ERCOT Cyber Security Supplier Guideline

Introduction

The security of the Texas bulk power system, as well as the security of our customers' and ERCOT's data, is of great importance to ERCOT.

ERCOT realizes and respects the important role that our suppliers play in the successful delivery of our missions, and we expect all suppliers to support our cyber security efforts. Therefore, we require our suppliers to complete the ERCOT Supply Chain Risk Management Questionnaire and comply with the cyber security requirements of ERCOT's Professional Services Agreement, if required, based upon the goods or services being procured by ERCOT. Both documents are available at http://www.ercot.com/about/procurement.

The Supply Chain Risk Management Questionnaire includes a set of cyber security controls that constitute the minimum baseline of cyber security measures by which ERCOT expects its suppliers to comply.

This guideline contains information and clarifications for each of the cyber security controls listed in the Supply Chain Risk Management Questionnaire.

ERCOT will evaluate responses to our questionnaire in order to assess a supplier's security posture and to determine potential risks to ERCOT and the Texas bulk power system.

ERCOT requires that organizations substantiate their answers via a third-party assessment, such as a relevant SOC assessment or an ISO 27001 certification, or by referencing their internal documents.

Applicability

Completion of ERCOT's Supply Chain Risk Management Questionnaire is required of all suppliers of hardware, software, cloud-based services, and information technology goods and services, including business critical systems and services from a reseller, sole source, or original equipment manufacturer (OEM).

Explanation of ERCOT Supply Chain Risk Management Questionnaire

During the evaluation of a supplier's cyber security posture, ERCOT will evaluate various supply chain categories. The following are the supply chain categories in ERCOT's questionnaire. Each category contains questions that require a detailed response from the supplier. These responses will be reviewed and scored by ERCOT in order to determine the supplier's cyber security risk level. Depending upon ERCOT's evaluation of a supplier's responses to ERCOT's questionnaire and the subsequent risk level, ERCOT may take additional steps to ensure mitigation of identified risks. Where applicable, these categories include a reference to specific NERC CIP Standards and/or the NIST Cyber Security Framework within the questionnaire.

Category 1: Country of Origin and Operations
ERCOT seeks to find out the geolocation (city and country) of the supplier’s headquarters and data centers. ERCOT is also interested in the country where the supplier sources its staffing resources, software development, and hardware components, as well as any additional countries in which the supplier has a presence. The country where the supplier is located or headquartered is considered. For example, if the supplier is located or sources its staff in the United States or a friendly foreign country, it is more likely that the supplier has supply chain security processes similar to ERCOT’s already in place.

Category 2: History
ERCOT seeks to find out when the company of the supplier was founded. A company that is well established with a measurable length of time in business will be more likely to have mature business processes, including those applicable to supply chain security practices.

Category 3: Industry, Core Business, Type of Supplier
Industry: ERCOT evaluates each supplier to determine if it specializes in products for the electric utility industry or if its portfolio includes a large number of solutions for a broad range of industries. This can be an important risk attribute in determining the level of specialized support available.

Core Business: ERCOT’s evaluation of a supplier will also be influenced by the supplier’s core business offerings. If the purchase includes products within a supplier’s core business, support and continued development is more likely than that if the purchase includes a recently acquired or ancillary offering.

Type of Supplier: The type of supplier being considered will also influence the risk level assigned by ERCOT (i.e., manufacturer, supplier, developer, integrator, reseller, or service provider). Resellers of pre-packaged software may be subject to less scrutiny than suppliers that are developing or customizing software.

Category 4: Asset Management
ERCOT seeks to find out the maturity of the supplier’s asset management program and whether the supplier has a holistic view of its entire assets. The ability of a supplier to view and manage its entire portfolio of assets impacts the risk exposure to ERCOT.

Category 5: Change Management and Software Development Considerations
ERCOT seeks to find out the maturity of supplier’s hardware development lifecycle, software development life cycle (SDLC), and change management processes. Suppliers able to demonstrate that they have developed and abide by a documented hardware development lifecycle, software development life cycle, or change management or similar process are viewed as a lower risk.

ERCOT also seeks to determine the risk posed by a vendor based on where the supplier sources its physical and software components. For example, components sourced from a foreign country may suffer from quality and cyber security issues, thus posing a higher supply chain risk. In some cases, ERCOT may seek additional information regarding the original source of materials in a supplier's supply chain.

Category 6: Governance

ERCOT seeks information regarding a supplier's governance model as it relates to supply chain risk management and cyber security. These factors include the maturity of a supplier's security program and adherence to NERC CIP requirements.

The following criteria indicate a reduced supply chain risk:

- Supplier has a mature security program
- Supplier demonstrates due diligence in adhering to NERC CIP requirements
- Supplier demonstrates PCI DSS compliance

In order to assess the risk associated with a supplier's governance strategy, ERCOT also seeks to determine if PCI DSS compliance assessments are performed with an accredited party and are performed to cover all services provided to ERCOT. Vendors that demonstrate assessments were performed with an accredited party pose a lower supply chain risk.

Category 7: Logging and Monitoring Considerations

Suppliers that maintain a program to log and monitor data have records useful in case of a supply chain compromise. Suppliers that utilize such a program have a lower supply chain risk.

Monitoring programs help to notify the supplier of a potential breach. In the event of a breach or supply chain compromise, complete logs are crucial to fully understanding the nature of the breach and any affected information. ERCOT expects this information to be passed on to ERCOT if the breach or vulnerability impacts ERCOT in any way.

Category 8: Information Protection Considerations

ERCOT seeks to determine the information protection technologies and controls a supplier has implemented. Suppliers that utilize strong encryption have a lower risk of security vulnerabilities and thus pose a lower supply chain risk. This encryption applies to all data including cardholder and PII, in transit and at rest.

