are associated with the tech provider supply chain and service team risks.
- d) Procurement and tariff risk: these risks may occur due to delays in the procurement processes due to bureaucratic delays or changes to the tariff environment as a transaction is ongoing.



- e) Unanticipated maintenance risk: The risk that the amount of maintenance demand is much higher than expected, or any delays and unexpected difficulties in maintenance.
- f) Service continuity risk: External risks such as power outage or other business interruptions which disables the proper operation of the equipment.
- g) Commercial risks:
 - i) Customer disputes: disputes with the customer may lead to contract terminations.
 - ii) Change of customer: when providing EaaS contracts in the build-environment, the owner of the building/ asset may change during the contracted period (i.e sale of building, of business etc).
 - iii) Counterparty existential risk: The solution provider is exposed to customer financial capacity to pay for the service.
 - iv) Failure of counterparty infrastructure: if some or all of the equipment of the solution provider is placed within the infrastructure of the client, there are risks associated with any damage to the infrastructure of the client which may damage the equipment of the solution provider.
 - v) Counterparty demand risk: The demand / usage of the equipment may exceed what has been contractually agreed.
 - vi) Volume risk: the equipment might not be in use for a substantial period of time.
 - vii) Residual value risk: when the equipment is returned before it is fully depreciated.
 - viii) Balance sheet risk: as the company shifts from selling a product to selling a service, the balance sheet of the company changes considerably. There is no one solution that fits all against risks which may appear due to this, but the company providing the service must be aware and know how to tackle this change with its shareholders.
 - ix) Partnership risks: the provider should look whether providing their solutions as a service could compete with existing commercial partnerships on the ground. If the latter is the case, it is recommended that these partners are involved in the process, in order not to damage the partnership. Else, an alternative is to end these partnerships, if it makes sense commercially.



- h) Management risk: when implementing a new model in the company, it is key to have internal support, such as a sponsor on the board level or high management, so that the whole company can drive the vision of implementing a servitisation offer.
- i) Policy Regulatory and accounting standards risks: the solution provider must consider upcoming regulations to ensure their solutions are compliant
- j) Foreign exchange risk: Risk associated to foreign exchange losses
- k) Force majeure event: any circumstances beyond the solution provider reasonable control which directly prevent the performance of its obligations and includes without prejudice to the generality of the foregoing any of the following:
 - i) War, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, breaking off of diplomatic relations or similar actions.
 - ii) Terrorist attack, civil war, civil commotion or riots.
 - iii) Epidemic or pandemic.
 - iv) Any law or government order, rule, regulation or direction, or any action taken by a government or public authority, including but not limited to imposing an embargo, export or import restriction, quota or other restriction or prohibition, or failing to grant a necessary licence or consent.
 - v) To the extent beyond the reasonable control of the solution provider - any labour dispute, including but not limited to general strikes, industrial action or lockouts (other than in each case any such Labour Disputes involving employees of the Affected Party, or employees of any of the Affiliates of the Affected Party or employees of any contractor of the Affected Party).
 - vi) Unavailability of, or disruption in the supply of electricity and water from a supplier licensed to provide such services to the public.
 - vii) Floods or other usually severe weather conditions, earthquake, hurricane, drought, other natural disasters, explosions or fire.

2.2.2 For the EaaS Client

There are different risks associated with the EaaS model for the client. These include:



- a) Tech provider existential risk: There is a risk that the solution provider becomes solvent in which case the customer will no longer be receiving the services required.
- b) System breakdowns: This risk refers to the situation when the system stops working due to a manufacturing, installation or factory defect. This might cause product damage (e.g. frozen food decomposition in a food processing industry), production delays or discomfort for the users (e.g. heating breakdown in a hotel case discomfort to guests).
- c) Slow response to repair: This risk refers to the slow response from the Provider to solve a technical malfunctioning or damage of the efficient system due to natural phenomena, accidents, or factors external to the Provider.
- d) Force majeure event

Several of the risks faced by the solution provider are also impacting the EaaS client; the study outlines these in table 1.

2.2.3 For the EaaS Financier

Several of the risks associated with the Solution provider and the EaaS client impact the financing partner in the project; indeed, any malfunctions may lead to lower expected returns on the investment made. Risks faced by the financing partner typically occur in the second and third phases of EaaS projects: i.e. “the supply, construction, installation” and “Operation” phases; the latter depending on if the financing partner agrees to start funding the project from the start of the construction.

