

Avangrid Third-Party Risk Management Rule

Corporate Security & Resilience / Policy & Governance

Avangrid
A member of the Iberdrola Group

Corporate Security & Resilience

Document Name:	Third-Party Risk Management Rule ("Rule")
Company:	Applicable to Avangrid Inc. ("AVANGRID"), and its subsidiary companies (collectively the "AVANGRID Group")
Date:	October 2025
Purpose:	AVANGRID depends on Third Parties for the provision of services and the execution of operations. These dependencies have the potential to create risks to the company, including Cybersecurity and Data Protection, which must be properly understood and mitigated. This Rule establishes common criteria and guidelines across the AVANGRID Group for the management of the Cybersecurity and Data Protection risks derived from the Group's relationship with Third Parties.
Owner:	Chief Security Officer – AVANGRID
Updating Document:	The Owner shall review and update this Rule as necessary. The initial document and any material changes to the document must be reviewed and acknowledged by the AVANGRID Chief Security Officer. The acknowledged date and approval date are noted in the table below.

Update to 2021 Approved Rule - complete revisions to rule identifying process and methodology.



Brian Harrell, VP & Chief Security Officer

October 1, 2025

Internal Use

Table of Contents

1. Purpose & Scope 5
2. Third-Party Risk Management Basic Principles 5
3. Definitions 6
4. Methodology 8
4.1 Data Sensitivity and Classification 9
4.2 Timeline for the Evaluation Process 10
4.3 How to locate the Third-Party Risk Evaluation Form: 10
4.4 Submission and Review Process 10
4.5 Further Assessments and Documentation 11
4.6 Special Evaluation Circumstances 12
4.6.1 Framework Agreements 12
4.6.2 RFP/RFI's 13
4.6.3 Energy Service Entities (ESEs) 14
4.6.4 Interconnections: 15
4.6.5 Payment Authorization Order Invoices: 15
4.7 Continuous Risk Monitoring and Contract Termination 16
4.8 Additional Reviews and Documentation 18
4.9 SOP-66 Response TPRM Vendor Breach Process & Responsibilities 19
4.10 Third-Party Contractual Risk Acceptance (Previously Risk Exception) 20
4.11 General Provision 22
5. Roles & Responsibilities 22
5.1.1 Requestor (Project Manager, Business Area, etc.) 22
5.1.2 Corporate Security & Resilience 22
5.1.3 Corporate IT 25
5.1.4 Procurement and Vendor Management 26
5.1.5 Legal Services 26
5.1.6 Corporate Risk 26
5.1.7 NERC Reliability & Assurance 26
5.1.8 CEII Team 27

Internal Use

5.1.9 Other Relevant Teams 27
6.1. Prohibited Countries 28
7. Related and Dependent Policy Compliance 28

Internal Use

1. Purpose & Scope

Purpose: The protection of Avangrid cyber, physical and information assets is driven by business, legal, regulatory, financial and operational requirements. Avangrid depends on Third Parties for the provision of services and the execution of operations. These dependencies have the potential to create Cybersecurity, Physical Security, and Data Protection risks to the company which must be properly understood and mitigated.

Scope: The purpose of this Third-Party Risk Management Rule (hereinafter, the "Rule") is to establish common criteria and guidelines across Avangrid for the management of Cybersecurity, Physical Security, and Data Protection risks derived from Avangrid's relationships with Third Parties. The Rule is intended to supplement the Global Third-Party Cyber Risk Management Rule and align with Iberdrola policies and rules.

Application: The Rule is the set of process controls which Avangrid employees will follow when considering procuring goods and services from a Third-Party. This Rule applies to Avangrid, its subsidiaries, and all its employees in connection with all their activities, regardless of location. Capitalized terms shall have the meaning set forth in Section 3 of this Rule.

2. Third-Party Risk Management Basic Principles

Responsibility: Identification and mitigation of Cybersecurity, Physical Security, and Data Protection risks stemming from a relationship with a Third-Party, is the responsibility of the business or corporate area contracting the service, with the support, tools and procedures provided by Corporate Security.

Risk Determination: The potential to introduce Cybersecurity, Physical Security, and Data Protection risks to the Company shall be determined based on the nature of the Third-Party relationship. This includes, but is not limited to:

- Access to Avangrid information/data and the type (classification) of information/data involved.
- Access to the Group IT or OT Network infrastructure and type of connectivity.
- Provision of applications, websites, or information systems.
- Cloud services, development or maintenance of information systems; and
- Compliance risk with applicable regulations (Data Protection, Cybersecurity, Critical infrastructure, etc.).
- Any international connections which could affect supply chain or security.

Internal Use

Lifecycle Management: In line with industry best practices, Cybersecurity, Physical Security, and Data Protection risks shall be managed and controlled throughout the entire lifecycle of the relationship with the Third-Party, from the start of the procurement process to the termination of provisioning, based on risk.

Integration: Third-Party services and associated processes, infrastructure, users, resources, etc. shall be integrated into existing internal Cybersecurity management and oversight mechanisms to the extent possible.

3. Definitions

Bid Evaluation Technical Report (ITEO): Report prepared by Avangrid requesting Business containing a summary of the offers received in a specific tender, objectively evaluating the technical, Cybersecurity, Physical Security, and Data Protection, environmental and quality aspects thereof, and objectively concluding on which are the valid vendors.

