SECURITY ASSURANCE PLAN

Contract number:
Supplier name:[NAME OF SUPPLIER]
Project/contract name:[CONTRACT NAME]
Date of validation of the Committee: *To be defined*

SAP Model Name: *Standard SAP Model V4.1*

Validation

Name	Entity
	TotalEnergies
	[NAME OF SUPPLIER]

Developments

Version	Date	Modification	Author	Entity

SUMMARY

Procedure

The Supplier is expected to comply with the security requirements to which he undertakes. For each requirement, the Service Supplier checks his commitment level in the **blue section** (Yes [compliant], No [non-compliant or N/A]) and provides the details requested in the " Description of the implementation or alternative" section:

- Answers to requirements should be as explicit as possible.
- Any reasons for non-compliance should be described, possibly providing alternative/complementary proposals to meet the requirement as closely as possible.
- If a requirement is "Not Applicable", it will be necessary to provide the reasons related to the context of the service.

TotalEnergies may request clarification of the commitments if responses provided by the Supplier on the compliance of the commitments are considered insufficient.

The **sections in red** are to be completed by TotalEnergies.

1. Presentation of the Security Assurance Plan

1.1 Object

The purpose of the Security Assurance Plan (SAP) is to ensure the implementation of best practices and compliance with totalEnergies' Information System Security framework, in accordance with the rules ISS-005-3.1 "Contracting the outsourcing of an IT service" and ISS-005-5.1 "Control and Monitoring of the outsourced service", in order to ensure the REG-SSI-005 document:

- Compliance with ISS requirements and rules established within outsourcing contract and throughout its duration.
- Formal consideration of changes in contractual documents.
- Ability to TotalEnergies to maintain control of the outsourced services and, more particularly, of the ISS systems implemented.

The SAP describes the service commitments and security assurance provisions made by the Supplier during the Services described in the Contract. This plan guarantees the quality of service in terms of security between TotalEnergies and the Supplier.

1.2 SAP lifecycle

1.2.1 Organization of the management of the Security Assurance Plan

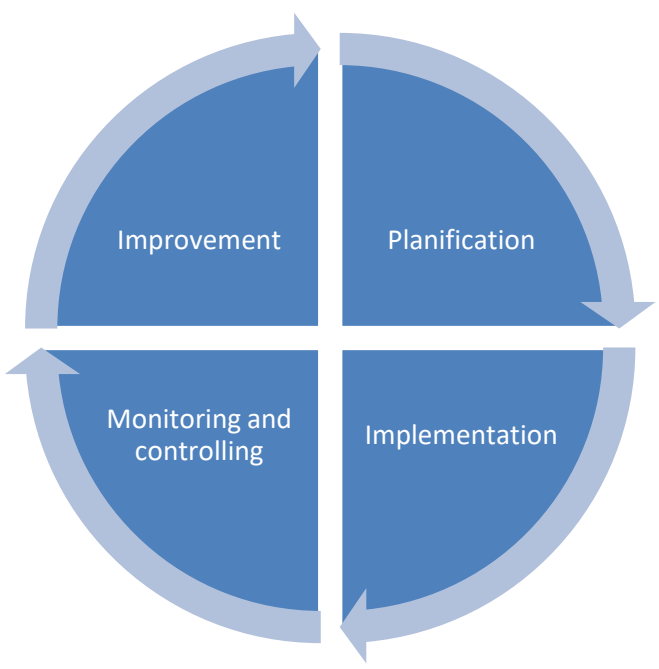
The three main actors involved in the SAP life cycle are:

- The TotalEnergies Information System Security Manager, hereinafter referred to as CSO,
- The TotalEnergies Information System Security Manager for the Contract, hereinafter referred to as CCD,
- The Supplier's Information System Security Correspondent, hereinafter referred to as RESP SEC[NAME OF SUPPLIER].

The CCD has the best overall vision to assess the risks associated with the outsourcing of the delivered services.

The SEC RESP [NAME OF SUPPLIER] is a responsible employee of the Service Supplier, appointed by the latter. He is the privileged TotalEnergies CCD’s priviledged point of contact and acts as an interface between TotalEnergies and the Service Supplier. In addition, the [NAME OF SUPPLIER] SEC RESP is responsible for the Information Systems Security of the Service Supplier and for its possible Subcontractors.

1.2.2 Security Assurance Plan Lifecycle Procedures



1.2.2.1 Establishment of the Security Assurance Plan

The initial drafting of the SAP is carried out in the study phase by the Supplier's SEC RESP in collaboration with the CSO, the CCD and the [NAME OF SUPPLIER] project team. It is based on TotalEnergies‘ information systems security and information safety standards as well as recognized norms and standards (ISO 27001, ISO 27002, etc.).

After taking TotalEnergies’ requirements into account, the [NAME OF SUPPLIER]’s SEC RESP then, writes in the SAP, the application procedures relating to the requirements of the Contract and sends them to the CSO for approval.

The SAP is approved by both parties represented respectively by the CSO for TotalEnergies and by the RESP SEC [NAME OF SUPPLIER] for the Service Supplier. The SAP constitutes an Annex to the Contract.

1.2.2.2 Implementation of the Security Assurance Plan

The SEC RESP [NAME OF SUPPLIER] is responsible for distributing and ensuring the application of the Security Assurance Plan by the different parties involved for TotalEnergies within the teams under the responsibility of the Service Supplier.

1.2.2.3 Monitoring and follow-up of the Security Assurance Plan

The effective implementation and the effectiveness of the measures described in the SAP must be verified by TotalEnergies via control actions implemented by the Service Supplier and via the monitoring of security indicators.

It is the responsibility of the SEC RESP [NAME OF SUPPLIER] to ensure that the SAP is always in line with the expected level of security: any changes which can directly or indirectly impact the overall security level must be reported to the CCD and along with actions to re-establish the expected security level, if required.

The controls are described in the "Security Governance of Information Systems" chapter.

1.2.2.1 Improvements of the Security Assurance Plan

The SAP life cycle is dynamic. Also, the SAP will be subject to updates upon Contract's scope changes. Approvals for the SAP updates can only usually be given by the COSEC committee quarterly meeting, while recurring Services are provided by the Contract. If required, an exceptional revision may be requested and / or suggested during a COSEC.

As a result, any changes impacting the security level must lead to a change in the SAP. All SAP updates must result in a proposal by the SEC RESP [NAME OF SUPPLIER] or the CCD for a new version (minor or major) which must be approved via a process identical to the one described for the initial creation of the SAP and validated at the COSEC. This new version will be broadcasted by the SEC RESP [NAME OF SUPPLIER] to all involved parties.

Any change to the SAP must be entered in the change log at the start of the SAP document.

1.3 SAP Update Process

1.3.1 Evolution and approval procedure

All changes to the Security Assurance Plan are subject to the provisions of Article "Changing the contractual documents" of the Framework Contract.

1.3.2 Diffusion

The distribution of a new, signed version cancels and replaces the previous version.

The two parties signing the SAP commit to communicate the objectives and provisions of the SAP to their underlying parties involved in providing the Service. This action is the responsibility of the signatories.

