Cybersecurity of Critical Energy Infrastructure – Two Case Studies

Hisham Choueiki, Ph.D., P.E.
NARUC

Meeting of ERRA Member Chairmen, Presidents and Commissioners
October 28, 2024 | Tirana, Albania

Hosted by:

GOAL OF SECURITY

The goal of security is to manage risk by reducing the impact and/or likelihood of harm to an organization's asset committed by a malign actor targeting the asset's vulnerability.

INFORMATION SECURITY AND CYBERSECURITY

- Information security is the protection of information.
  - Documents, text, video, audio
  - Analog information (printed documents, books, reports, information displayed on monitors, spoken by people, …)

- Cybersecurity is the protection of cyber.
  - Computer networks
  - Data storage
  - Software
  - Digital information at rest and in transit

A VULNERABILITY/THREAT ASSESSMENT

- Assets can be vulnerable.
  - Asset vulnerabilities are independent of threats.
  - Asset vulnerability exposures can change over time.
- Threats can exploit vulnerabilities.
  - Threats are independent of vulnerabilities.
  - Threats require capabilities and knowledge to exploit vulnerabilities.
  - Threats exploit vulnerabilities through attack scenarios.
  - Threats can be used to assist with the identification of vulnerabilities (e.g., white hat hacking).

VULNERABILITY TREATMENT OPTIONS (TTTT)

- Treat
  - Protection measures – Defend the asset risk/vulnerability from attack.
  - Resilience strategy – Establish a resilience response ahead of time to respond to an attack.
- Transfer
  - Give the responsibility for managing the asset risk/vulnerability to another party.
  - Purchase insurance, subcontract the responsibility, sell the asset and establish a service contract, etc.
- Terminate
  - Dispose of the asset with the vulnerability (destroy, sell, retire, etc.).
- Tolerate
  - Do nothing – Leave the asset vulnerability exposed and deal with the fallout if an attack does occur.

A REGULATOR'S FINANCIAL CONSIDERATIONS

- Information security and cybersecurity cost money.
- Protection measures and building resilience cost money.
- There is not enough money to go around.
- A risk-based approach to information and cybersecurity can reduce costs.
- Therefore, the *prioritization of the assets and their associated risks achieve this goal.*

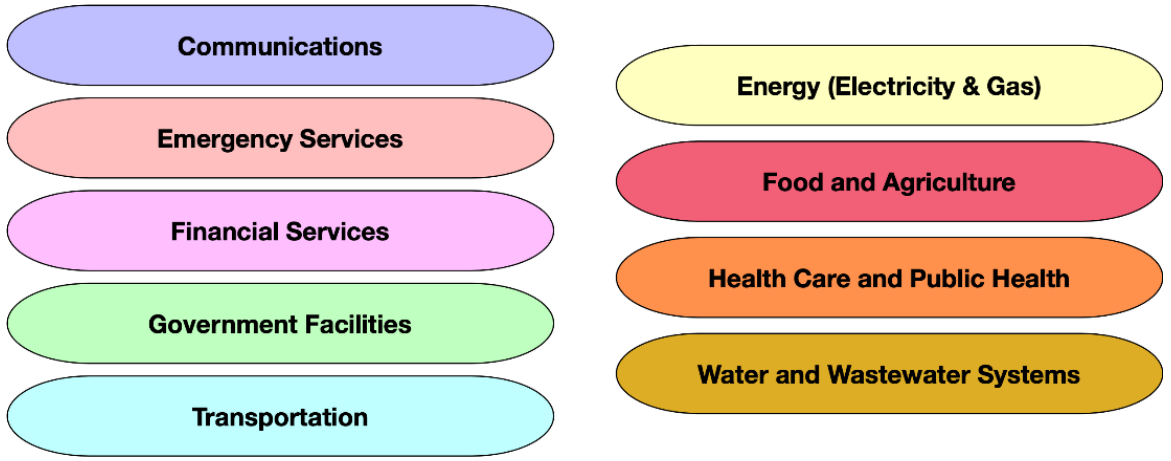
A REGULATOR'S FINANCIAL CONSIDERATIONS (cont.)