Evaluation: Third-Party Risk Management tool used to engage Corporate Security in the procurement of Third-Party products and services.

Services/Materials Agreement: Contractual relationship with a Supplier, including the terms and conditions agreed upon, which identifies the equipment, materials, works and services to be acquired.

Framework Agreement: An internal, system mechanism, under which Call-Off Purchase Orders can be made throughout the duration of the Contract or Agreement. Requesting Organization can directly release Purchase Orders against the Framework Agreement for their specific requirements. Call-off Orders may be released up to the approved value of the Framework Agreement.

Information/ Data Owner: An information/data owner is a manager or above (or his/her designees), who is responsible for ensuring the classification and identification of security requirements applicable to the information he/she owns is done properly and in accordance with internal rules and external regulations. It will be identified whenever the information he/she owns is being stored, processed or transmitted by a System / Asset Owner belonging to a different organizational area.

Owner/Manager: A member of the requesting business or corporate area which manages the relationship with the vendor and for which the Third-Party provides products or services.

Personal Data: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of which natural person.

Requesting /Organization: Business or corporate area which initiates a purchasing process.

Requestor: A member of the requesting business or corporate area responsible to manage the purchasing process on behalf of the requesting business. The service requestor might be the same as the service owner.

Request for Proposal (RFP): The process within the Procurement organization requesting a product or service, including detailed technical specifications and any other documents needed to ensure that the proposal is clear and unbiased; to encourage competition and equal opportunities.

Technical Specification (TS): Document(s) prepared by the Requesting Organization describing business and technical requirements for the tender.

Third-Party: Any natural or legal person which, not being an employee or member of the administrative bodies of the Iberdrola Group (the Group), which manages information assets owned by the Group, either in its own infrastructure or within the Group's infrastructure, or who has access to the latter, and particularly those who meet any of the following conditions:

- Provide cloud services in any of its modes.
- Have access to sensitive, critical or confidential customers or employees, business, strategic or financial information or information related to the Group's critical infrastructure and systems protection mechanisms.
- Are involved in the processes or development, integration, maintenance and/or operations of the Group's systems and components or,
- Have physical access to the Group's facilities and to critical infrastructure.
- Third parties include among others, vendors, consultants, partners, regulators and government agencies.

Internal Use

Cybersecurity Risk: The potential for loss or harm resulting from threats to digital assets, information, or technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.

Data Protection Risk: The potential for loss of, or damage to sensitive or confidential information from threats to Avangrid information security, including Personal Data resulting in Privacy concerns.

Artificial Intelligence (AI): Technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

4. Methodology

All Products and/or Services procured for Avangrid shall be subject to a Third-Party Risk Evaluation. TPRM must review any purchase of a product or service which may affect IT/OT infrastructure, company data, BES cyber asset, critical business processes, or similar like purchases to evaluate Cybersecurity, Physical Security, or Data Protection risks to the company, regardless of the type of purchase it is (i.e. Centralized, Agile, Direct, etc.).

The purpose of the Evaluation is:

- Determine if the product or service has the potential to create a Cybersecurity, Physical Security, or Data Protection risk to the company.
- Identify Cybersecurity, Physical Security, and Data Protection requirements in the technical specifications to mitigate risks.
- Determine the need to perform a comprehensive Cybersecurity risk assessment of potential vendor(s).
- Identify advisable monitoring and assurance controls throughout the lifecycle of the vendor engagement.
- Ensure compliance with relevant NIST, ISO, and NERC CIP standards as well as other applicable regulatory requirements and industry best practices.
- Integrate Cybersecurity Supply Chain Risk Management (C-SCRM) practices to evaluate and mitigate risks associated with suppliers and their supply chains.

- Evaluate Non-Financial Information (including ESG Objectives) factors to ensure suppliers adhere to ethical practices.
- Implement continuous monitoring to detect and respond to new risks throughout the vendor engagement's lifecycle.
- Identify the use of AI to protect company data.
- Assess additional risk factors beyond Cybersecurity, Physical Security, and Data Protection Risk, including financial stability, operational resilience, regulatory compliance, and other supply chain risk factors.

4.1 Data Sensitivity and Classification

Data classification is a critical and foundational component of the Third-Party Risk Management process, and the Requestor must adhere to the Avangrid Data Classification and Treatment Rule. It is the responsibility of the Subject Matter Expert (SME), manager, or director overseeing the engagement to accurately classify the data involved and communicate this classification to the Third-Party Risk Management Team during the evaluation process.

4.1.1 Data Classification Responsibilities:

SMEs, managers, and directors must assess the sensitivity of the data involved in the Third-Party engagement.

Data should be classified according to Avangrid's data classification standards (e.g., public, internal use, confidential, restricted secret).

The classification must be documented and communicated to the Third-Party Risk Management Team.

All data classification and handling must comply with the Avangrid Data Classification and Treatment Rule, ensuring appropriate security measures are applied to reduce the risk of unauthorized access, disclosure, alteration, and destruction of Avangrid information/data.

4.1.2 Evaluation Process:

The Third-Party Risk Management Team will use the data classification information to determine the appropriate level of risk evaluation and monitoring. Confidential and Restricted classified data will require more stringent security controls and assessments.