1.4 Description of the service

Service Manager	
Contract Manager	
Description of the service *What is the typology of the service, what does it consist of?*	
Type of contract	☐ Type 1: Supply of goods or services involving privileged access to the Company's assets ☐ Type 2: Supply of "sensitive" goods or services ☐ Type 3: All other supplies of goods or services

1.5 Scope of application

1.5.1 Scope of service (including technical environments)

Which is the role of the Service Supplier?	☐ Functional (intellectual service, business project management support, etc.) ☐ Administration (outsourcing) ☐ Hardware maintenance ☐ Development (including software maintenance) ☐ Other *Specify:*
What applications, services and/or materials fall within the scope of the service?	*Specify here*
Which workstations are used by the Service Supplier?	☐ TotalENERGIES Workstations ☐ Service Supplier workstations ☐ Other. Please specify:

Does the Service Supplier have remote access to the TotalEnergies IS?	☐ No ☐ Yes. In this case, how does the Service Supplier access the TotalEnergies IS? *Please specify:*
Does the Service Supplier IS interconnected with TotalEnergies IS ?	☐ No ☐ Yes. Please *specify*:
Are the exchanges secure? *(VPN, encryption, etc.)*	☐ No ☐ Yes. Please *specify*:
Are the Service Supplier's teams dedicated to the provided service?	☐ Yes ☐ No. Please *specify*:
Does the service Supplier have to handle TotalEnergies' data?	☐ No ☐ Yes. Please *specify the type of data and purpose*:
Does the service Supplier have privileged accounts on TotalEnergies' IS?	☐ No ☐ Yes. Please *specify* :

1.5.2 Lists of service sites

Sites	**Description**
TotalEnergies sites	

Service Supplier Sites		Is part of the site dedicated to TotalEnergies?
		☐ Yes ☐ No.
		☐ Yes ☐ No.
		☐ Yes ☐ No.

2. Security Governance of Information Systems

2.1 Security organization

The management of the contract security activities implies the following roles and responsibilities:

The CSO- Chief Information Security Officer at TotalEnergies

- Responsible for the ISS at TotalEnergies during the Contract,
- Informs the TotalEnergies Contract Manager about the operation of the ISS,
- Responsible for the application of the ISS, together with the Suppliers, and reports any ISS non-compliance,
- Attends security committees.

The CCD - Chief Information Security Officer for the Contract at TotalEnergies

- Defines with the SEC RESP [NAME OF SUPPLIER] the ISS resources and the organization during the Contract period,
- Reports to the CSO of TotalEnergies,
- Informs the TotalEnergies Contract Manager about the operation of the ISS,
- Acts as the interface for IS security incidents on behalf of the Technical Domain, for which he is responsible at TotalEnergies,
- Responsible for the ISS implementation in the Technical Domain which he is in charge at TotalEnergies, together with Suppliers, and reports any ISS non-compliance to the CSO.

The SEC RESP [NAME OF SUPPLIER] - Information Security System Correspondent of the Supplier

- Manages the Supplier's ISS governance organization for the Contract,
- Ensures that all of the Service Supplier's ISS commitments to TotalEnergies are carried out,
- Has authority over the local centers' managers for the ISS,
- Responsible for agreeing the schedule of the annual unannounced penetration test (no communication will take place with the operational staff). This will be funded and carried out by the customer, the SEC RESP [NAME OF SUPPLIER] will receive notification upon completion of the test by the CCD security officer,
- Responsible for the communication of the test and its outcome to the operational teams impacted and the COSEC Security Committee,
- Reports directly ISS results to the CSO and CDD,
- Defines the guidelines and ISS resources to fulfill the commitments,
- Implements the SAP measures around the perimeter of the Services, specifically:
    - Organizes training and awareness-raising to the parties involved,
    - Closely monitors staff movements to ensure fine grained access to the TotalEnergies Information System,
    - Analyzes the periodic security incident report with the CCD,
    - Provides the SAP indicators and their analysis at each security committee,
    - Prepares the security committee agenda and the meeting report within five (5) business days following the meeting, at the latest.

Service Center local security manager of the Supplier (local correspondent - SEC RESP [NAME OF SUPPLIER] LOCAL) (The role eventually given by the SEC RESP [NAME OF SUPPLIER] or another person on the local site)

- The local correspondent is under the authority of SEC RESP [NAME OF SUPPLIER] for security issues in the scope of the SAP as part of the execution of the Contract,
- Provides on its area, by delegation of the SEC RESP [NAME OF SUPPLIER], missions equivalent to those of the SEC RESP [NAME OF SUPPLIER] .
- In particular,
    - Organizes information security training and awareness-raising to the parties involved,
    - Closely monitors staff movements to ensure fine grained access to the TotalEnergies Information System,
    - Participates in the security incident management, with the SEC RESP [NAME OF SUPPLIER] and the CCD,
    - Provides elements on its site for the SAP security indicators,
    - Carries out the various reports and security controls related to his site.

Supplier Security Auditors

- Are under the security manager's responsibility [NAME OF SUPPLIER] and report directly to him,
- Conduct security penetration tests within the Supplier's service infrastructures to check the compliance with ISS standards.

TotalEnergies Security Auditors

- Are sponsored by the CSO,
- Perform security controls on the service infrastructures to check compliance with ISS standards,
- May intervene in the service centers of the Service Supplier according to the terms defined in section "Specials for security audits" of the Framework Contract.

Note: Other TotalEnergies involved parties (Internal Control and DAG auditors, etc.) or Service Supplier staff (SOX / SAS70 / ISAE3402 or quality auditors) can carry out audits on specific areas of the scope within the context of audits regarding the Framework Contract. Although they sometimes request assistance from company staff members for related aspects, they are not part of the Contract security organization.

TDM (Technical Domain Manager)

- Technical Domain Manager TotalEnergies

[NAME OF SUPPLIER] team:

- [NAME OF SUPPLIER] team (see role [NAME OF SUPPLIER] described in the QAP)

Document to be provided	**Directory of security contacts** *This document is the nominative list of the actors of security governance and their contact details. These updates must be communicated to the safety committees.*

2.2 Security management

The Service Supplier must provide, implement and maintain an Information Security Management System (ISMS) within their own organization. This management system must ensure the appropriate security level of IS resources used within the framework of the Contract with TotalEnergies.

A Chief Information Security Officer must be appointed by the Service Supplier (in coordination with the CCD or the CSO). This manager will be given the title of SEC RESP [NAME OF SUPPLIER]. Note that they can have other responsibilities than IS security management, depending on the context. However, this SAP describes their activity as the SEC RESP [NAME OF SUPPLIER] for the Contract.

If the Supplier has several service centers, each center must appoint a local security manager who will report to the SEC RESP [NAME OF SUPPLIER].

2.3 Security committee (COSEC)

The entire service must be covered during the COSEC.

The standard agenda for the past period is:

- Analysis of SSI management indicators.
- Follow-up of security action plans (*).
- Detailed analysis of the incidents of the period and remediations.
- Evolutions of the SAP.
- Possibly analysis of changes in the security architecture, related risks and countermeasures.
- Follow-up of derogations.
- Follow-up of the deviation sheets to the non-compliance with the SAP.
-

(*) Including awareness-raising and training actions, control actions and reviews carried out.