- Appropriateness of selected option
  - Treat, transfer, terminate, tolerate
- Effectiveness of the protection measure
  - Once implemented, did the protection measure achieve or exceed the residual risk?
  - Over time, does the protection measure continue to achieve or exceed the residual risk?
- Effectiveness of the cyber investment
  - Was the cost of the cyber investment warranted?
  - Did the cyber investment provide an acceptable return on investment?
  - Was the additional investment required to sustain the effectiveness of the protection measure?

DEFINITION OF CRITICAL NATIONAL INFRASTRUCTURE (CNI)

A paraphrase of the NIST definition of CNI is:

> "Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters."



IMPORTANT DEFINITIONS

- **Critical load** is the electrical load upon which an organization relies to keep its key operations running. As a corollary to critical load is non-critical load, which is electrical load that is not important to keep on. Once critical loads have been identified, they need to be prioritized by their importance and how long they need to be kept running when the security of supply has been compromised.

- **Critical energy infrastructure information** is the important network infrastructure, information systems, and technological systems in the energy industry. These are the systems whereby their destruction, harm, or loss of functionality may result in a severe impact on national security, the national economy and people's livelihood and health, or the public interest.

TYPES OF QUESTIONS TO ASK

1. What is critical infrastructure?
2. Does critical infrastructure include the power grid?
3. Is the entirety of the power grid considered critical infrastructure?
4. What should be considered critical infrastructure?
5. Should the critical infrastructure asset list be public domain?
6. Does the government or NRA have any protective marking policies?
7. Does the government or NRA have any policy regarding the handling of protected information
8. Other…

HOW DOES CRITICAL INFRASTRUCTURE RELATE TO CYBERSECURITY?

- Digital automation has created a dependency with critical infrastructure.
- IT systems are a conduit to disrupting critical infrastructure.
- IT is not the critical infrastructure; rather, it supports the critical infrastructure.
- Most IT systems serving critical infrastructure were designed and implemented without consideration to cybersecurity – this brings about more vulnerability.

WHAT IS RISK MANAGEMENT?

- Risk is the probability that a vulnerability will be exploited such that it results in harm. It is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

- Risk is the product of likelihood and impact.

- Risk management is the identification and reduction of risks to manageable levels.

COSTS ASSOCIATED WITH CYBERSECURITY

- Implementation of an ISMS (like an ISO 27001)
- Operations costs for running the implemented ISMS
- Mitigation for implementing controls to protect against an attack incident
- Training is not a one-time activity; it needs continuous reinforcement.
- Communications with staff regularly to reinforce knowledge and understanding of cybersecurity
- Internal audits performed at least annually (ideally twice annually or even quarterly)
- Certification audits performed to achieve formal certification

THE CASE OF ALBANIA
ASSESSMENT OF UTILITY PREPAREDNESS

LAW No 2/2017 ON CYBERSECURITY

- The purpose of law no. 2/2017 is to achieve a high level of cybersecurity by defining security measures, rights, obligations and mutual cooperation between the entities operating in the field of cybersecurity.
- Achieving this requires the implementation of organizational and technical security measures.
- Organizations are required to implement measures needed to prevent and minimize the impact of risks and cybersecurity incidents.
- The law lists 20 security objectives, divided into technical and organizational measures, based on international standards used by electronic communications sector providers in the European Union.
- ERE issued the cyber regulation order on July 30, 2020.