All Risks potentially impacting the Finance Partner are listed in Table 1. In the first column, each risk is also associated with the respective phase of the project it is occurring.

Solution providers shifting to offering EaaS may need some tools to set up a pricing strategy for the new service. The pricing model can support this process, as it provides an estimate for the price per unit of service delivered as well as the expected return of the project. The tool may also be useful for providers to show to interested customers that the EaaS service may offer economic benefits against investments in low- or medium- efficiency equipment.



2.2.4 EaaS project risks: key aspects

| Risk | Description of risk | Party bearing risk under a business-as-usual transaction | Party best positioned to bear the risk | Parties in transaction | Amount of risk borne by party in EaaS | Likelihood | Consequence |
|---|---|--|--|------------------------|---------------------------------------|------------|-------------|
| Tech provider performance risk (Phase 3) | Risk that the equipment underperforms with regards to the projected specifications over the expected/contracted lifetime. | Customer | Tech Provider | Customer | | | |
| | | | | Financier | | | |
| | | | | Tech provider | Full | Mid | Mid |
| Tech provider HW risks (Phase 3) | Any malfunction on solution provider HW. | Customer | Tech Provider | Customer | | | |
| Tech provider SW risks (Phase 3) | Any malfunction on solution provider SW | | | Financier | | | |
| | | | | Tech provider | Full | Mid | Mid |
| Tech provider metering risk (Phase 3) | Risk that the metering device of the solution provider is not functioning properly | NA | Tech Provider | Customer | Partial | Mid | Mid |
| | | | | Financier | | | |
| | | | | Tech provider | Partial | Mid | Mid |
| Tech provider existential risk (Phase 1, 2, 3) | Risk that the technology manufacturer will no longer be solvent/ exist or able to meet the terms of the warranty or provide replacement parts/materials support. | Customer | Tech Provider or Guarantee Provider | Customer | Minority | Low | High |
| | | | | Financier | Majority | Low | High |
| | | | | Tech provider | | | |
| Construction and Completion risk (Phase 2) | Tech provider's cost of implementation as compared with that anticipated at financial close. This may lead to penalties to the tech provider as well (depending on contractual terms), as it may impact the customer. | Tech provider or contractor | Tech provider | Customer | | | |
| | | | | Financier | | | |
| | | | | Tech provider | Full | Low | High |
| Tech provider operation risk (Phase 2, 3) | Supply chain service risk: any replacement of parts are associated with | Tech provider or contractor (if applicable) | Tech provider | Customer | Partial | Mid | Mid |
| | | | | Financier | | | |



| | | | | | | | |
|---|---|---|----------------------------|---------------|----------|-----|------------|
| | supply chain and service team risks. | | | Tech provider | Partial | Mid | Mid |
| Procurement risk / tariff risk (Phase 2) | Risk of delays in procurement processes due to bureaucratic delays or changes to the tariff environment as a transaction is ongoing. | Tech Provider or contractor (if applicable) | Tech Provider | Customer | | | |
| | | | | Financier | Minority | Low | Low |
| | | | | Tech provider | Majority | Low | High |
| Unanticipated maintenance risk (Phase 3) | Risk of much greater maintenance demand than anticipated for the customer. | Customer | Tech provider | Customer | | | |
| | | | | Financier | | | |
| | | | | Tech provider | Full | Low | Mid |
| Service continuity risk (Phase 3) | Risk that equipment cannot be operated due to power outage or that equipment is inoperable due other business interruptions (geography dependent) | Customer | Customer | Customer | Partial | Low | High |
| | | | | Financier | | | |
| | | | | Tech provider | Partial | Low | High |
| Customer change risk (Phase 3) | Depending on the application there is a risk that the customer paying for the service changes: for instance, if the owner of a building changes. | Tech provider | Tech provider | Customer | | | |
| | | | | Financier | | | |
| | | | | Tech provider | Full | Mid | Mid |
| Failure of counterparty infrastructure (Phase 2, 3)) | Risk that the interface between the tech provider and the customer is not ideal. | Tech provider or contractor or customer | Tech provider and Customer | Customer | | | |
| | | | | Financier | Partial | Low | Mid |
| | | | | Tech provider | Partial | Low | High |
| Residual value risk (Phase 3) | When the equipment is returned before it is fully depreciated. | Tech provider, financier | Tech provider | Customer | | | |
| | | | | Financier | Partial | Mid | Mid/ High |
| | | | | Tech Provider | Partial | Mid | Mid / High |
| Balance Sheet risk (Phase 2, 3) | The balance sheet of the company changes considerably shifting from selling a product to selling a service. | Tech provider | Tech provider | Customer | | | |
| | | | | Financier | | | |
| | | | | Tech Provider | Full | Low | Low |
| Partnership risk (Phase 1) | Potential competition with existing | Tech provider | Tech provider | Customer | | | |