A committee presentation support is necessary for the COSEC. It must be provided 5 working days before by the Service Supplier. At the end of the COSEC, a report must be drawn up by the Service Supplier 5 working days after the committee and then, validated by the CCD within 5 working days following delivery.

COSEC must be planned at least one month in advance.

TotalEnergies COSEC attendees	[NAME OF SUPPLIER] COSEC attendees
• CSO or his representative; • CCD; • Responsible for the service or service.	• SEC RESP [NAME OF SUPPLIER]; • Operational Manager of Services; • Contract manager.

COSEC's frequency	COSECs are carried out on a Choisissez un élément. basis or on demand in the event of a security problem identified (exceptional COSEC).

2.4 RACI Matrix

The matrix below is a variation of the safety chapter of the general RACI matrix presented in the AQP of this contract. This matrix presents the details of the responsibilities, the CSO TotalEnergies being responsible for monitoring the application of all safety rules.

	CSO	**CCD**	**SEC RESP [NAME OF SUPPLIER]**	**Local correspondent (LOCAL SEC RESP [NAME OF SUPPLIER])**	**RESP SERVICE**	**[NAME OF SUPPLIER] team**
Definition of the ISS resources to be implemented in the Service Centers of the Supplier	C	C	A/R	R		
Definition of the Service Supplier's IS security policy applied to the Contract [CONTRACT NAME]	C	C	A/R	R		
Definition of the Service Supplier's security procedures applied to the Contract [CONTRACT NAME]	C	C	A/R	R		
Definition of the Service Supplier's security guidelines applied to the Contract [CONTRACT NAME]	I	I	A/R	R		
Verification of the ISS audits	I	I	A	R		
Supervision of security events	I	I	A/R	A/R		
ISS dashboard dedicated to TotalEnergies	I/R	I/R	A/R	R		
Security incident management	C	C	A	R		
Exception management	I	I	A	R		
Connectivity & connectivity architecture revision	I	I	A	R		
Staff training	I	I	A	R		
Staff exits and position changes management	I	I	A	R	R	R
Vulnerability management	I	C	A/R	R	R	R
Definition of the vulnerability management process						

Legend:

- **(R)**: Responsible
- **(A)** Accountable
- **(C)** Consulted
- **(I)** Informed

3. Implementation of security measures

The purpose of this section is to describe all the security measures implemented by the Service Supplier to meet TotalEnergies requirements.

Certain measures will be monitored by indicators and checked during COSEC.
The summary of the indicators is available in Appendix 4.1.
It describes the expectations of TotalEnergies and how the indicators will be implemented by the Service Supplier.
The requirements listed below are repeat of the cybersecurity requirements defined by TotalEnergies.

3.1 Resources management

3.1.1 Classification of Contract specific resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

***Requirement 1**: "The Supplier must identify the various Contract-Specific Resources and establish, in collaboration with the Customer and based on the Customer's reference system, a Classification of these Resources."*

The objective of this requirement is to control implemented measures to ensure the identification, classification and monitoring of sensitive data carriers and equipment (encryption boxes, firewalls, etc.).

Is the requirement applicable in the context of the provided service?	**☒ Yes No☐**
Justification	
Time of control in the contract lifecycle	At the start and during the modification of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes No☐	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Please describe here*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.1.2 Map Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

***Requirement 30**: "Supplier must map the Contract-specific Resources implemented under the Contract in the form of architectural schematics and must maintain an inventory detailing the main features necessary to maintain security.*

This mapping must be validated by the Security Committee."

The objective of this requirement is to ensure that [NAME OF SUPPLIER] maintains up to date the inventory of resources and architectural schematics.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the modification of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No

Description of the implementation or alternative	*Please specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	Architectural diagram Inventory of resources	
TotalEnergies reference document	N/A	

3.1.3 Maintain contract-specific resource mapping up to date

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 31: "*The Supplier must maintain the mapping of the Contract-specific Resources up to date.*

Major changes must be presented to the Security Committee within a sufficient and reasonable time before being implemented."

The objective of this requirement is to check that the mapping of the [NAME OF SUPPLIER] resources specific to the Contract is kept up to date.

Is the requirement applicable in the context of the service?	**☒ Yes No☐**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.1.4 Train actors on the classification of Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 32: *"The Supplier must train any actor involved in the use or management of the Contract-Specific Resources on the Classification Profile of these Resources. Administrators must master with the applicable Security Measures."*

The objective of this requirement is to ensure that stakeholders are aware of the sensitive resources identified in the contract and that administrators master the security measures defined to protect the resources.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No

Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.2 Cybersecurity Risk Management

3.2.1 Analyze Cybersecurity Risks on Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 2: *"The Supplier must carry out and keep up-to-date Cybersecurity Risk Analysis of the Contract-Specific Resources, including the data processed by these Resources, according to a mutually agreed method of analysis.*

The Supplier must be able to provide at any times a detailed report on all the Risks identified, classified by sensitivity, the means of prevention or mitigation and to reveal the residual Risks."

The objective of this requirement is to verify that the perimeter covered by the contract has been the subject of risk analysis, and that for each risk identified corresponds a security measure.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	Analysis report of the cyber risks regarding the contract	
TotalEnergies reference document	N/A	

3.2.2 Apply an action plan to reduce the identified risks

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 3: *"The Supplier must put in place, at its own expense, an action plan in connection with the analysis of Cybersecurity Risks, or the results of a Cybersecurity Audit, to reduce or prevent the occurrence of these Cybersecurity Risks or to limit their consequences. The Supplier must implement the necessary remediation measures following the notifications by the Customer as part of its data leakage program."*

The objective of this requirement is to control that cybersecurity risks are addressed through a corrective and preventive action plan.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	Plan of cyber actions associated with the contract	
TotalEnergies reference document	N/A	

3.3 Cybersecurity Awareness and Training

3.3.1 Raise awareness of Cybersecurity among personnel

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 4: *"The Supplier must conduct awareness-raising actions among the personnel involved in the performance of the Contract (including subcontractors), to ensure that they are aware of the Cybersecurity rules to be applied to ensure the protection of the Contract-Specific Resources."*

The purpose of this requirement is to ensure that the process of staff awareness of Cybersecurity is in place throughout the contract.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-4: Percentage of stakeholders who have followed a cyber awareness less than a year	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.3.2 Train your staff on cybersecurity issues

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 33: *"The Supplier must ensure that the employees assigned to the performance of the Contract (including subcontractors' stakeholders) acquire the knowledge and skills required for the performance of the tasks entrusted to them and the issues related to Cybersecurity.*

The Supplier must undertake the necessary training actions to maintain the skills of all employees and stakeholders concerned.

The Supplier must, on request, provide evidence of the existence of an awareness and training program"

The objective of this requirement is to control that a cybersecurity awareness and training program has been put in place for the contract's stakeholders.