ORGANIZATIONAL MEASURES

		Measures			Documentation	
	ORGANZATIONAL MEASURES	Level 1	Level 2		Level 1	Level 2
1	a) Information Security Management	4	2		5	9
2	b) Risk Management	6	1		7	1
3	c) Security Policies	4	1		10	2
4	ç) Organizational Security	4	1		11	2
5	d) Security Requirements for Third Parties	4	2		8	2
6	dh) Asset Management	2	1		9	2
7	e) Security of human resources and access of people	3	1		17	1
8	ë) Security events and management of cyber security incidents	3	2		6	2
9	f) Management of work continuity	3	5		7	4
10	g) Control and audit	4	1		7	1
	Sub Totals	*37*	*17*	*Sub Totals*	*87*	*26*
	Levels 1+2	*54*		*Docs 1+2*	*113*	

TECHNICAL MEASURES

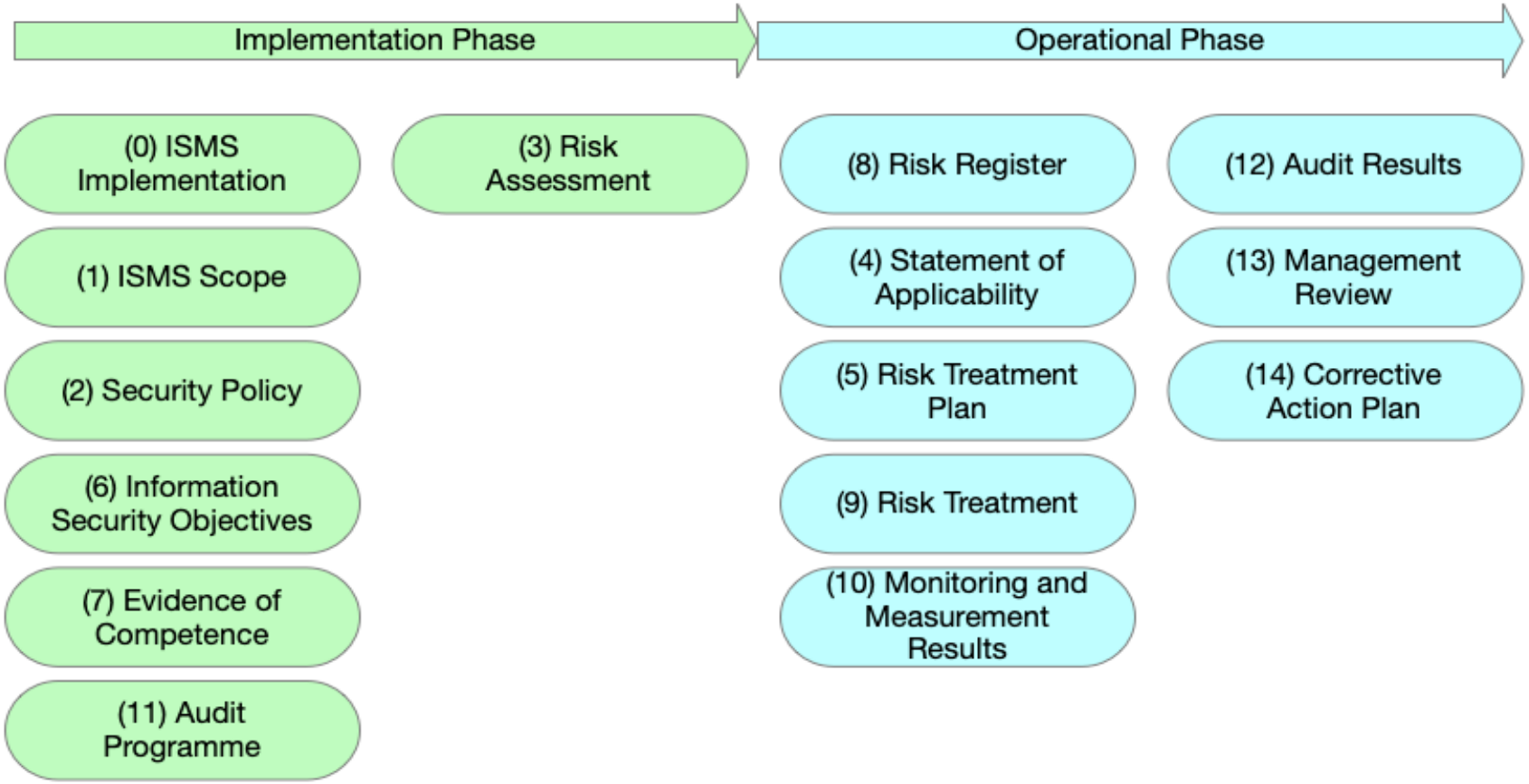
		Measures			Documentation	
	TECHNICAL MEASURES	Level 1	Level 2		Level 1	Level 2
1	a) Physical security	3	2		3	2
2	b) Protecting the integrity of communication networks	4	2		6	2
3	c) Verifying user identity	3	1		3	1
4	ç) Access authorization management	3	1		5	1
5	e) The activity of administrators and users	4	1		3	1
6	dh) Discovering cyber security events	3	1		2	2
7	e) Tools for tracking and evaluating cyber security events	1	1		1	1
8	ë) Applications Security	1	1		1	1
9	f) Of cryptographic devices	2	1		5	2
10	g) Security of industrial systems	0	2		0	14
	Sub Totals	*24*	*13*	*Sub Totals*	*29*	*27*
	Levels 1+2	*37*		*Docs 1+2*	*56*	

