ChecklistGuro

Energy Cybersecurity Risk Assessment Checklist Template

Asset Identification & Inventory

Identify critical energy assets and maintain a comprehensive inventory including hardware, software, and data locations.

Asset Name

Write something...

Asset ID

Enter a number...

Asset Description

Write something...
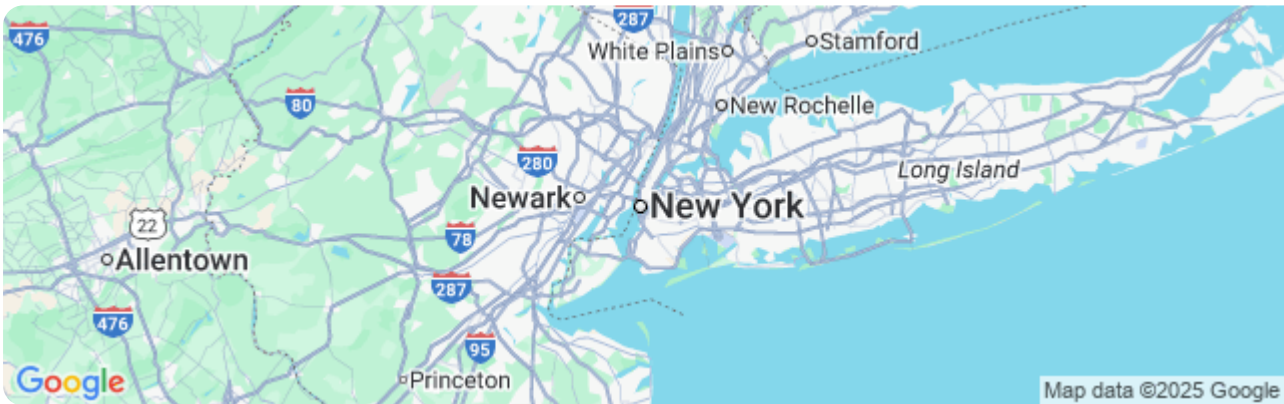
Asset Type (e.g., Turbine, Substation, Solar Panel)

☐ Turbine

☐ Substation

☐ Solar Panel

☐ Wind Turbine

☐ Generator

☐ Transformer

Date of Last Inventory Update

Enter date...

Asset Location (GPS Coordinates)

📍 Set My Current Location

Asset Documentation (Manuals, Schematics)

⬆ Upload File

Network Security

Assess network segmentation, firewall configurations, intrusion detection/prevention systems, and remote access controls.

Firewall Rule Count

Enter a number...

Firewall Vendor

- [ ] Cisco
- [ ] Palo Alto
- [ ] Fortinet
- [ ] Check Point
- [ ] Other

Network Segmentation Zones

- [ ] OT Network
- [ ] IT Network
- [ ] DMZ
- [ ] Guest Network

Last Firewall Rule Review Date

Enter date...

Description of Network Segmentation Strategy

Write something...

Intrusion Detection System (IDS) Status

☐ Active

☐ Inactive

☐ Needs Review

Number of VPN Connections

Enter a number...

Endpoint Security

Evaluate endpoint protection, vulnerability scanning, patch management, and mobile device security policies.

Last Vulnerability Scan Score

Enter a number...

Last Patching Date

Enter date...

Antivirus Software

☐ Enabled

☐ Disabled

☐ Not Installed

Software Updates Enabled?

☐ Automatic

☐ Manual

☐ Disabled

Latest Endpoint Security Report

⤒ Upload File

Firewall Status

☐ Enabled

☐ Disabled

Number of Active EDR Agents

Enter a number...

Data Security & Privacy

Review data encryption, access controls, data loss prevention measures, and compliance with data privacy regulations.

Data Encryption Status

☐ Fully Encrypted

☐ Partially Encrypted

☐ Not Encrypted

Number of Data Breaches (Last Year)

Enter a number...

Data Privacy Regulations Compliance

- ☐ GDPR
- ☐ CCPA
- ☐ NERC CIP
- ☐ Other

Data Classification Policy Description

Write something...

Access Control Review Frequency

- ☐ Monthly
- ☐ Quarterly
- ☐ Annually

Last Data Privacy Impact Assessment Date

Enter date...

Identity & Access Management (IAM)

Assess user account management, authentication methods (MFA), privileged access management, and role-based access control.

Authentication Method Used

- ☐ Password
- ☐ Multi-Factor Authentication (MFA)
- ☐ Biometrics
- ☐ Certificate-Based Authentication

Number of Active User Accounts

Enter a number...

Privileged Access Management (PAM) Implementation

- ☐ Implemented
- ☐ Partially Implemented
- ☐ Not Implemented

Last Password Policy Review Date

Enter date...

Account Access Review Frequency

- ☐ Monthly
- ☐ Quarterly
- ☐ Annually
- ☐ Ad Hoc

Description of Role-Based Access Control (RBAC) Model

Write something...