4.1.3 Ongoing Responsibility:

SMEs, managers, and directors must ensure any changes in data sensitivity are promptly communicated to the Third-Party Risk Management Team. Regular reviews of data classification should be conducted to ensure accuracy and compliance with Avangrid's policies.

4.2 Timeline for the Evaluation Process

The Third-Party Risk Evaluation process shall follow the timeline below:

- **Initial Screening:** The TPRM Team has a 5-business day Service Level Agreement (SLA) to review the initial Third-Party Risk Evaluation.
- **Reliability Assurance Assessment:** If the purchase may be in scope for CIP-013, additional time may be needed for the NERC CIP team to review the Third-Party Risk Evaluation.
- **Contractual or Supplemental Security Assessments:** The TPRM Team has a 10-business day SLA to review any additionally required contractual or supplemental Security Assessments.

4.3 How to locate the Third-Party Risk Evaluation Form:

The Third-Party Risk evaluation form is located on the Corporate Security & Resilience Office SharePoint site, within the Third-Party Page. Additional contractual documents which may be required are located in the Contractual Documentation page on the Third-Party SharePoint site.

4.4 Submission and Review Process

The Requester shall notify the Third-Party Risk Management Team by submitting the Third-Party's name and active website via the Risk Evaluation.

Review of the Risk Evaluations by Corporate Security and Resilience Office will determine Risk Security Assessment requirements.

The Third-Party Risk Evaluation may include a request for an overview of the proposed and/or existing Third-Party relationship with the Third-Party.

It is the responsibility of the Requestor to communicate the determined Cybersecurity, Physical Security, & Data Protection Security Assessment requirements to the Third-Party.

The Requestor is responsible for obtaining completed Risk Security Assessments from the Third-Party and submitting them to the Third-Party Risk Management Team for review.

The Requestor is responsible for identifying the classification level of data shared, stored or processed by the Third-Party.

4.5 Further Assessments and Documentation

Based on the review of the initial Evaluation, the Corporate Security and Resilience Office may determine the need to perform further Third-Party assessments of Cybersecurity and/or Data Protection controls.

- An email notification will be sent to relevant teams including but not limited to Cybersecurity, OT Cybersecurity, Threat Management Intel, Data Protection, and others as necessary, informing them of the need for further assessments and documentation. This ensures all relevant stakeholders are aware and can provide input as needed to fully mitigate the risk to Avangrid.

Once Corporate Security has received and reviewed the initial Evaluation and any additional requested documentation, the need for the following information and/or documentation will be determined and communicated to the Requestor via email:

- Need for a Data Security Rider (DSR) or other contract security Annexes.
- Cyber Insurance recommendation.
    - Questions regarding cyber insurance amounts should be directed to the Avangrid Insurance team at: insurancerisk@avangrid.com.
- Other relevant materials, e.g. data flow diagrams, design specifications, System & Organizational Controls 2 (SOC 2), CIP-013 documentation, or the use of AI, etc.
- Requests for Corporate Security, Subject Matter Expert (SME) participation in Data Security Rider (DSR), and other materials review with the business

and/or the Third-Party, shall be coordinated by the Project Manager/Business Requester.

- Corporate Security shall require 10 business days to schedule a materials review.

4.6 Special Evaluation Circumstances

Conducting a thorough Third-Party Risk Evaluation is essential to identify and mitigate Cybersecurity, Physical Security, and Data Protection risks. This section outlines specific unique situations requiring a possible variation to the Third-Party Risk Evaluation process.

4.6.1 Framework Agreements

Recognizing the need to maintain an auditable record of all purchases to ensure compliance with NERC and the Third-Party Risk Management Rule, while also balancing the Business Area's administrative workload and need to remain flexible in multi-PO Framework Agreements, the following approach is designed to avoid multiple redundant evaluations:

- The Business Area (except in the case of those engagements already deemed in NERC-CIP scope) can use the original completion/approval email from the TPRM tool as evidence the Third-Party Framework Agreement was evaluated and all relevant Cybersecurity Risk paperwork (or risk exceptions) were completed, received, approved, and filed with the Third-Party Risk Management Team.
- In lieu of the need for multiple evaluations within the Framework term, the Business Area can submit a quarterly Third-Party Risk evaluation via the Third-Party Risk Evaluation Form located on the Corporate Security & Resilience SharePoint Site.
    - It is incumbent on the Business Area to track and submit its quarterly reporting and communicate about the reporting with the TPRM program.
- The Business Area must ensure the evaluation accurately and clearly reflects:
    - The relevant purchase number for identification
    - The SAP Vendor Number

    - Identifies within the free text "scope of engagement box," which submission is the quarterly filing under the Framework Agreement and provide the original Third-Party ID number (5- or 6-digit number).
    - Attach a document which details, at minimum, all PO reference numbers, date, payment amounts, and payee (either by number or name reference) for the reporting quarter.
- The Business Area will ensure purchases are within the scope of the original Framework.
- This evaluation will allow Third-Party to perform any due diligence necessary to mitigate ongoing risk and will serve to satisfy the audit needs.
- This methodology will not supersede requirements to require High Risk and Very High-Risk Third-Party engagements to provide updated documentation when required.
- This process will continue to be adjusted to meet both Third-Party Risk Management and Business Area needs while maintaining compliance with policy and regulatory requirements.