ISO 27001 ALLIGNMENT WITH LAW No 2/2017

- All 91 of the Law No. 2/2017 security objective measures were mapped by NARUC to the 60 ISO27001 requirements.

- By documenting this mapping, compliance to the Law No. 2/2017 security objective measures can be demonstrated to the ERE through the twice annual ISO27001 internal audits and by an ISO27001 certification.
  - Compliance to the Law No. 2/2017 security objective measures is proven through induction (i.e. via the mapping process).
  - By virtue that an ISO27001 requirement is found compliant, it implies that each mapped Law No. 2/2017 security objective measures is also compliant.

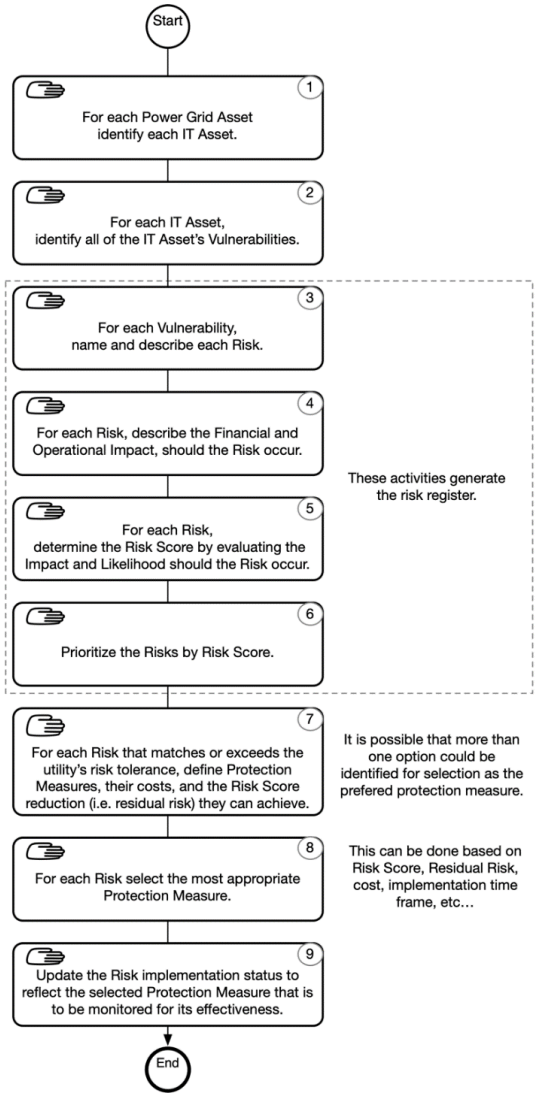
MANDATORY DOCUMENTS FOR ISO 27001 IMPLEMENTATION