Typical Time for User Account Provisioning

Account Lockout Policy Enforced?

☐ Yes

☐ No

Supply Chain Risk Management

Evaluate cybersecurity practices of third-party vendors and service providers involved in the energy supply chain.

Vendor Tier Level

☐ Tier 1 (Critical)

☐ Tier 2 (Important)

☐ Tier 3 (Supporting)

Vendor Risk Score (1-10)

Enter a number...

Vendor Cybersecurity Assessment Completed?

☐ Yes

☐ No

☐ Pending

Last Cybersecurity Assessment Date

Enter date...

Summary of Vendor Cybersecurity Assessment Findings

Write something...

Vendor Cybersecurity Assessment Report

⬆ Upload File

Key Services Provided by Vendor

☐ Software Development
☐ Data Storage
☐ Network Services
☐ Physical Security

Remediation Plan for Identified Risks (if any)

Write something...

Incident Response & Recovery

Review incident response plans, disaster recovery procedures, and business continuity planning for cybersecurity events.

Date of Incident

Enter date...

Time of Incident

Detailed Description of Incident

Write something...

Incident Severity Level

☐ Low

☐ Medium

☐ High

☐ Critical

Systems Affected

☐ SCADA

☐ Historian

☐ Network Infrastructure

☐ Workstations

☐ Cloud Services

Containment Actions Taken

Write something...

Eradication Actions Taken

Write something...

Recovery Actions Taken

Write something...

Estimated Downtime (hours)

Enter a number...

Incident Responder Signature

Security Awareness & Training

Assess the effectiveness of cybersecurity awareness training programs for employees and contractors.

Number of Employees Trained (Last Year)

Enter a number...

Training Delivery Method (Select all that apply)

☐ Online Modules

☐ Classroom Sessions

☐ Phishing Simulations

☐ Tabletop Exercises

Date of Last Cybersecurity Awareness Training

Enter date...

Summary of Key Training Topics Covered

Write something...

Frequency of Refresher Training (Choose one)

☐ Annually

☐ Bi-Annually

☐ Quarterly

Training Content Topics (Select all that apply)

☐ Phishing Awareness

☐ Password Security

☐ Malware Prevention

☐ Data Privacy

☐ Social Engineering

Regulatory Compliance

Verify adherence to relevant cybersecurity regulations and industry standards (e.g., NERC CIP, GDPR).

Applicable Regulations (Select all that apply)

- ☐ NERC CIP
- ☐ FERC Regulations
- ☐ State-Specific Energy Regulations
- ☐ GDPR (if applicable)
- ☐ Other (Specify in Long Text)

Specify 'Other' Regulations (if selected)

Write something...

Last Compliance Audit Date

Enter date...

Audit Score (if applicable)

Enter a number...

Upload Compliance Documentation

⬆ Upload File

Compliance Status

- ☐ Compliant
- ☐ Non-Compliant
- ☐ Partial Compliance

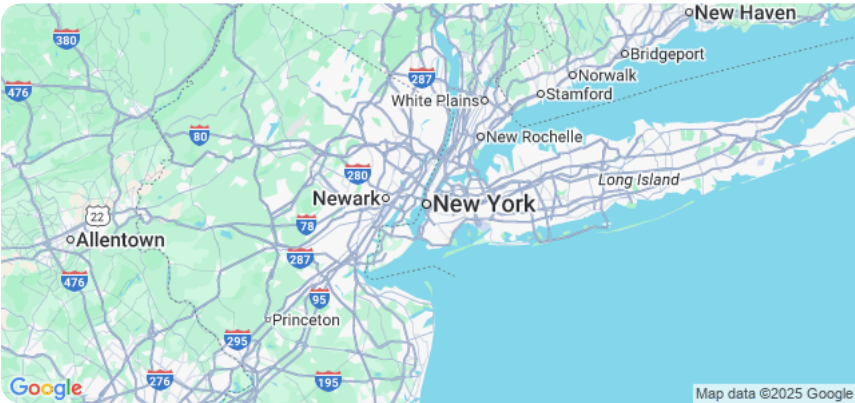## Details of Non-Compliance (if applicable)

Write something...

Physical Security

Evaluate physical access controls, surveillance systems, and security measures protecting energy infrastructure.

Location of Main Control Room

📍 Set My Current Location

Number of Security Cameras (Active)

Enter a number...

Type of Perimeter Fencing

☐ Chain-link

☐ Welded Mesh

☐ Concrete Wall

☐ None

Date of Last Perimeter Fence Inspection

Enter date...

Access Control Methods Employed

☐ Keycards

☐ Biometrics

☐ PIN Codes

☐ Guards

Description of Visitor Management Process

Write something...

Security Personnel Signature (Confirmation of Physical Security Check)