4.6.2 RFP/RFI's

1. To ensure comprehensive risk management and compliance with Avangrid's security standards, all Requests for Proposals (RFPs) and Requests for Information (RFIs) must undergo the Third-Party Risk Management (TPRM) process.
    - During RFP/RFI creation, the Requestor should anticipate submitting two (2) Third-Party Evaluations. The initial evaluation will risk rank the Scope of Work (SOW) within the RFP/RFI. A follow-up evaluation will include the assessment of any required cybersecurity materials and the review of a DSR if necessary. This evaluation needs to be completed by the TPRM Team before a contract is signed with the Third-Party.
    - The TPRM Team strongly suggests a requirement of all bidders on High Risk/Very High-Risk RFPs/RFIs to submit the anticipated cybersecurity documents without the DSR (which can be completed by the selected bidder at the time of negotiating the final contract.) With the cybersecurity documents submitted at this point in the Procurement Process, the Requestor can utilize the TPRM Team's review of the bidders' cybersecurity profile and history as part of the technical review in the bid process.

2. Below outlines the necessary steps and responsibilities for the requesting organization and the TPRM Team to effectively evaluate and manage Third-Party risks during the RFP/RFI stage and before awarding a bid to a Third-Party.
    - The Requestor must identify the engagement as being in the RFP/RFI stage within the TPRM Risk Evaluation.
    - The TPRM Team will provide an initial recommendation regarding the anticipated Cybersecurity documentation required to mitigate the risk or indicate if no further Cybersecurity documentation will be needed.
    - This initial evaluation is based only on the SOW and does not factor in all risk or supply chain concerns. Therefore, it is not a final risk ranking approving the engagement with a Third-Party.
    - The Requestor is responsible to ensure any Third-Party contracted to complete the SOW of an RFP has been evaluated by TPRM.
    - TPRM suggests within the ITEO process, a Third-Party evaluation is conducted for all submitted bidders as part of the technical evaluation within this part of the Procurement Process.
    - Upon submitting the new evaluation for the Third-Party intended to contract to complete the SOW, ensure the original Third-Party Evaluation ID Number is referenced in the appropriate section of the new evaluation form.
    - The TPRM Team will conduct a final review of the Third-Party(s) intended to contract to complete the SOW.
    - Define the specific requirements needed to complete the process, ensuring all necessary steps are followed as outlined in the Methodology section

4.6.3 Energy Service Entities (ESEs)

ESE are Third-Parties which provide energy or perform an energy related service.

When considering the risk to the Company of an ESE, Customer data is usually the primary focus. Therefore, best practice dictates any data is shared via a customer consent mechanism. The data shared should be documented by an evaluation to Third-Party in order to monitor the ESE in the event they are affected by a data security incident.

Ultimately, the standard of review will be dictated by the data requested to be shared and a historical Cybersecurity analysis of the Third-Party.

4.6.4 Interconnections:

Interconnections are Third-Parties which connect directly or indirectly to the electrical grid. These types of Third-Parties include DERs/DG energy entities, Aggregators of meter energy generation, or Aggregators which facilitate connection to DERs/DGs. While these entities often are registered and evaluated by utility commissions and regional ISOs, TPRM will conduct its own evaluation for risk and inventory concerns.

When interconnecting Third-Party systems with Avangrid's infrastructure, it is crucial to ensure comprehensive security and regulatory measures are in place to protect sensitive information and maintain operational integrity. The following shall be considered:

- **Data Security Agreement (DSA)**: Use a Data Security Agreement (DSA) instead of a Data Security Rider (DSR) for managing interconnections between Avangrid and Third-Party systems, as a DSA is specifically focused for this type of engagement.
- **Security Controls Evaluation**: Evaluate the security controls of Third-Party systems which will interconnect with Avangrid's infrastructure.
- **Risk Mitigation**: Identify and mitigate potential risks associated with data exchange and system integration.
- **Compliance Assurance**: Ensure compliance with Avangrid's Cybersecurity policies and standards, as well as relevant regulatory mandates.
- **DSA Documentation**: Ensure that the DSA includes detailed security requirements, data handling procedures, and compliance obligations.

4.6.5 Payment Authorization Order Invoices:

A PAO is an internal purchasing document which is required for enabling and documenting the payment of certain contracting categories which do not require purchasing activity. PAOs are used for payment obligations where there is no possibility to negotiate with a vendor and all PAO concepts must be previously approved by the Purchasing Department. (*Accounts Payable Policy, Section 5.2. & Appendix A*)

Internal Use

TPRM recommends before the Purchasing Department approve a PAO, the vendor is submitted to TPRM for evaluation of risk and to maintain a complete inventory of Third-Parties.

The Purchasing Procedure provides guidance to comply with the Avangrid Purchasing Risk Policy for the Avangrid Group which establishes a global framework for monitoring and managing the risk resulting from the purchasing activities undertaken for the procurement or contracting of equipment, materials, works and services throughout the Group. The procedure detailed in this document, does not apply to any fuel, energy, raw material purchases, real estate, contracts with municipalities, government agencies, legal services, financial services and other Payment Authorization Orders (PAO), where there is no possibility for negotiation and this concept has been previously approved by the Purchasing Department. (*Avangrid Purchasing Procedure, Section 1*)

4.7 Continuous Risk Monitoring and Contract Termination

Corporate Security and Resilience Office will continuously monitor specific third parties identified in the Third-Party Risk Evaluation process. This includes, for example, defining alert rules to notify the Third-Party Risk Management Team of new incidents, data breaches, merger/acquisitions, and/or decrease in security scoring tool score. TPRM will notify procurement and the business requestor of a significant change or risk. Additionally, Corporate Security and Resilience Office will provide Project Managers/Business Requesters with an annual Third-Party status report.