| | | | | | | | |
|---|---|---------------------------------------|---------------------------------|---------------|----------|-----|------|
| | commercial partnerships on the ground | | | Financier | | | |
| | | | | Tech Provider | Full | Low | Low |
| Foreign exchange risk (Phase 3) | Risk of potential foreign exchange losses, when capital is borrowed in foreign currency and revenue is gathered in domestic currency (geography dependent) – not applicable for Europe, except if the investor is non-European. | NA | Guarantee provider | Customer | Partial | Low | Mid |
| | | | | Financier | Partial | Low | Mid |
| | | | | Tech provider | Partial | Low | Mid |
| Counterparty existential risk (Phase 2, 3) | Risk that customers will default on loan/ equipment usage fee payments. | Tech Provider/contractor or Financier | Financier & Technology Provider | Customer | | | |
| | | | | Financier | Partial | Low | High |
| | | | | Tech provider | Partial | Low | High |
| Counterparty demand risk (Phase 3) | Risk that the customer demand goes above contractual agreed levels | Tech provider | Customer | Customer | Majority | Low | Mid |
| | | | | Financier | | | |
| | | | | Tech provider | Minority | Low | Mid |
| Electricity price risk (Phase 3) | Downstream risk of higher electricity prices due to greater generation/distribution/transmission costs and/or greater utility market power (geography dependent). | Customer | Tech provider | Customer | | | |
| | | | | Financier | | | |
| | | | | Tech provider | Full | Low | Mid |
| Policy regulatory and accounting Standards risk (Phase 2, 3) | Risk of policy or regulatory changes that affect recapitalization options and risk of changes in accounting standards. | Tech Provider | Guarantee provider | Customer | | | |
| | | | | Financier | Partial | Low | Low |
| | | | | Tech provider | Partial | Low | High |
| Extreme weather / environmental damage risk (part of Force Majeure) (Phase 2, 3) | Risk that equipment is damaged and requires additional corrective maintenance due to storms/flooding/other extreme weather (geography dependent). | Customer | Tech Provider or customer | Customer | Partial | Low | High |
| | | | | Financier | Partial | Low | High |
| | | | | Tech provider | Partial | Low | High |



| | | | | | | | |
|---|---|----------|----------------------------|---------------|---------|-----|------|
| Other force majeure risks (Phase 2, 3) | Risks related to pandemic, war, terrorist attack, riots, strikes (geography dependent). | Customer | Tech Provider or customer? | Customer | Partial | Low | High |
| | | | | Financier | Partial | Low | High |
| | | | | Tech provider | Partial | Low | High |

Table 1: Risks with EaaS projects

| Scale | Consequence | Likelihood |
|-------|------------------------|-------------------------|
| Low | Insignificant to minor | Rare to unlikely |
| Mid | Moderate | Possible |
| High | Major to Catastrophic | Likely to highly likely |

Table 2: Scale of risks for EaaS projects

2.3 Risk analysis heatmap on the business

Table 1 was analysed in the geographies of Belgium, the Netherlands and Spain. The key risks were summarised in heat maps for each stakeholder as shown below. Please note that these maps are only indicative and risks should be properly evaluated for each project. Within EaaS, these risks will be iterated with field data throughout the project duration.

