

Assessment details

ID 3555

Name GRID BOT

Organisation Southern Europe

Description

Approver Rooman Alam

Respondent Rooman Alam

Template Consulting Cyber Security Plan (Revised V1)

Workflow Default assessment workflow

Creator Rooman Alam

Date created 31/03/2026 11:07

Deadline

Completed date 31/03/2026 11:18

Submitted date 31/03/2026 11:16

Last updated 31/03/2026 11:45

Stage Completed

Approval stage

Status Active

Very high risks 0

High risks 3

Medium risks 2

Low risks 0

Total risks 5

Residual risk level High

Residual risk score 16.0

Result Approved

Result comments

Under Review (Rooman Alam - Approved) ;

Primary record ID 1621

Primary record name GRID BOT

Template version 1

Open risk count 5

Open info request 0

Tags

Submission Progress (%) 71

Assessment questions

1 Project Details

1.1 Please identify the system in scope for the project.

Please identify the system in scope for the project, if new system please input the new system name.

Response

GRID BOT | Southern Europe | Spain

Justification

None

1.2 Please provide the Project ID Number.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.3 Please provide the Project Cost Code.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.4 Please provide the ITSC Security Ticket Number.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.5 Please select the Business Unit.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.6 Please provide the Sub Unit.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.7 Please provide information about the Business Sponsor / Owner.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.8 Please provide the Project Name.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.9 Please provide details of the Project Manager.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.10 Please provide details of the Data Protection Officer Name.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.11 Please provide the details of Business Relationship Manager (BRM)

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.12 Please provide details of the Business Analyst.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.13 Please provide details of the Solution Architect.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.14 Please provide details of the Security Officer.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.15 Please provide details of the Security Architect.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.16 Please provide details of the Line Service Manager.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

1.17 Please provide details of the Procurement Officer.

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

2 Data Scope

2.1 Please select all the type of data that apply to the project.

If you have selected the 'Others' Option, please provide more details.

Response

GRID BOT | Southern Europe | Spain

Response

Others

Justification

Public information and SSE employee SaaS accounts.

3 System and Data Classification

3.1 Please select the type of Data Classification.

Response

GRID BOT | Southern Europe | Spain

Response

Public

Justification

None

3.2 Please select the Data Availability (Recovery Time Objective)

Response

GRID BOT | Southern Europe | Spain

Response

Low

Justification

None

3.3 Please provide the Data Recovery point (Recovery Point Objective)

Response

GRID BOT | Southern Europe | Spain

Response

Medium

Justification

None

3.4 Please provide the System Classification.

Response

GRID BOT | Southern Europe | Spain

Response

Public

Justification

None

3.5 Please provide the System Availability Recovery Time Objective.

Response

GRID BOT | Southern Europe | Spain

Response

Low

Justification

None

3.6 Please provide the System Recovery Point Objective.

Response

GRID BOT | Southern Europe | Spain

Response

Low

Justification

None

3.7 What is the overall system criticality score?

Response

GRID BOT | Southern Europe | Spain

Response

Not answered

Justification

None

4 Third Party Assurances

4.1 Please select a supplier that the project is engaging with? if a new supplier please add that that information in

If new supplier, please select 'Other' and enter the name of the supplier.

Response

Grupo Atlante | SSE Renewables | Consulting

Justification

None

4.2 Have we agreed a Standard Information Security clause with the supplier?

Have we agreed a standard information security clause with the supplier.

Response

Yes

Justification

None

4.3 Does the Supplier have a valid ISO-27001 and Statement of Applicability (SoA)

Response

☒ Yes

Justification

None

4.4 Does the supplier have a valid SSAE-16/18 SOC1 report

Response

☒ No

Justification

None

4.5 Does the supplier have a valid SSAE-16/18 SOC2 report

Response

☒ No

Justification

None

4.6 Does the supplier hold any recognised cybersecurity certification (e.g., UK Cyber Essentials, ISO 27001, SOC 2, or equivalent)? If yes, please provide details, including the certification type and level.

Response

☒ Yes

Justification

None

4.7 Does the supplier carry out Pentesting/Security testing, If yes please provide more details on the type of testing and frequency

Response

☒ Not sure

Justification

None

5 Service Scope

5.1 What is the Application/Service Name?

Response

GRID BOT | Southern Europe | Spain

Response

☒ GRID BOT

Justification

None

5.2 What is the Application/Service ID information (Can be found on ITSC Service Now)

Response

GRID BOT | Southern Europe | Spain

Response

N/A

Justification

None

5.3 Business Owner

Response

GRID BOT | Southern Europe | Spain

Response

Javier Asensio

Justification

None

5.4 IT Service Owner

Response

GRID BOT | Southern Europe | Spain

Response

n

Justification

None

5.5 Description of Application/Service

Response

GRID BOT | Southern Europe | Spain

Response

The scope of the project is to develop a bespoke intelligent platform that centralises and analyses public energy-sector data in Spain to identify and monitor grid capacity, projects, and regulatory activity in real time. The system will collect and correlate information from transmission and distribution operators, REE, RAIPRE, and national and regional public bulletins, apply predefined technical and regulatory criteria to filter viable opportunities, track project status and ownership structures, and generate alerts and customised KPIs. All information will be presented through an interactive, filterable, and exportable dashboard designed to support early-stage decision-making and strategic opportunity identification.