All Third Parties ranked High and Very High Risk will be subject to a Continuous Risk Monitoring (CRM) Process after the initial risk evaluation is completed. Third Parties ranked Medium Risk will be reviewed on an ad hoc basis within the CRM Process.

The CRM Process will consist of:

- Continuous monitoring within Vendor Risk Management Solutions[1] by defining alert rules to notify TPRM of new data security incidents, mergers/acquisitions, decrease in Cybersecurity score, and other risk areas as applicable to the scope of work in the initial engagement.

[1] Currently Avangrid Corporate Security and Resilience employs the use of Security Score Card and Recorded Futures as its Vendor Risk Management Tools.

Internal Use

- Regular Audit and Risk Review of High Risk and Very High Risk Third Parties during the contract lifecycle.

The Audit and Review of Very High Risk Third Parties may consist of:

- Annual evaluation (proactive) of the Third-Party within the Vendor Risk Management Solutions as defined above.
- A request (not to extend beyond 18 months) to the Third-Party to re-submit an updated Annex 2 NATF Questionnaire for review by TPRM.
- Upon analysis of the above, if there is any significant change or issues of concern TPRM will conduct a more thorough review. This review should include, as appropriate, the re-submission and review of Business Continuity Plans, Incident Response Plans, Communication Plans, Cybersecurity Policies and Procedures, Training & Awareness activities as well as an onsite inspection.
- The analysis will be a new review considering the initial scope of work and information provided by the Third-Party and regarding current threat intelligence.

The Audit and Review of High Risk Third Parties may consist of:

- Continuous monitoring (reactive) within Vendor Risk Management Solutions as defined above.
- A semi-annual request (not to extend past 24 months) to the Third-Party to re-submit an updated Annex 2 NATF Questionnaire for review by TPRM.
- Upon analysis of the above, if there is any significant change or issues of concern TPRM will conduct a more thorough review. This review may include, as appropriate, the re-submission and review of Business Continuity Plans, Incident Response Plans, Communication Plans, Cybersecurity Policies and Procedures, and Training & Awareness activities.
- Any analysis will consider the initial scope of work compared to the information provided by the Third-Party.

The Audit and Review of Medium Risk Third Parties may consist of:

- Review of Medium Risk Vendors may be conducted only in special risk circumstances, including but not limited to:

Internal Use

a. Consultants with access to confidential or restricted data as a scope of work,
b. Medium Level NERC-CIP assets,
c. An ad hoc review of the Third-Party's Cybersecurity profile within Vendor Risk Management Solutions as defined above.

- If there is any significant change or issues of concern arising from above, TPRM may request an Annex 2 NATF Questionnaire for review by TPRM.
- Annual Reviews and Audits: For engagements involving confidential or restricted data, the Corporate Security and Resilience Office shall require annual reviews and audits to ensure ongoing compliance with security and Data Protection requirements. This includes reassessing risks and updating security controls as necessary. Additionally, the Corporate Security and Resilience Office reserves the right to audit low-risk engagements or those which fall under the internal classification, as well as request any additional reviews, documentation, or actions deemed necessary to address emerging risks or compliance requirements not explicitly covered in this policy.

Upon contract termination, the Requester shall ensure, as applicable:

- The termination of all digital identities and access rights to include those of contractors.
- The return of equipment and devices provided by Avangrid.
- The destruction, or return by secure storage, of Avangrid information/ data.
- Secure disconnections from Avangrid's cyberinfrastructure.
- Closure/ deregistering of IP addresses, domains, applications and web sites.
- Closure / decommission of any platform or mechanism used for information exchange.
- Verification of supplier access to organizational resources is deactivated.

4.8 Additional Reviews and Documentation

If a risk with a vendor is identified at any point during the engagement, the TPRM Team reserves the right to require additional reviews and documentation. This may include, but is not limited to:

- **Comprehensive Risk Assessments**: Conducting further risk assessments to evaluate the identified risk and its potential impact on the company.
- **Updated Security Documentation**: Requesting updated security policies, procedures, and controls from the vendor.

- **Incident Reports**: Requiring detailed reports on any incidents, breaches, or security concerns which have arisen.
- **Mitigation Plans**: Requesting a detailed plan from the vendor outlining steps to mitigate the identified risk.
- **Regular Audits**: Scheduling regular audits and reviews to ensure ongoing compliance with security and Data Protection requirements.
- **Enhanced Monitoring**: Implementing enhanced monitoring measures to detect and respond to new risks promptly.

4.9 SOP-66 Response TPRM Vendor Breach Process & Responsibilities

If Corporate Security & Resilience receives information about a possible security event/breach of a Third-Party vendor, the Third-Party Risk Management (TPRM) team is responsible for managing its internal process to determine if, or to what extent, Avangrid is affected. The TPRM Team will conduct their investigation consistent to SOP 66.