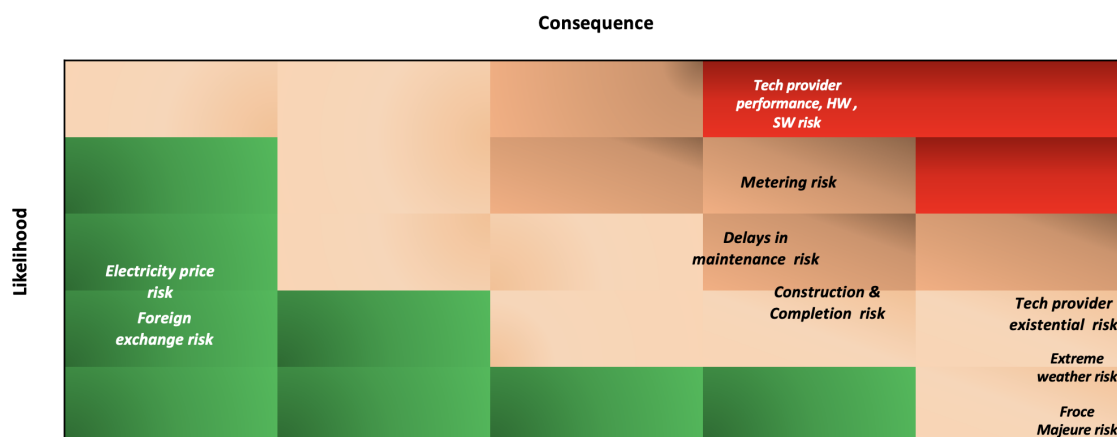


Figure 2: Risk heat map for the customer

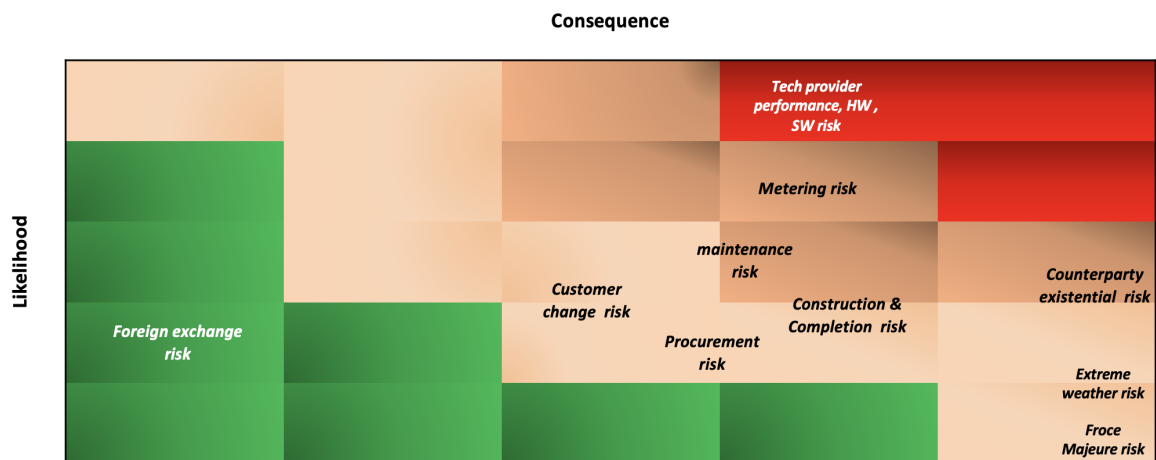


Figure 3: Risk heat map for the solution provider

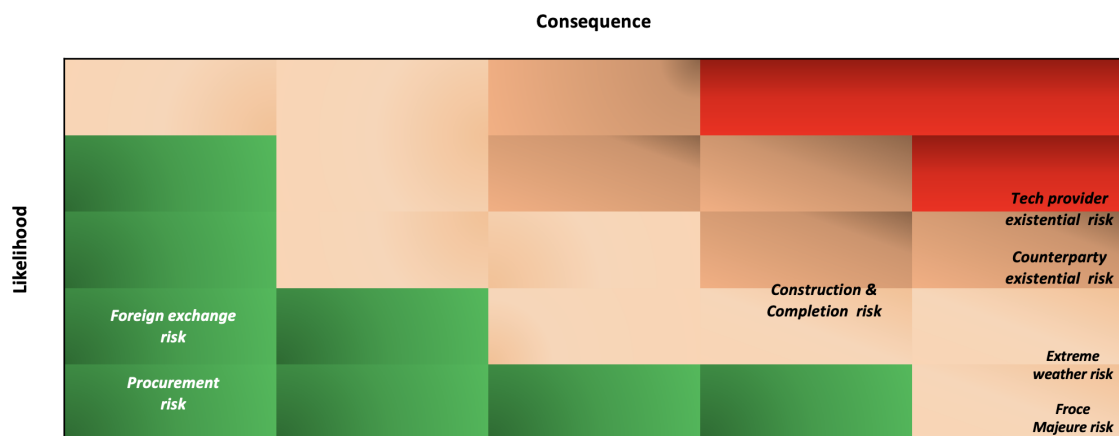


Figure 4: Risk heat map for the financier

Figures 2-3 show that EaaS contracts expose higher risks for the solution provider, who keeps ownership of the equipment. However, it is believed that they are the stakeholder best positioned to properly control these risks with adequate measures.