Additionally, suppliers that have the capability to manage malicious code have a lower supply chain risk.

ERCOT expects each supplier to protect ERCOT-related data. As such, these factors strongly influence the risk rating of a particular supplier.

Category 9: Account Management

ERCOT seeks to find out the maturity of the supplier's account management program. Suppliers that have a formal Access Control Policy, manage their inventory of accounts, and enforce password complexity requirements have a lower supply chain risk.

These basic security policies prevent unintended or malicious access attempts to supplier systems where ERCOT data might be accessed.

Category 10: Notification of Cyber Security Incidents

ERCOT has developed a supply chain cyber security risk management plan, which manages processes used in procuring BES cyber systems that address the notification by the vendor of vendor-identified incidents that pose cybersecurity risk to ERCOT. ERCOT will seek information about a supplier's process to notify ERCOT of vendor-identified incidents related to the products or services that pose cyber security risk to ERCOT. This can include cyber security incidents that may not directly impact the product or service itself, such as data breaches that disclose ERCOT data.

Suppliers that have a process to notify ERCOT in the event of a data breach have a lower supply chain risk

Additionally, ERCOT strives to determine if a vendor carries insurance to cover ERCOT due to non-compliance with PCI DSS and whether a supplier offers support and protection to cover ERCOT due to non-compliance with PCI DSS. Suppliers that carry cyber insurance have a lower supply chain risk.

Per ERCOT's Professional Services Agreement (PSA), ERCOT must be notified of any breach or cyber incidents. All such notifications should be sent immediately to SupplierNotification@ercot.com.

Prompt notification of potential breaches or vulnerabilities allows ERCOT to minimize the impact of such cyber security related issues.

Category 11: Coordination of Responses to Cyber Security Incidents

ERCOT has developed a supply chain cyber security risk management plan that addresses processes used in coordination of responses to vendor-identified incidents that pose cyber security risk to ERCOT. ERCOT will seek information about supplier's process to coordinate responses to supplier-identified incidents related to the products or services provided to ERCOT that pose cyber security risk to ERCOT. Beyond the notification process, ERCOT needs to know if the supplier has processes to provide notifications to ERCOT as soon as practicable, if the supplier develops security updates and provides them to customers as soon as practicable, and if the supplier identifies compensating measures ERCOT can implement.

It is the expectation that the supplier will work together with ERCOT to respond to security breaches and vulnerabilities as soon as practicable.

Category 12: Remote and On-site Access

ERCOT has developed a supply chain cyber security risk management plan that addresses notification by vendors when remote or on-site access to ERCOT systems and premises should no longer be granted to vendor representatives.

ERCOT seeks to determine if the supplier has developed a process to provide notification to ERCOT when a supplier's employee's remote or on-site access is no longer granted. Suppliers should notify ERCOT immediately upon resignation, termination, or reassignment of any individuals with ERCOT access privileges.

Each supplier is expected to abide by a process to provide notification to ERCOT when vendor personnel's remote or on-site access is no longer granted. Supplier and third-party support personnel should only be granted remote network access on a need-to-know basis and their activity should be logged while active. All access should be removed upon completion of an individual's assignment.

Suppliers that are able to address ERCOT's remote and on-site access requirements help ERCOT to reduce supply chain risk by ensuring that only active employees retain access to ERCOT systems and data and that they're only able to interact with relevant information.

Category 13: Vulnerability Identification

ERCOT has developed a supply chain cyber security risk management plan that addresses disclosure by vendors of known vulnerabilities related to the products or services provided to ERCOT.

ERCOT's risk management plan depends upon early notification of risks and vulnerabilities by suppliers. ERCOT seeks to understand a supplier's vulnerability management program and to verify a supplier's commitment to communicate any identified vulnerabilities. A supplier's ability to meet these requirements reduces ERCOT risk and improves ERCOT's ability to mitigate future risks.

Category 14: Software Integrity and Authenticity

ERCOT has developed a supply chain cyber security risk management plan that addresses verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES cyber system.

As part of the evaluation of potential suppliers, ERCOT will assess a supplier's software and patch management program, including any processes to allow ERCOT to verify the integrity or authenticity of software and patches (i.e., fingerprints or cipher hashes). Suppliers should communicate their software development lifecycle management plans and processes.

These processes ensure that only legitimate and authentic software and patches are exposed to ERCOT's systems, reducing the risk of malicious code impacting ERCOT systems.

Category 15: Supplier Remote Access
ERCOT has developed a supply chain cyber security risk management plan that addresses coordination of controls for vendor-initiated interactive remote access and system-to-system remote access with the vendor.

ERCOT seeks to determine whether the supplier's remote access policy addresses account control and monitoring for interactive and system-to-system remote access, and ensures that hardware, software, and firmware connected to ERCOT's network is maintained and updated in order to remediate security vulnerabilities or weaknesses.

Category 16: Description
ERCOT seeks to validate the type of service or product being provided by the supplier to ERCOT. Supplier risk will be commensurate with how closely the supplier's service or product aligns with ERCOT's business needs. The description may also be used to determine whether future supply chain risk assessments are necessary based upon any subsequent change in scope, product, or service.

Category 17: Cloud-Based Services
Suppliers offering cloud-based services introduce additional risks to ERCOT, including loss of control over data and other considerations. ERCOT seeks to determine whether controls have been implemented by the cloud provider to the extent reasonably possible. ERCOT seeks to determine controls around application security, governance, information protection standards, physical security, API architecture, application architecture, business continuity architecture, data architecture, operations architecture, and security architecture, among other factors.

Suppliers demonstrating secure controls around cloud components have a lower supply chain risk.