Is the requirement applicable in the context of the service?	**☒ Yes ☒ No**
Justification	

Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-33: Percentage of stakeholders who have completed a cyber training/certification.	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.4 Fight against Malicious Code

3.4.1 Protect Contract-Specific Resources against Malicious Code

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 5: *"The Supplier must put in place, for its Contract-Specific Resources, a protection device against the Malicious Codes."*

The objective of this requirement is to control that it is committed to equipping servers and workstations with an anti-virus and an EDR.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-5: Percentage of systems with anti-virus solutions in place and up to date.	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.4.2 Manage Malicious Code Incidents

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 6: *"The Supplier must define and implement processes and procedures for the managing Threats and Malicious Codes. The Supplier is required to comply with its contractual and legal obligations about reporting Security Incidents to the Customer, including the breach of personal or non-personal data."*

The objective of this requirement is to control that the treatment of malicious code is well formalized.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	

Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.4.3 Provide a periodic status of how to combat malicious code

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 38: *"The Supplier must regularly present to the Security Committee a quantitative (completeness) and qualitative (effectiveness) monitoring report of the means of combating Malicious Code deployed to protect the Contract-Specific Resources, according to a periodicity to be defined at the time of the firs Security Committee."*

The purpose of this requirement is to control that the relationship for the protection of the resources specific to the contract is produced by [NAME OF SUPPLIER].

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.5 Security for systems, workstations and nomadic equipment

3.5.1 Harden the base systems for Contract-Specific resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 7: *"The Supplier must implement the necessary and relevant technical, human, and organizational Measures, to ensure the security of the base Systems (operating Systems, middleware, applications and related communication and security services) of the Contract-Specific Resources. These Measures must make it possible to preserve the confidentiality, availability and integrity of the data processed."*

The objective of this requirement is to verify that the measures to secure the base systems of the resources specific to the contract are well formalized.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**

Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.5.2 Protect Contract-Specific Resources data

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 8: *"The Supplier must document and implement the necessary and relevant means to secure the administration, maintenance, and operation of the System bases (operating Systems, middleware, applications and related communication and security services) of the Contract-Specific Resources."*

The objective of this requirement is to verify that the measures to secure operations are well formalized.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.5.3 Secure the mobile devices used under the Contract

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 9: *"The Supplier must ensure the existence of specific and appropriate Measures for the security of its mobile devices (all types of connected equipment) used by its personnel (and/or those of its subcontractors) in the context of the execution of the Contract."*

The objective of this requirement is to ensure that the protection measures for mobile terminals are well formalized.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	

Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.5.4 Secure the workstations used under the Contract

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 39: *"The Supplier must ensure the hardening of the workstations used by its personnel (and/or subcontractors) in the context of the performance of the Contract so that this equipment does not constitute a vector of breach of the security of the Resources used for the performance of the Contract (e.g. theft of equipment resulting in the disclosure of confidential information or the loss of essential data, the propagation of Malicious Code or the logical intrusion and illicit access to sensitive Resources)."*

The purpose of this requirement is to control that [NAME OF SUPPLIER] 's workstations used by its staff are secured to prevent the loss, damage, theft, or compromise of equipment.

Is the requirement applicable in the context of the service?	**☒ Yes No☐**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes No☐	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.6 Security of computer media

3.6.1 Protect network access used under the Contract

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 11: *"The Supplier must deploy and update the security Measures, necessary, relevant, and in accordance with the State-of-the-art, to ensure the security of the networks used by the Contract-Specific Resources, to prevent or limit the consequences of Cybersecurity Risks."*

The objective of this requirement is to control that [NAME OF SUPPLIER] manages and controls the networks used by the Contract-Specific Resources in order to protect the information contained in the Systems and applications.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**

Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.7 Administration of Contract-Specific Resources

3.7.1 Use the means of Authentication made available

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 12: *"The Supplier will use the means of Authentication made available by the Company to access the Customer's Information Systems.*

The means of Authentication to access the Contract-Specific Resources must be previously validated by the Customer."

The objective of this requirement is to verify that the authentication procedure for the Contract-Specific Resources is well formalized and validated by the Customer.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.7.2 Track Administrator Actions on Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 42: *"The Supplier must ensure that the actions of the administrative accounts used on the Contract-Specific Resources are logged, retained for a default period of twelve (12) rolling months, and that Events are Audited for suspicious activities or actions."*

The purpose of this requirement is to control that the actions of administrators are monitored and that any suspicious actions can be detected.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At start-up and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.7.3 Empowering Directors

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 56: *"The Supplier must ensure that its personnel (and those of its subcontractors) assigned to administrators' functions are held accountable for its actions carried inherent in the privileges granted.*

The process of hold administrators accountable of their actions must be formalized (documented) and traceable."

The objective of this requirement is to verify that the approach to administrative accountability has been formalized in the Security Assurance Plan.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.7.4 Protect passwords for Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 57: *"The personnel assigned to the Contract must protect their passwords and their means of Authentication, in accordance with the methods validated by the Security Committee and alert without delay the Security Operation Center (SOC) of the Customer in case of compromise or suspicion of compromise."*

The objective of this requirement is to verify that the means used for authentication (passwords and other factors) are well secured and that in the event of an incident, [NAME OF SUPPLIER] is able to report it to the Customer's SOC.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.7.5 Secure Contract-Specific Resource administration flows

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 58: *"The Supplier must use the means and methods of access validated by the Security Committee to administer the Contract-Specific Resources.*

The Supplier undertakes not to attempt to circumvent the Security Measures put in place by the Client."

The objective of this requirement is to control that the methods to access resources for carrying out activities are formalized in the Security Assurance Plan.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.8 Remediation Management

3.8.1 Address Vulnerabilities in Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 13: *"The Supplier must define and implement a Remediation process to correct vulnerabilities and misconfigurations of The Contract-Specific Resources."*

The objective of this requirement is to control that [NAME OF SUPPLIER] is able to manage vulnerabilities and configuration defects of the Contract-Specific Resources.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.8.2 Provide reporting on Remediation actions within the scope of the Contract

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 43: *"The Supplier must draw up and provide, according to the terms and frequency defined in the Security Insurance Plan, the reports defined by the Security Committee."*

The objective of this requirement is to verify that the reporting on remediation actions is well defined in the Security Assurance Plan and that the remediation reports are well produced.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At start-up and during EC COS

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.8.3 Coordinate Remediation within contractual deadlines

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 44: *"The Supplier must implement the necessary means to apply the Remediations on the Contract-Specific-Resources, within the deadlines defined in the Security Insurance Plan for the Vulnerability Levels "Critical" or "P0", "Urgent" or "P1", and Standard (default).*

The P0 and P1 remediations are defined by the CERT TotalEnergies and communicated to the Supplier."

The objective of this requirement is to verify that the remediation process is defined and applied within the requested deadlines.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-44: Percentage of vulnerabilities (P0 and P1) addressed on time.	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.9 Logical access controls and entitlements

3.9.1 Apply an authorization procedure for access to Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 14: *"The management of logical access to Contract-Specific Resources, implemented by the Supplier for the purposes of the Contract, must be described in a Security Assurance Plan (if any) or in a document sent to the Customer before the start of the Services/Supply and each time it is updated.*

Access to the Customer's Information System is subject only to the Customer's rules and procedures."