3. Existing risk analysis tools

Several projects (some EU funded) have focused on developing tools to measure energy efficiency projects' risks. The below sub-section outlines some which are relevant to be reviewed.

3.1 QualitEE

[QualitEE](#), an EU funded project, has provided a toolkit for quality assessment, financial assessment, best practices, and a dedicated procurement handbook for energy efficiency projects that aims to build trust between consumers, suppliers and financiers¹.

3.2 EEFIG tools

The Energy Efficiency Financial Institutions Group (EEFIG) has proposed several tools, amongst them:

- the De-risking Energy Efficiency Platform (DEEP)
- and the underwriting Toolkit²

Cooperation with insurance companies is envisaged as well as with national guaranteed programmes. These include:

- Identify main insurance companies, raising interest and engaging them.
- Provide material for insurance companies' internal evaluation and matching of existing products.
- Negotiate the insurance or guarantee premiums.
- Support insurance or guarantee fund to define the financial conditions and standardise the evaluation and rating practices that may subject an insurer to underwrite a project.

3.3 LAUNCH protocol

The EU H2020 project LAUNCH developed a Risk Assessment Protocol along its standardised contract. The evaluation, called "Risk Assessment Protocol (RAP) V1.3, outlines the set of risks which commonly occur in energy

¹ https://qualitee.eu/wp-content/uploads/QualitEE_D3.3_FinancialGuidelines_200617_e7.pdf

² available at

https://ec.europa.eu/eefig/system/files/2020-11/EEFIG_Underwriting_Toolkit_June_2017.pdf .
EEFIG was established in 2013 by the European Commission Directorate-General for Energy and the United Nations Environment Programme Finance Initiative (UNEP FI)



efficiency projects investment, and also lists guidelines for quantifying the risk levels, who are the best parties to bear the risks and the possible mitigation measures. The RAP V1.3 can be downloaded from the project page.³

3.4 International Energy Efficiency Financing Protocol (IEEFP)

In February 2021, the Efficiency Valuation Organization (EVO) released the International Energy Efficiency Financing Protocol (IEEFP), a Blueprint for financial institutions to evaluate (among other topics) energy efficiency projects risks and possible mitigation options. We highly recommend the reader to review the document available on the website⁴, in addition to table 1 and table 5 on pages 11 and 31 respectively of the referred protocol. Those tables expose how estimated energy savings can be more easily evaluated for one particular equipment compared to another, therefore attributing the risks associated to each energy efficiency measure. For instance, the savings for energy efficient lights are more easily estimated than for energy efficient motors, therefore bearing a lower risk. Table 5 on page 31, exposes the performance risks and mitigation strategies per project phase (as described in figure 1 of this document); some of which are mentioned in the next chapter.

4. Possible mitigation actions

4.1 National guarantee systems (financial)

Within the Private Finance for Energy Efficiency (PF4EE) instrument, which is a joint agreement between the EIB and the European Commission aiming to address the limited access to adequate and affordable commercial financing for energy efficiency investments, the program includes the design of a risk guarantee. This risk guarantee is highly valuable to unlock affordable commercial debt at scale. For more information, please review the information made available on their website⁵.

The PF4EE instrument provides support on three core pillars:

1. a portfolio-based credit risk protection provided by means of cash-collateral (Risk Sharing Facility),
2. a long-term financing from the EIB (EIB Loan for Energy Efficiency)

³ <https://www.launch2020.eu/launch-material>

⁴ <https://evo-world.org/en/products-services-mainmenu-en/protocols/ieefp>

⁵ <https://www.eib.org/en/products/mandates-partnerships/pf4ee/index.htm>



3. an expert support services for the Financial Intermediaries (Expert Support Facility)