1. **FOLLOW-UP ACTIVITY**

a. TPRM will continue to collaborate with our business partners to ensure the vendor is contacted, Avangrid receives regular updates from the vendor including the extent of the overall impact if any and what mitigation steps the vendor has taken to prevent reoccurrence.
b. TPRM will continue to update the Kaseware Third-Party Breach Investigation Form of relevant updates received.
c. In a confirmed, direct cyber event, the C-SIRT team is responsible for collecting information and managing technical issues.
d. The Incident Response Team (IRT) will work with C-SIRT and other Corporate Security and business areas to set a regular update schedule, via email or calls depending on the situation, so departments can provide updates, and key stakeholders can be provided regular updates on the situation and investigation status.
e. If the cyber breach is determined to be an incident, the UIRP will take the lead on managing communications.

Internal Use

4.10 Third-Party Contractual Risk Acceptance (Previously Risk Exception)

In rare circumstances, the Requestor may need to continue to contract with the Third-Party although the required Cybersecurity documentation has not been completed. In those cases, the Requestor can submit a Third-Party Contractual Risk Acceptance the Requestor will need to submit a Third-Party Contractual Risk Exception if a Third-Party will not comply with the required contractual documents or the residual risk remaining to Avangrid remains extremely high and use of the Third-Party cannot be recommended.

Before the Requestor seeks a risk exception, the TPRM Team should be engaged to work with the vendor to narrow the outstanding risks. Additionally, the Requestor and TPRM should work together to identify the risk mitigation strategy which will be documented in the Risk Acceptance Agreement and presented to Corporate Security's Risk Review Board.

To obtain an approved Risk Acceptance, the Requestor opens a Third-Party Contractual Risk Exception Form and completes the following steps:

1. The Risk Exception Form includes the following sections to be completed by the Requestor:
2. Third-Party ID Number (this is the original Third-Party Risk Evaluation ID Number)
3. Third-Party Name
4. Requester's Information and Business Area
5. Whether the Third-Party will require access to NERC CIP Restricted information
6. Applicable section of the Third-Party Management Rule, the Third-Party cannot comply with.
7. Requestor Reasoning and Justification for Requested Exception
8. The Reason Section should not just be a recitation of the SOW but ***must*** detail how this Third-party is the only choice to complete the required work. The Justification Section ***must*** detail the risk to Avangrid if the work is not completed by the Third-Party. If these sections are not completed to the satisfaction of the Risk Board, the exception will be returned to the Requestor to be resubmitted with those changes noted.
9. The Requestor ***must*** Identify the Compensating Controls or risk mitigation strategy to be employed to address the associated risks.

Internal Use

10. This can include the Third-Party's contractual documentation in lieu of Avangrid's.
11. Any relevant documents should be attached.
12. Once the Risk Exception Form has been submitted, the Requestor will receive an email from the TPRM Tool stating it has been successfully received by Corporate Security & Resilience Office and will be reviewed.
13. The Risk Exception Review Board meets biweekly. The Board consists of the SME Directors and/or their delegates to discuss the circumstances of the exception and ensure all due diligence was conducted and that the greatest effort of remediation of risk will be employed. If any questions or concerns arise, the TPRM Team will communicate back to the Requestor.
14. If the Risk Acceptance is approved by the Risk Board, the Requestor is responsible for obtaining a signature from the VP (or higher,) of the business area, accepting the risks defined in the exception form.
15. Approval by the Risk Board should not be construed that Corporate Security & Resilience recommends the Third-Party, but that the Risk Acceptance Agreement clearly defines the necessary information and contains a mitigation strategy which will allow the business area VP to conduct a valid risk assessment before accepting the risk on behalf of Avangrid.
16. Once signed, the Requestor must submit the Signed Risk Acceptance Agreement to the TPRM team for final approval.
    - The Risk Exception is active for 1 year from the date of signature, unless otherwise specified. Upon date of expiration of the Risk Acceptance Agreement, the Project Requestor will receive an automated email stating the Risk Acceptance is up for renewal. The Requestor may choose to renew the Acceptance or inactivate the exception within 60-business days.
17. An expired Risk Acceptance will be treated as that the Third-Party is no longer conducting the scope of work or contracted to do work and the TPRM Team will notify the Requestor to begin the procedure necessary to inactivate connections or reclaim data under the contract termination terms of the contract.
18. Renewals of a Risk Acceptance Agreement will trigger a review of the Third-Party by the TPRM Team and may require the resubmission of outdated or expired Cybersecurity documentation.

Internal Use

4.11 General Provision

The Corporate Security and Resilience Office may request additional reviews, documentation, or actions deemed necessary to address emerging risks or compliance requirements such as emerging Cybersecurity threats, changes in regulatory requirements, and any other factors which may impact the security and integrity of Avangrid's information/data assets.

5. Roles & Responsibilities

5.1.1 Requestor (Project Manager, Business Area, etc.)

- **Complete Evaluations:** Complete the Avangrid Third-Party Risk Evaluation for all new/renewal Third-Party engagements by submitting a request for evaluation from the Corporate Security & Resilience SharePoint site..
- **Technical Evaluation:** Complete the Cybersecurity/Data Protection technical evaluation of the received bids and identify any Cybersecurity/Data Protection non-compliances.
- **Coordinate Action Plans:** Coordinate the Third-Party action plan to mitigate the risks, when required. Ensure which the contract meets the requirements established in this Rule. Ensure service provisioning complies with any applicable Cybersecurity and Data Protection rules & procedures.
- **Manage Risks:** Ensure Cybersecurity & Data Protection risks are properly managed throughout the life of the contract.
- **Business Continuity:** Integrate Critical Services into relevant Business Continuity plans and procedures and conduct periodic testing of these plans.