The objective of this requirement is to verify that the procedure for managing logical access to The Contract-Specific Resources is well formalized and validated by the Customer.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.10 Cybersecurity Incident Management

3.10.1 Alert in the event of a Major Security Incident

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 15: *"Major Security Incidents must be reported to the CERT TotalEnergies within four (4) hours from the moment the Supplier becomes aware of them, specifying in particular the nature and extent of the Major Security Incident, proven and potential, as well as any information to enable the Customer to assess the consequences for himself.*
The Supplier actively collaborates with the Customer and regularly updates and completes this information."

The purpose of this requirement is to verify that [NAME OF SUPPLIER] responsibilities and procedures have been established and effective procedures in place to report information to CERT within the time limits set in the event of a major incident.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.10.2 Respond to requests from a crisis unit of the Client

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 16: *"The Supplier must have a crisis management organization allowing it to respond to requests from the Customer's crisis unit as soon as possible"*

The objective of this requirement is to control that [NAME OF SUPPLIER] is able to communicate with the Client's crisis unit

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.10.3 Report Cybersecurity Incidents

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 49: *"The Supplier must notify the CERT TotalEnergies of any incident affecting or likely to affect the Cybersecurity of the Contract-Specific Resources, within the deadlines and according to the terms agreed contractually or in application of a regulation, this period being fixed in default at a maximum of twenty-four hours from the moment when the Supplier becomes aware of the Cybersecurity Incident"*

The objective of this requirement is to control that the service Supplier cyber alert system is in place and that it is able to meet deadlines.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-49: Average cyber incident alert time	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.10.4 Implement a Cybersecurity Incident Management Process

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 50: *"The Supplier must put in place the technical, human, and organizational means to detect, alert, support and remedy Cybersecurity alerts or Incidents, and in particular to report to the Customer Cybersecurity Incidents concerning the Contract-Specific Resources or the Customer Data used under the Contract, to react effectively according to the nature and severity of the Incidents detected, to limit their impacts and to resolve quickly and formally all Cybersecurity Incidents"*

The purpose of this requirement is to control that the Supplier's detection device in the event of a cybersecurity incident is implemented.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-50: Average cyber incident handling time	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.10.5 Implement a CERT

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 51: *"The Supplier must describe in the Security Insurance Plan its response organization to a Cybersecurity Incident, equivalent to an organization of a CERT (Computer Emergency Response Team) for the monitoring and response to Cybersecurity Incidents involving Contract-Specific Resources that are not integrated into SOC and CERT devices of TotalEnergies. It designates a contact point capable of reporting to the CERT TotalEnergies.*

The Supplier must establish a communication protocol between its CERT and that of the Customer."

The objective of this requirement is to verify that the Supplier's SOC and CERT organizations are well connected to the Customer's SOC and CERT.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.10.6 Provide reporting on Cybersecurity Incidents

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 64: *"The Supplier must reports relating to CyberSecurity Incidents up to date and submit them to the Customer according to the periodicity and with the information provided for in the Security Insurance Plan."*

The objective of this requirement is to verify that the incident report is produced for each COSEC.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	Cybersecurity Incident Report	
TotalEnergies reference document	N/A	

3.11 Business Continuity

3.11.1 Ensure availability of Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 17: *"The Supplier must assess the Risks of unavailability of the Contract-Specific Resources that could be detrimental to the Customer.*
The Supplier must implement solutions (technical, human, and organizational) covering the scenarios of unavailability identified, and making it possible to ensure the minimum level of service required by the Customer in a crisis situation and the resumption of service under conditions that comply with the tolerance thresholds defined with the Customer."

The objective of this requirement is to monitor the organizational and technical means that [NAME OF SUPPLIER] has implemented to guarantee continuity of the service in the event of the unavailability of its IT resources.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**	
Justification		
Time of control in the contract lifecycle	At the start and during the evolution of the contract	

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.11.2 Document the continuity of business related to the Contract

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 18: *"The Supplier must carry out systematic tests of its organizational, human, and technical solutions for ensuring business continuity and disaster recovery, at the end of their implementation or evolution, supplemented by tests and regular exercises to evaluate the functioning of all the continuity and disaster recovery plans that it has defined.*
The Supplier must obtain the Customer's written consent before conducting any tests and exercises based on a partial or complete and programmed shutdown of the Contract-Specific Resources or its other Resources necessary for the Supply (including any switch to backup systems).
All testing and exercises of disaster recovery and business continuity devices must follow protocols documented by Supplier. Their execution must be the subject of a balance sheet showing the results in accordance with expectations and /or anomalies detected, which the Supplier must transmit to the Customer and which will be commented in Security Committee meeting."

The purpose of this requirement is to verify that a business continuity plan for the contract has been implemented.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**	
Justification		
Time of control in the contract lifecycle	At the start and during the evolution of the contract	

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	

Document to be provided	N/A
TotalEnergies reference document	N/A

3.11.3 Emergency backup

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 Type 3☐

Requirement 52: *"The Supplier must carry out separate production backups and backup backups covering all the Contract-Specific Resources (configuration of System, network and telecommunications equipment, basic software, applications, and Customer data).*

The Supplier must outsource the backup (used as part of the execution of continuity plans) to a location sufficiently distant from the production site not to suffer damage from a disaster that could impact it. The Supplier must ensure the ability to permanently access all emergency backups, regardless of their storage location."

The objective of this requirement is to control that the means for backups (for production and emergency) are formalized and implemented.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**	
Justification		
Time of control in the contract lifecycle	At start-up and once a year during the contract	

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.12 Collaborative tools & shared spaces

3.12.1 Favor the use of collaboration tools

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 19: *"In its exchanges with the Customer, the Supplier must use, as far as possible, the collaborative work tools suggested or made available to it by the Customer. In certain cases, in particular for reasons of confidentiality, the Supplier will be obliged to use the collaborative work tools of the Client."*

The objective of this requirement is to ensure that the rules associated with the use of messaging and collaborative tools will be respected by stakeholders.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:**

		Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.12.2 Delete e-mail messages and documents related to the Contract at the end of the Contract

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 20: *"Unless otherwise stipulated in a contractual document that takes precedence over these requirements and unless there is a mandatory legal obligation or for the purposes of certifying the product or service that is the subject of the Contract, the Supplier must delete from its own Resources, including Contract-Specific Resources, Customer Data and electronic messages and documents, within a maximum period of one month from the termination of the Contract for any reason whatsoever."*

The purpose of this requirement is to verify at the end of the contract that the information and documents belonging to TotalEnergies will be destroyed unless mutually agreed.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**	
Justification		
Time of control in the contract lifecycle	At the end of the contract	

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.12.3 Comply with rules governing messaging and collaborative tools

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 Type 3☐

Requirement 21: *"The Supplier must comply with the rules of good practice associated with messaging and collaborative tools provided to it by the Customer."*

The objective of this requirement is to ensure that the rules associated with the use of messaging and collaborative tools will be respected by stakeholders.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by[NAME OF SUPPLIER]?	☒ Yes ☐ No
Description of the implementation or alternative	*Specify*

Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.12.4 Protect documents used under the Agreement

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 53: *"The Supplier must ensure that all data and documents relating to the Customer (including Customer Data or those generated by the service defined in the Contract or inventory data) remain on the dedicated and secure environments defined in the Security Insurance Plan.*

The transfer of data or documents outside these environments is strictly prohibited. In particular, the documents and messages exchanged under the Contract must not be communicated to third parties without the prior consent of the Customer."