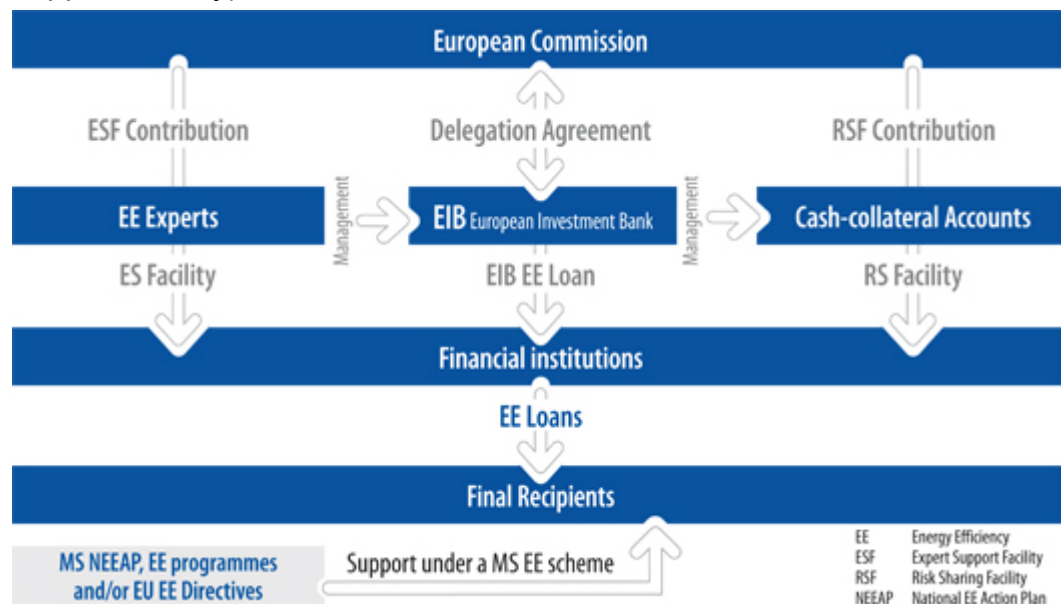


Figure 5: PF4EE instrument

PF4EE is notably implemented with banks in Belgium and Spain, part of the scope of the EaaS initiative, among other countries.

4.2 Insurance products (financial)

HSB is a leader in equipment breakdown insurance & other specialty coverages, inspection services, loss reduction & engineering-based risk management for business, home & farm (more information on their website⁶).

4.3 IEEFP Mitigation strategies

As mentioned in section 3.4, the IEEFP exposes mitigation strategies per project phase for energy efficient equipment. However, please note that these are listed for Energy Performance Contracts (EPC), which are different from EaaS contracts, in the perspective that savings are not guaranteed, but the clients are contractually agreeing to a price per unit of service consumed. Nonetheless, some of the risks and mitigation procedures are valid for EaaS contracts and it is valuable for the reader to study these.

⁶ <https://www.munichre.com/hsb/en.html>

4.4 Other (financial and non-financial)

4.4.1 SLA agreements

SLA agreements, also known as Service Level Agreements, are well known in industry and often requested by customers to protect them from system breakdowns; these are typically used in business-as-usual sales. Aspects of these agreements can be integrated in EaaS contracts to the end customer, whereby a certain level of up-time is guaranteed, and service protocols can be defined.

4.4.2 EaaS assistance

Both technical and financial assistance can be provided to providers looking to implement EaaS contracts. Several companies provide services; the Advanced Servitization Group from the Aston Business School, or Invigors are two firms providing management and financial advice on how to implement Servitisation contracts.

5. Conclusion and disclaimer

Overall, this risk analysis document is useful for solution providers who want to engage with EaaS to properly evaluate the various risks that may occur in such a project.


Since this document is written in a generic format across technologies and industries, it should be used for indicative purposes only. It is highly recommended for providers to compare it to their internal tools, and where applicable integrate factors and methods according to their best internal practises.

Every EaaS project needs a tailored analysis of the present risks, and might require more complex models and functionalities than offered by this tool.

6. Annex: List of key stakeholders interviewed

The consortium would like to share their gratitude to the individuals and organisations that shared knowledge on evaluating the risks of EaaS projects and contributed to the content of this document.





We would like to especially thank two members of the Advisory Board: Iain McKechnie (Director of Strategic Programs at the Advanced Services Group, Aston Business School, University of Birmingham) and Rod Janssen (President, Energy Efficiency in Industrial processes, EEIP) for their insights as well as stakeholders interviewed under the Chatham House Rule and who agreed to disclose their names*

- Simon Lutzenberger, CHG Meridian
- Marc Boeijen, Rikkert Hein, Atradius