5.1.2 Corporate Security & Resilience

Cybersecurity

- **Risk Assessment:** Assess Third-Party vendors' security risks and their potential impact on the organization's systems, data, and operations. Provide risk-based recommendations to mitigate threats and ensure compliance with corporate security standards.
- **Review Exceptions:** Review all Cybersecurity-related risk exceptions for Third-Party risk management evaluations, ensuring deviations from security requirements are documented, justified, and appropriately mitigated.

- **Investigate Breaches:** Investigate Third-Party data breaches upon notification from the vendor or team within Corporate Security. Analyze root cause, assess the impact on the company, and recommend corrective actions to prevent future incidents.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Drone Program

- **Compliance:** Ensure all drone acquisitions and operations comply with federal and state regulations prohibiting the use of drones from certain foreign manufacturers.
- **Policy Adherence:** Ensure compliance with UAS Grid Protection Rule.

- **Review Exceptions:** Ensure all Third-Party Risk Exceptions regarding drones are reviewed and documented.

Governance, Risk & Assurance

- **Implementation:** Ensure the TPRM rule is effectively implemented, updated, and aligned with regulatory requirements, industry best practices, and corporate risk tolerance.
- **Review Risk Acceptance Agreements:** Review Third-Party Risk Exceptions to ensure all deviations from security and operational standards are properly documented, justified, and mitigated.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Operational Technology

- **Compliance:** Confirm which all products and services comply with regulatory requirements and internal safety protocols.
- **Network Segmentation:** Maintain appropriate network segmentation and implement robust controls, when necessary, to securely integrate OT solutions into Avangrid's environment.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Physical Security

- **Protocol Review:** Review Third-Party's physical security protocols, including but not limited to access controls, surveillance systems, facility security, and emergency response capabilities.

Internal Use

Data Protection

- **Contract Review:** Review all contractual documents from Third-Party's related to the Third-Party Risk Management Process to ensure they align with Avangrid's security standards, regulatory requirements, and internal policies.
- **Data Protection:** Evaluate Third-Party's Data Protection practices, identifying potential Data Protection risks and ensuring which Third-Party's implement robust controls to safeguard sensitive information.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Resilience / Business Continuity

- **Impact Assessment:** When notified that a critical process or system involves a Third-Party engagement, assess the potential operational impact.
- **Risk Evaluation:** Evaluate the Third-Party's role within the critical process, identify risks, and determine how disruptions could affect overall business continuity.
- **Recovery Strategies:** Outline recovery strategies, identify alternative vendors or backup procedures, and establish recovery time objectives for critical systems reliant on these Third-Parties.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Third-Party Risk Management

- **Oversight:** Oversight and maintenance of the Third-Party Security Risk Evaluation process, database and reporting to support the requesting business.
- **Support:** Support the Requesting Business in identifying & managing Third-Party Cybersecurity & Data Protection risks.
- **Communication Protocol:** Develop a protocol for the communication and coordination of vulnerabilities, threats and incidents with relevant vendors.
- **Key Risk Indicators:** Establish Key Risk Indicators and reporting mechanisms to track the effectiveness of the TPRM Program. Provide regular updates to senior leadership highlighting key risks, trends, and necessary improvements in Third-Party risk management.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Third-Party Intelligence

- **Independent Review:** When notified of an Avangrid high or very high-risk Third-Party engagement, conduct an independent review to assess the potential

Internal Use

threats—including the Third-Party's exposure to Cybersecurity risks, geopolitical risks, and industry-specific vulnerabilities.

- **Gap Analysis:** Identify any gaps or emerging risks by comparing internal evaluations with real-time threat intelligence.
- **Recommendations:** Develop actionable recommendations, where possible, to mitigate identified risks including additional monitoring requirements, enhanced security controls, and/or alternative Third-Party strategies.
- **Risk Board:** Participate in the Risk Review Board as an SME.

Training & Awareness

- **Training Materials:** Support the creation of training materials which educate employees on Third-Party risk management fundamentals, best practices, and the potential impacts of Third-Party related risks.
  Internal Campaigns: Support the TPRM team in leading internal campaigns and communications to promote the TPRM program across Avangrid.

5.1.3 Corporate IT

- **Database Maintenance:** Maintain updated databases with the information related to Iberdrola Group users and assets related to Third-Party contracts.
- **Technical Monitoring:** Perform technical monitoring of the users & assets related to Third-Party contracts.
- **Incident Management:** Collaborate in the management of vendor incidents.
- **Risk Review Board:** Participate in the Risk Review Board as an SME.
- **AI CoC:** IT will work with CSRO to ensure all Third-Party evaluations containing the use of AI are evaluated through TPRM before the use of AI is presented to the AI COC as the use of AI by that specific vendor may be a relevant dimension of the risk to be weighed by the AI COC members.
  - IT will also work with CSRO to ensure all Third-Party evaluations involving AI systems—defined as machine-based systems that make predictions, recommendations, or decisions—are reviewed through the AI Code of Conduct (AI COC) process. This includes:
    - Identifying AI use cases during the initial risk evaluation
    - Applying AI-specific risk criteria (e.g., model transparency, data provenance, bias mitigation)

Internal Use

- Coordinating with Legal and Data Protection teams for compliance with emerging AI regulations
- Documenting the AI risk assessment outcome in the TPRM record (Insert finalized link to AI COC and any related SOPs)

- **Offboarding:** Manage Third-Party offboarding initiatives when the vendor engagement is complete.