The purpose of this requirement is to ensure that the Customer's documents made available to the Supplier are protected in the manner described in the Security Assurance Plan.

Is the requirement applicable in the context of the service?	**☒ Yes No☐**
Justification	
Time of control in the contract lifecycle	At start-up and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes No☐	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.12.5 Encrypt e-mail messages

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 54: *"The Supplier must encrypt the messages exchanged with the Customer, according to the means described in the Security Assurance Plan."*

The purpose of this requirement is to control that the messages exchanged by the Customer and his Supplier are encrypted when the content requires it.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No

Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.13 Cybersecurity Governance

3.13.1 Define Cybersecurity roles and responsibilities

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 22: *"The Supplier must implement Cybersecurity governance to guarantee the level of security expected by the Customer and to meet all Cybersecurity requirements, general and specific, provided for in the Contract and all its annexes. In the event of subcontracting, the Supplier must establish its own governance with its subcontractors.*
This Governance is based in particular on the Supplier's participation in the Security Committee (SECCO) to meet according to the terms defined by the parties in a Security Insurance Plan (SIP).
The topics of the Security Committee will focus on the achievement of the security levels expected of the Customer, the Security Incidents that have occurred, any security derogations impacting the Customer, ongoing Security Incidents, the results of Audits or certifications conducted.
Action plans resulting from Risk analyses or Cybersecurity Audits must be reviewed during the Security Committees.
The processes of Remediation, detection and reaction must be validated by the Security Committee."

The objective of this requirement is to control a governance of the Cybersecurity of the contract has been defined.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.13.2 Appoint a security officer

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 23: *"The Supplier must designate a security officer.*

This security officer is the single point of contact for security throughout the duration of the Contract. It must be easily reachable by the Customer, in a secure manner and the means of communication must be established at the start of the Contract.

The participation of the security officer in the Security Committee is mandatory."

The objective of this requirement is to control that a privileged contact has been defined for the customer for all questions relating to the Cybersecurity of the contract.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.13.3 Appoint a Remediation officer

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 24: *"The Supplier must designate, within its teams, a person responsible for the application of the Remediation, in relation to the Customer."*

The purpose of this requirement is to control that a privileged contact has been defined for the customer for questions relating to remediation.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.14 Supplier Cybersecurity Certifications

3.14.1 Produce qualification evidence

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 25: *"The Supplier must produce any certification / accreditation / label / reference to the Customer supporting its competence, in particular in the Cybersecurity's domain as well as that of its employees and subcontractors within the scope of the Contract. Evidence of defined qualification imposed within a specific regulatory framework must also be made available."*

The objective of the requirement is to control that [NAME OF SUPPLIER] is able to produce its cyber certification list.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.14.2 Maintaining Cybersecurity Qualifications

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 26: *"The Supplier is responsible for maintaining the required certifications, accreditations and labels. Cybersecurity certifications required under the Contract must be valid for at least the duration of the Contract."*

The objective of this requirement is to control that [NAME OF SUPPLIER] has set up a cyber certification program.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.14.3 Notify in case of any loss of qualification

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☒ Type 3

Requirement 27: *"The Supplier must notify the Customer as soon as possible, and at the latest within seven (7) working days, in the event of loss of accreditation, label or certification, whether a "Company" certification or one or more required certifications applying to the personnel, equipment, services or processes of the Supplier or that of its subcontractors."*

The objective of this requirement is to control that the service Supplier's cyber certification losses are well reported to the Customer.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.15 Cybersecurity Audits

3.15.1 Audit the Cybersecurity of Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 28: *"Supplier must conduct Cybersecurity Audits of Contract-Specific Resources.*

These Audits mainly concern compliance with the requirements set out in this document.

They may also relate to the security Measures applicable to specific regulations, such as those applicable to the processing of personal data.

These Audits do not exclude the application of other contractual provisions relating to Audits of the Supplier's Resources and Information Systems, including pen testing / red team Audits. These Audits are the responsibility of the Supplier, unless otherwise agreed in advance by the Parties."

The objective of this requirement is to monitor that [NAME OF SUPPLIER] carry out frequent audits on the resources of the contract to verify compliance with all the requirements of the cyber annex applicable to the contract.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.15.2 Transmit Cybersecurity audit results

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 29: *"The results of the Audits carried out by the Supplier on the Contract-Specific Resources will be communicated to the Customer. An Audit certificate, as well as a summary of the Audit report and the progress of the Remediation and improvement actions, will be given free of charge to the Customer no later than thirty (30) working days after the date of the Audit report. All Remediation and improvement actions will be at the expense of the Supplier."*

The objective of this requirement is to verify that [NAME OF SUPPLIER] transmits audit results of the resources of the contract (reports or executive summary) within the required deadlines.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start of the contract and once a year during the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.16 Categorization of cybersecurity zones

3.16.1 Protect physical access to Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 34: *"The Supplier must ensure that the physical security Measures adapted to the level of sensitivity of the Contract-Specific Resources, including data processed under the Contract, and in accordance with applicable regulations, are in place.*
The Supplier must ensure the protection of physical access to the various security zones in which the Contract-Specific Resources are located by means of graduated and relevant devices depending on the type of zone to be secured.

The Supplier must ensure that the monitoring and control Measures for physical access protection devices are in place."

The purpose of this requirement is to control that [NAME OF SUPPLIER] prevents any unauthorized physical access to Contract Specific Resources, as well as any damage or any intrusion relating to the information and the means of processing the information is prevented.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.17 Protection against environmental risks

3.17.1 Ensure the provision of essential services for Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 35: *"The Supplier must ensure the installation and proper maintenance of the electrical supply, air conditioning and protection of the Contract-Specific Resources."*

The objective of this requirement is to ensure that [NAME OF SUPPLIER] has set in place physical protection measures to properly maintain the power supply, air conditioning and protection devices that guarantee the permanent availability and integrity of the Specific Resources relating to the contract.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.17.2 Fire protection

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 36: *"The Supplier must ensure the implementation of fire safety Measures to protect the Contract-Specific-Resources. These Measures must include, in particular:*

- *Fire detection means.*
- *Fire suppression means.*
- *Measures for periodic verification of the means of protection and firefighting.*
- *Procedures to be implemented in the event of fire.*

The Supplier must communicate to the Customer the list of fire protection Measures put in place."

The purpose of this requirement is to control that the protective measures are put in place by [[NAME OF SUPPLIER] to protect the Resources specific to the Contract against the risk of fire.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	

Document to be provided	N/A
TotalEnergies reference document	N/A

3.17.3 Protection against water damage

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 37: *"The Supplier must ensure the implementation of the water damage protection Measures.*

The Supplier must communicate to the Customer the list of water damage protection Measures put in place."