This threat model highlights to the Cyber Security Threats with creating a bespoke AI bot to complete the scope of work and how the impact to the business from these threats poses a Risk for SSE.

Justification

None

5.6 If a supplier is required to support the Application/Service please provide details

Response

GRID BOT | Southern Europe | Spain

Response

Grupo Atlante

Justification

None

6.1 Is this a new or an existing service/system/software implementation

Response

New Software / System

Justification

None

6.2 Will the service be managing industrial control systems and if the service was adversely affected or SSE data was lost corrupted or unavailable for use. It could affect the UK or ROI Critical National Infrastructure?

Response

No

Justification

None

6.3 Will the service provide any information or data interfacing equipment (e.g. Smart Meters; Networks Control Systems) If Yes, please provide more details

Response

No

Justification

None

6.4 Will the service support Operators of Essential Services. If Yes, Please provide more details.

Response

Yes

Justification

None

Risks



Inherent risk score
16-High



Residual risk score
16-High



Target risk score
9-Medium

Risk description

There is a risk of compromise through third-party products and services, due to limited visibility of supplier security practices, components, and changes, leading to unauthorised access, malicious code insertion, and business disruption.

Stage

Evaluation

Treatment plan

1. Only use external suppliers and services that process, store, or transmit information when their security controls have been verified and appropriate terms and conditions are in place.
2. Multi-Factor Authentication (MFA) must be enforced for suppliers accessing data from outside the SSE network.
3. Further details of how to manage the OpenAI API from any supply chain risk are provided in the threat model recommendations- these need to be considered by the Grupo Atlante during the development of the SaaS solution.

6.5 Please describe how the system will managed (will it be in a SSE datacentre or will it be managed by a third party or will it be managed by a hybrid of both)

Response

Third-party SaaS

6.6 Will the service transfer data outside the EEA members states. If Yes please provide details of the location.

Response

No

Justification

None

6.7 Please describe if the service will process, transfer or store data.

Response

GRID BOT | Southern Europe | Spain

Response

Store Process

Justification

None

Risks



Inherent risk score

9-Medium



Residual risk score

9-Medium



Target risk score

6-Medium

Risk description

There is a risk of privilege escalation and data compromise, due to insufficient isolation and prioritization of privileged/sensitive processes from lower-trust domains and services, leading to unauthorised actions, tampering, and service disruption.

Stage

Evaluation

Treatment plan

1. Access to information systems and records must be restricted to authorised parties and granted strictly on the principle of least privilege.
2. There must be assurance that any person or process is correctly authenticated to provide appropriate system access and to detect and block unauthorised or malicious activity.
3. Enforce Privileged Access Management (PAM), incorporating Just-In-Time (JIT) and Just-Enough-Access (JEA) approvals where appropriate, alongside session recording.
4. Apply phishing-resistant Multi-Factor Authentication (MFA) and store secrets securely in vaults.
5. Log all privileged actions and monitor for anomalies.



Inherent risk score

9-Medium



Residual risk score

6-Medium



Target risk score

6-Medium

Risk description

There is a risk of unauthorised disclosure or tampering of stored information, due to weak or absent encryption and key management, leading to data breach, loss of trust, and regulatory penalties.

Stage

Evaluation

Treatment plan

1. Encrypt all data at rest, including backups and replicas.
2. Ensure encryption standards, procedures, and policies are in place. Use secure encryption algorithms with appropriate key sizes.
3. Implement centralised key management with dual control and regular key rotation.
4. Use vault secrets and prevent plaintext credentials in logs.

6.8 Please select the type of cloud model for this project.

Response

GRID BOT | Southern Europe | Spain

Response

On
Prem

Justification

None

6.9 What type of service model is being introduced?

Response

GRID BOT | Southern Europe | Spain

Response

SaaS

Justification

None

Risks



Inherent risk score
20-Very high



Residual risk score
12-High



Target risk score
9-Medium

Risk description

There is a risk of data exposure and service disruption, due to insecure configuration of SaaS application controls (identity, access, logging, network/API, and data protection), leading to unauthorised access, data loss, and operational outages.

Stage

Evaluation

Treatment plan

The threat model outlines recommendations which should be reviewed by the Supplier and Applied where possible. Below are some high-level requirements needed from the Supplier:

1. Data in transit between the client and the SaaS product must be securely protected.
2. Certificates used for external TLS connections should adhere to industry best practices.
3. Data exchanged between the SaaS provider's internal and external microservices should be encrypted and protected.
4. Externally exposed API endpoints that return sensitive information must require successful authentication.
5. The product should implement role-based access control (RBAC) with authorisation mechanisms that enforce clear separation of privileges across different account types.
6. The SaaS product must generate all relevant security-critical logs
7. The SaaS provider should maintain a clearly defined policy for patching internal systems and addressing security vulnerabilities.
8. The SaaS provider should publish clear, transparent details about the security features they implement and provide guidance on optimal configuration.