5.1.4 Procurement and Vendor Management

- **Platform and Process:** Provide the platform and the process (I-buy).
- **Compliance:** Procurement will assist TPRM with the goal of ensuring Third-Parties, within their scope, are evaluated pursuant to this rule and effective audit and control measures are in place within the systems and processes.
- **Risk Assessment:** To ensure the entirety of the Cybersecurity risk assessment process within the TPRM Rule has been completed.
- **RFP Requirements:** Ensure that the RFP includes a specific section on Cybersecurity & Data Protection requirements before it is published.
- **ITEO Completion:** To verify that the Cybersecurity section of the ITEO has been completed.
- **Risk Review Board:** Participate in the Risk Review Board as an SME.

5.1.5 Legal Services

- **Contract Clauses:** To prepare standard and ad hoc Cybersecurity & Data Protection clauses to be included in the contracts.
- **Support:** To support the Requestor throughout contract negotiation.
- **Risk Board:** Participate in the Risk Review Board as an SME.

5.1.6 Corporate Risk

- **Risk Board:** Participate in the Risk Review Board as an SME.

5.1.7 NERC Reliability & Assurance

- **Evaluation Review:** Review and oversee Third-Party Risk Management Evaluations to ensure which Third parties in scope for CIP-013 meet all NERC reliability assurance requirements for Corporate, Networks and Renewables.

- **Record Maintenance:** Support the TPRM team in maintaining detailed records of compliance findings, risk assessments, and any exceptions identified during the review process.
- **Reporting:** Support the TPRM team in preparing comprehensive reports and documentation to demonstrate adherence to CIP-013 requirements for internal and NERC regulatory reviews.

5.1.8 CEII Team

CEII Team

- **Evaluation Oversight:** Assess and oversee Third-Party Risk Management Evaluations which involve the access, storing and/or processing of CEII data for Corporate, Networks, and Renewables.
- **Ongoing Monitoring:** Oversee the ongoing monitoring for Third-Party's handling CEII data, ensuring continuous compliance and alignment with evolving regulations.

5.1.9 Other Relevant Teams

- Any other teams not explicitly mentioned in this section which are, or may become involved in Third-Party Risk Management, Cybersecurity, Physical Security, Data Protection or related activities, are expected to collaborate and fulfill their roles and responsibilities necessary to ensure compliance with this policy. This includes providing input, support and documentation as required to manage and mitigate risk effectively.

6. Supply Chain Risk Management Concerns

The purpose of this section is to provide Avangrid personnel with guidance regarding how the sourcing of goods and services from Third-Parties can create risk to the company beyond Cybersecurity considerations. This guidance should be consulted in conjunction with the Avangrid Third-Party Risk evaluation process and factors herein may be considered aggravating concerns increasing the initial Third-Party risk rank.

This guidance also applies to the sourcing and/or procuring of goods or services from suppliers owned or controlled by, or otherwise connected to, the Peoples

Republic of China, Russia, North Korea, and Iran (each, a "Prohibited Country", and collectively, the "Prohibited Countries" which would affect from countries which present known security threats to the United States.)

6.1. Prohibited Countries

Corporate Security & Resilience does not support the procurement of goods and services, which could have a negative security implication, from Prohibited Countries.

When situations arise in which the procurement of goods or services, which could be sensitive items, are required and known to be sourced from a Prohibited Country, the Avangrid (Networks, Renewables, Corporate) Business Area Lead (BAL) VP or higher, should be informed and confirm acceptance, prior to accepting a bid.

The Third-Party Risk Acceptance process should be used to acknowledge this confirmation.

Where situations arise in which a joint project/procurement with Iberdrola includes the sourcing of goods or services which could be sensitive items from a Prohibited Country, the Avangrid project/relationship manager should inform and receive confirmed acceptance from the Avangrid (Networks, Renewables, Corporate) Business Area Lead (BAL) VP or higher.

The Third-Party Risk Acceptance process should be used to acknowledge this confirmation.

Confirmed acceptance from an Avangrid Operating Company C-level executive does not supersede the requirements for an RFP (Request for Proposal), a Third-Party Risk Management evaluation, an ITEO, (Bid Evaluation Technical Report), as well as the compliance processes associated with the Protocol for the Management of Third-Party Fraud, Corruption Risk and OFAC Compliance Risk.

7. Related and Dependent Policy Compliance.

This rule is not intended to read as the sole standalone guidance but the baseline process to evaluate and mitigate risk to Avangrid posed by Third-Parties. Internal

related and inter-dependent policies, rules, guidelines and SOPs must be consulted for compliance in order to weave the greatest level of protection for Avangrid's people, assets, and information. Ultimately, the TPRM process is in search of the best decision for Avangrid.

It is incumbent of the Requestor to be familiar with, and ensure the provisions of this guidance, are followed.

Internal Use