The objective of this requirement is to control that the protective measures are put in place by [NAME OF SUPPLIER] to protect the Resources specific to the Contract against the risks of water damage.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**	
Justification		
Time of control in the contract lifecycle	At the start and during the evolution of the contract	
Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.18 Traceability and monitoring

3.18.1 Transmit events generated by a Cybersecurity Incident impacting Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 40: *"The Supplier must transmit to the Customer's Security Operation Center (SOC), at first request and within a time frame adapted to the situation that generated the request, all Events associated with a Cybersecurity Incident impacting the Contract-Specific Resources.*

These Events must be addressed to the Customer's technical means of logging."

The objective of this requirement is to verify that [NAME OF SUPPLIER] defined and put in place a process allowing the Customer to request all traces associated with an Incident related to the resources specific to the contract.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**	
Justification		
Time of control in the contract lifecycle	At start-up and during COSEC	
Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.

	Description of the indicator implementation: *Describe*
Document to be provided	N/A
TotalEnergies reference document	N/A

3.18.2 Implement a Security Operations Center (SOC)

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 41: *"The Supplier must monitor through a Security Operation Center (SOC) the Contract-Specific Resources that are not integrated into Customer's SOC.*
The Supplier must establish, at the start of the contract, a communication protocol between its SOC and that of the Customer."

The objective of this requirement is to control that [NAME OF SUPPLIER] is able to monitor resources that are not integrated into the Customer's SOC.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.18.3 Transmit events allowing cybersecurity monitoring of certain Contract-Specific Resources

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 55: *"If necessary, the Security Committee can define the feared Events and detection scenarios (logs, events or detection rules) to be transmitted to the Customer's SOC so that it is able to detect the occurrence. These events generated by Contract-Specific Resources must be addressed to the Customer's log collection systems."*

The objective of this requirement is to ensure that the feared events and associated detection scenarios are well defined in the Security Assurance Plan. These elements must be validated by the COSEC and be regularly updated. COSEC must define the feared events that must be detected by the Customer's SOC, the other events remaining under the responsibility of the Supplier.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:**

		Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.19 Design – carry out - evolution of The Contract-Specific Resources

3.19.1 Specify security measures to meet the requirements expressed by the projects

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 45: *"The Supplier must specify and document the security Measures to be implemented to respond, as part of the design and/or evolution projects of the Contract-Specific Resources, the levels of security and continuity of service required by the Customer.*

The Supplier must alert the Customer of a possible inability to offer Security Measures to meet the required security requirements."

The objective of this requirement is to verify that [NAME OF SUPPLIER] documented all cybersecurity systems and measures applied to the products developed under the contract.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.19.2 Validate the Security implemented measures

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 46: *"The Supplier must proceed, prior delivery, to the technical verification of the Cybersecurity Measures implemented and return these results to the Customer at the end of each control campaign. Where applicable, this report will mention the deviations from the previously validated security specifications and the identified residual security Risks."*

The objective of this requirement is to control that [NAME OF SUPPLIER] has set in place controls to verify the application of the cybersecurity measures defined to reduce the cyber risks of the contract.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No
Description of the implementation or alternative	*Specify*

Indicator(s)	IND-46: Percentage of cybersecurity measures correctly applied	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.19.3 Separate Production Information Systems environments from non-production environments

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 47: *"The Supplier must ensure the separation of the environments of production Information Systems and non-production Information Systems. Production data must not be used in non-production environments without the prior written consent of the Customer."*

The purpose of this requirement is to ensure that production data is not exported and used in vendor test or development environments.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.19.4 Follow secure development best practices

Applicability of the requirement according to the type of contract	☒ Type 1 ☒ Type 2 ☐ Type 3

Requirement 48: *"The programs and applications developed by the Supplier under the Contract must comply with the State of The Art, in terms of security of computer developments and in particular the recommendations of ENISA, ANSSI and OWASP (Open Web Application Security Project). These best practices are described in the Security Insurance Plan and are validated by the Security Committee.*
The Supplier will also apply the principles of "security by design", "security by default", considering, where appropriate, the specificities imposed by the processing of personal data.

The Customer may provide a specific requirements document on Cybersecurity according to the technologies implemented."

The objective of this requirement is to control that [NAME OF SUPPLIER] put in place cybersecurity testing measures in the products (hardware or software) that it develops for the Contract. [NAME OF SUPPLIER] must specify how it applies the principle of "security by design", the recommendations of official bodies and how it complies with any cybersecurity requirements applicable to the technologies implemented.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.20 Management of administrative positions

3.20.1 Ensure that administrator workstations always remain secure

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 59: *"The Supplier must ensure that the workstations used for administration are maintained in a safe condition throughout the duration of the Contract, and in particular kept up to date and free of viruses or Malicious Code in order not to represent a Threat to the Company Information System."*

The objective of this requirement is to control that administrators' workstations are regularly updated (version and patches of the OS) and that they are secured by an XDR (by default that of the Customer).

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At start-up and during COSEC

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	IND-59.1: Percentage of up-to-date administration workstation IND-59.2: Percentage of workstations protected by an XDR solution	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.20.2 Restrict Internet access from administrator's workstations

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 60: *"The accounts of administrators and workstations used for administration must be configured to limit access to the Internet (e-mail, browsing) to the strict needs necessary for the performance of the Contract."*

The purpose of this requirement is to control that the accounts of administrators and workstations used for administration must be configured to limit access to the Internet (e-mail, browsing) to the strict needs necessary for the performance of the Contract.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	

Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.20.3 Apply the principle of least privilege for administrators

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 61: "Supplier's employees (and those of its subcontractors) with administrator rights must have personal and unique accounts (no shared accounts) and respect the separation of roles for administrator actions.

Administrator rights must be assigned and managed in accordance with the principle of least privilege."

The objective of this requirement is to control that [NAME OF SUPPLIER] implements an Identity and Access Management process that complies with the cybersecurity objectives of the contract. In particular, the assignment of administrator's privileges must be governed by a formal process to ensure that privileges are appropriate to their activities.

Is the requirement applicable in the context of the service?	**☒ Yes ☐ No**
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER]?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.20.4 Encrypt administrator workstation data

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 62: *"All storage media used for the administration of the Customer Information System must be encrypted.*

Administrator sessions must be automatically interrupted after a specified period of inactivity and in accordance with the State of The Art."

The objective of this requirement is to control that workstation hard drives and other document storage spaces used to store TotalEnergies documents are encrypted so as not to be exploitable in the event of hardware theft. It must also be checked that a user's session is interrupted after a delay of inactivity of the user.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

3.20.5 Ensure the physical security of administrative positions

Applicability of the requirement according to the type of contract	☒ Type 1 ☐ Type 2 ☐ Type 3

Requirement 63: *"The Supplier must ensure that it implements anti-theft devices and the prevention of visual indiscretions.*

Administrator operations must under no circumstances be carried out in a space open to the public or visible to the public."

The purpose of this requirement is to control that measures are taken to protect the Supplier's workstations against hardware theft or data theft.