6.10 If a cloud service is being deployed, please select the type of cloud provider.

Response

GRID BOT | Southern Europe | Spain

Response

Non Cloud Service

Justification

None

- 6.11 Will a third party require to access SSE infrastructure from non-SSE IT equipment to deliver services? If yes please provide more information over the service they will be providing and location (Offshore/Onshore)

Response

☒ No

Justification

None

- 6.12 Is the service internet facing and if YES is SSE data accessible on a web application is the network configured in layered zones (such as a reverse proxy, web zone, application zone, database zone) that is separated by firewalls, going from the untrusted network to the trusted network?

Response

☒ No

Justification

None

- 6.13 Please describe in details of the underlying technologies the service will be sitting on (Type of operating systems, SQL engines, Webserver technology, SFTP service)

Response

Microsoft SQL Server 2022
.NET 8 REST API

- 6.14 Will the service inherit control from SSE's current security control list such i.e. Access Authentication controls (AD), Physical and environmental protection, AD. If Yes please provide more details.

Response

☒ No

Justification

None

7 System Access

7.1 Is there a requirement for individuals to authenticate to the service to perform a task . If Yes please describe they types of users (internet facing Customers/SSE Employee/Third-party) and the activities to be conducted on the system.

Response

Yes

Justification

SSE Employee

Login to the service to pull reports and interact with an AI bot.

Risks



Inherent risk score

12-High



Residual risk score

12-High



Target risk score

9-Medium

Risk

description

There is a risk of unauthorised system access, due to incomplete account lifecycle management, weak authentication, and insufficient enforcement of least privilege, leading to data compromise and service disruption.

Stage

Evaluation

Treatment plan

1. Access to information systems and records must be restricted to authorised parties and granted strictly on the principle of least privilege.
2. Implement automatic disconnection or require re-authentication of users and administrators after a defined period of inactivity (e.g., 15 minutes).
3. Enforce Multi-Factor Authentication (MFA) for all users wherever possible.
4. Enable logging and auditing for all user activities, ensuring that relevant details are captured in logs.
5. Apply privileged access management for Administrator account for GRID BOT.

7.2 Will a Third party be responsible for managing the service on behalf of SSE. If Yes list the level of access and activities they will carry out on the system

Response

Yes

Justification

SaaS managed by the provider

Risks



Inherent risk score

16-High



Residual risk score

16-High



Target risk score

9-Medium

Risk

description

There is a risk of compromise through third-party products and services, due to limited visibility of supplier security practices, components, and changes, leading to unauthorised access, malicious code insertion, and business disruption.

Stage

Evaluation

Treatment plan

1. Only use external suppliers and services that process, store, or transmit information when their security controls have been verified and appropriate terms and conditions are in place.
2. Multi-Factor Authentication (MFA) must be enforced for suppliers accessing data from outside the SSE network.
3. Further details of how to manage the OpenAI API from any supply chain risk are provided in the threat model recommendations- these need to be considered by the Grupo Atlante during the development of the SaaS solution.

- 7.3

Will SSE employees/contractors/Third-party be required to remote access to the system. If Yes, please describe the activities they will be carrying out on the system.

Response

No

Justification

n/a
- 7.4

Will there be devices used to access data. If Yes, describe the types of devices that will be used to access the data i.e. SSE Laptops, Third-party devices, Removable media

Response

Yes

Justification

SSE laptops

8 Application Development

- 8.1

Is there a requirement by the project to test and deploy code to software applications which if found vulnerable to misuse or loss of SSE data could affect SSE regulatory compliance. provide details on the activities that will be carried out

Response

No

Justification

None
- 8.2

Will a Third party be responsible for managing application development on behalf of SSE. If Yes, please provide details of services and location of the third party. Please provide information on the type of activities that will be conducted

Response

Yes

Justification

Creating a SaaS solution which will be hosted in Europe

Risks

	Inherent risk score 16-High
	Residual risk score 16-High
	Target risk score 9-Medium

Risk description

There is a risk of compromise through third-party products and services, due to limited visibility of supplier security practices, components, and changes, leading to unauthorised access, malicious code insertion, and business disruption.

Stage

Evaluation

Treatment plan

1. Only use external suppliers and services that process, store, or transmit information when their security controls have been verified and appropriate terms and conditions are in place.
2. Multi-Factor Authentication (MFA) must be enforced for suppliers accessing data from outside the SSE network.
3. Further details of how to manage the OpenAI API from any supply chain risk are provided in the threat model recommendations- these need to be considered by the Grupo Atlante during the development of the SaaS solution.

9 Security Plan Completed

9.1 Thank you for completing the NIST Security Plan Assessment.

If any further details are required, we will be in touch.

Assessment notes