Is the requirement applicable in the context of the service?	☒ Yes ☐ No
Justification	
Time of control in the contract lifecycle	At the start and during the evolution of the contract

Is the requirement enforced by [NAME OF SUPPLIER] ?	☒ Yes ☐ No	
Description of the implementation or alternative	*Specify*	
Indicator(s)	N/A	**Frequency:** Choose an item.
	Description of the indicator implementation: *Describe*	
Document to be provided	N/A	
TotalEnergies reference document	N/A	

4. Appendix

4.1 Appendix - Summary of indicators

The purpose of this table is to describe the indicators applicable to the Supplier and the associated thresholds. These are classified on 3 levels:

Indicator	Description	Threshold
IND-4	Percentage of stakeholders who have followed a cyber awareness less than a year	90%
IND-33	Percentage of stakeholders who have completed a cyber training/certification	To be defined
IND-5	Percentage of systems with anti-virus solutions in place and up to date.	0%
IND-44	Percentage of vulnerabilities (P0 and P1) addressed on time	95%
IND-49	Average cyber incident alert time	To be defined
IND-50	Average cyber incident handling time	To be defined
IND-46	Percentage of cybersecurity measures correctly applied	100%
IND-59.1	Percentage of up-to-date administration workstation	90%
IND-59.2	Percentage of workstations protected by an XDR solution	90%

4.2 Appendix - Summary of documents provided by the Supplier

The purpose of this table is to summarize the documents to be provided by the Supplier.
The documents below must be provided before the first COSEC.

Name	Vendor Document Name	Description	Date of dispatch
Schema of architecture			
Inventory of resources			
Cyber risk analysis of the contract			
Cyber action plan associated with the contract			
Cybersecurity Incident Report			

4.3 Appendix - Glossary and Abbreviations

The terms defined below apply only to security requirements – they may in no way be used or used as a reference in the other contractual documents of the Contract.

Terms	Definition
Privileged access	Authorization to access a Resource to perform resource administration operations (e.g. read the configuration, modify the configuration, execute a command reserved for an administrator, delete files ...).
Audit	An Audit verifies the accuracy of the declaration of the means implemented by the Supplier to protect the Resources at the Scope of the Contract. Types of Audits: organizational, compliance, configuration, and technical (intrusion, code review...)
Authentication	Method for verifying the identity of a user to the Information System.
Strong authentication	Authentication based on at least 2 of the following: a secret known to the user only (password, PIN); an object owned by the user (card generating one-time passwords, smart card, USB key); a physical characteristic of the user (fingerprint, retinal fingerprint, hand structure, or any other biometric element).
CERT (Computer Emergency Response Team) TotalEnergies	IT emergency response team responsible for coordinating incident response and cybersecurity assessment between TotalEnergies entities and TotalEnergies subsidiaries. See https://totalenergies.com/cert
Classification	The classification of a Resource by the Customer provides the Supplier with a concise indication of its importance and the need for an appropriate level of protection.

Malicious Code	Any program developed for the purpose of harming or by means of a Computer System or network.
Safety Committee (COSEC)	Decision-making and monitoring body for action plans and Cybersecurity indicators.
Contract	Refers to all the documents governing the contractual relationship between the Supplier and the Customer concerned.
Cybersecurity	All necessary and proportionate technical and organisational measures to protect the Customer's Information Systems and Resources , Contract-Specific Resources, Customer Data, users and third parties that could be impacted, against Events or actions likely to compromise the availability, authenticity, integrity or confidentiality of the aforementioned Information Systems and Resources and the services they offer or make accessible.
Customer Data	Customer Data means the data, including personal data, to which the Supplier has access under the Agreement, as well as the data (including logs and metadata) generated by the Systems.
State of the art	Principles and fundamental notions of the security of information systems described in particular in standards (ISO, IEC) and texts published by official bodies (ANSSI, NIST, ENISA)
Event	Information generated by a component of the Information System that is recorded in a log.
Cybersecurity Incident	Any event found likely to call into question the Cybersecurity or the normal functioning of a Resource of the Information System (or a service provided by the IS function) of the Customer or a Resource Specific to the Contract and likely to affect the availability, integrity or confidentiality of the Resource concerned or a Customer Data.
Major Cybersecurity Incident	Any Cybersecurity Incident with consequences, according to the levels indicated in the Security Assurance Plan.
Threat (Cybersecurity)	Potential cause of a Cybersecurity Risk, which can harm an Information System or an organization.
Measurement (cybersecurity)	Means to manage a Risk, which may be of an administrative, technical, managerial or legal nature, including in particular the policy, procedures, guidelines and organizational practices or structures.
Vulnerability Levels	The CERT defines the vulnerability levels. In general: the Critical vulnerability level or P0 corresponds in particular to the ability of an attacker to perform an action on a Customer Resource with a procedure or tooling made public. The Urgent or P1 vulnerability level corresponds in particular to the execution of a command on a server without publishing a procedure or tooling on the Internet without exploit code or internallyThe Standard vulnerability level corresponds to the other cases.
Security Assurance Plan (SAP)	Document describing the terms of execution of the Contract from the point of view of Cybersecurity. This document describes the Cybersecurity indicators, the Cybersecurity organization and the specific Cybersecurity Measuresput in place.
Classification Profile	The Classification approach, which consists in assigning a value corresponding to the potential impact of the Risks likely to affect the Resources, is analyzed according to the three criteria considered. Each Resource is therefore assigned, for each of the Availability, Integrity and Confidentiality criteria, a sensitivity level (0=Low impact level to 4=High impact level).
Internal Rules	Means the Customer's rules, in particular, any internal rules and procedures specific to the Information System(s) or the Customer's sites transmitted by the Customer to the Supplier or accessible from the Customer's Intranet.
Security Operation Center (SOC)	A Security Operations Center (SOC) is a centralized function within an organization that employs people, processes, and technologies to continuously monitor and improve the organization's security posture while preventing, detecting, analyzing, and responding to Cybersecurity Incidents.
Systems	Means the Customer’s or Supplier's Information Systems used under the Contract.
Information system	Organized set of Resources to process data and provide services. The Information System is essential to the Customer's activities. It includes the Enterprise Information System (EIS) and the Industrial Information System (AIS).
Enterprise Information Systems (EIS)	EIS are Information Systems comprising services and applications intended for the management of the company (office automation, human resources, customer relations, finance, treasury, purchasing, etc.).
Industrial Information Systems (IIC)	IIS are Information Systems comprising Systems and components that contribute directly to production processes, integrity, safety and security of sites (Command Control Systems, Laboratory Management, Technical Management Systems, etc.).
Remediation:	Implementation of security means or measures to resolve errors, flaws, defects or failures in cybersecurity.
Resource (of the Information System)	Includes all or part of the means, services and processes involved in the operation of the Customer Information System, such as applications, data, technical means, equipment, networks (local, corporate, etc.). It is specified that the Resources include the means, services and processes of the Suppliers who participate in the Customer Information System, including Cloud or SaaS service Suppliers, Suppliers in charge of managed or outsourced services, etc.

Contract-Specific Resources	Includes the Resources under the responsibility of the Supplier and its subcontractors that are implemented specifically for the Contract, including in particular the workstations of the employees involved in the Contract and the Resources dedicated to the execution of the Contract.
(Cybersecurity) Risks	A risk is characterized by: • a malicious threat or action, of internal or external origin on Information Systems. • a Threat or a non-malicious action, such as a failure, negligence or error of the Information Systems.

End of document.