THE CASE OF GEORGIA
REASONABLENESS OF CYBERSECURITY INVESTMENTS

SAMPLE RISK ASSESSMENT PROCESS

- It takes a power grid-centric view of assets.
- Critical power grid assets are reviewed for their dependencies on IT/OT assets.
- These become the IT/OT assets that need cybersecurity protection.
- Financial considerations are always at the forefront of risk assessments.
  - Handle risk via preemptive protection measures
  - Handle risk through resilience
- Once a protection measure has been implemented, it must be monitored for its effectiveness.
  - Poor performance warrants changing the protection measure or the treatment.
  - Outstanding performance warrants reducing the protection measure performance to reduce cost.



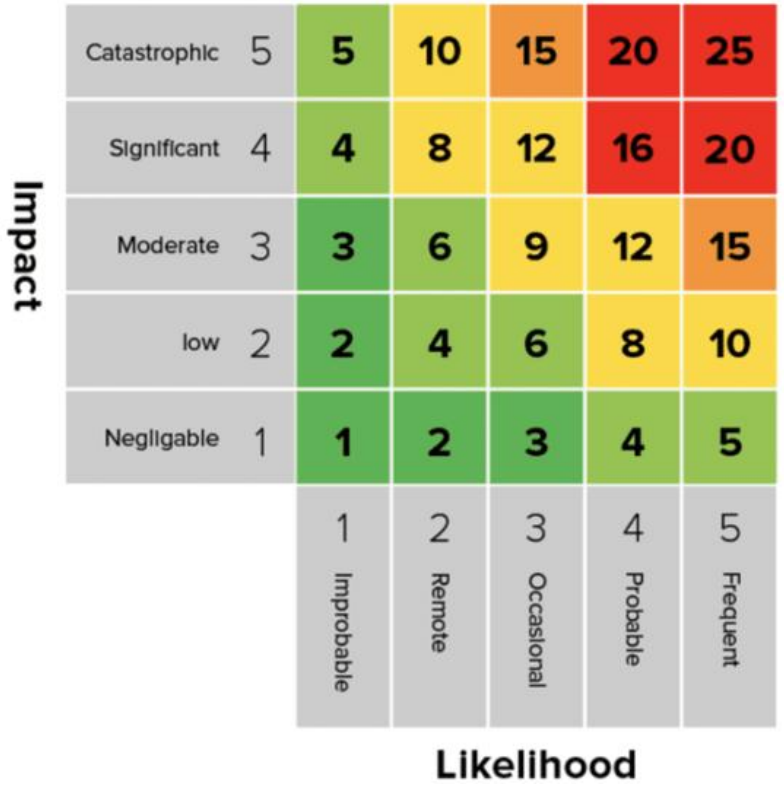
RISK REGISTER DATA SUBMITTED TO GNERC

Date	Risk Score (1-5)	Protection Measure	Applicable IT Asset
Risk ID	Impact (1-5)	Protection Measure Cost	Applicable Power Grid Asset
Risk Name	Likelihood (1-5)	Reduced Risk Score (1-5)	Power Grid Vulnerability
Risk Description	Financial Impact	Implementation Status	Critical Infrastructure Asset
Vulnerability	Operational Impact	Implementation Date	Critical Infrastructure Vulnerability

Typically shown as a list, beginning with the highest risk score and working to the lowest.

ISO27001 RISK REGISTER

Identifies all risks and prioritizes them based on risk value (See Annex for example)



- Risk #
- Risk Name
- Risk/Asset Owner
- Asset
- Critical Load (if applicable)
- Critical Infrastructure Dependecy (if applicable)
- Vulnerability
- Impact + Explanation
- Likelihood + Explanation
- Risk Value
- Treatment Option (TTTT)
- Risk Threshold (Management/Regulator)

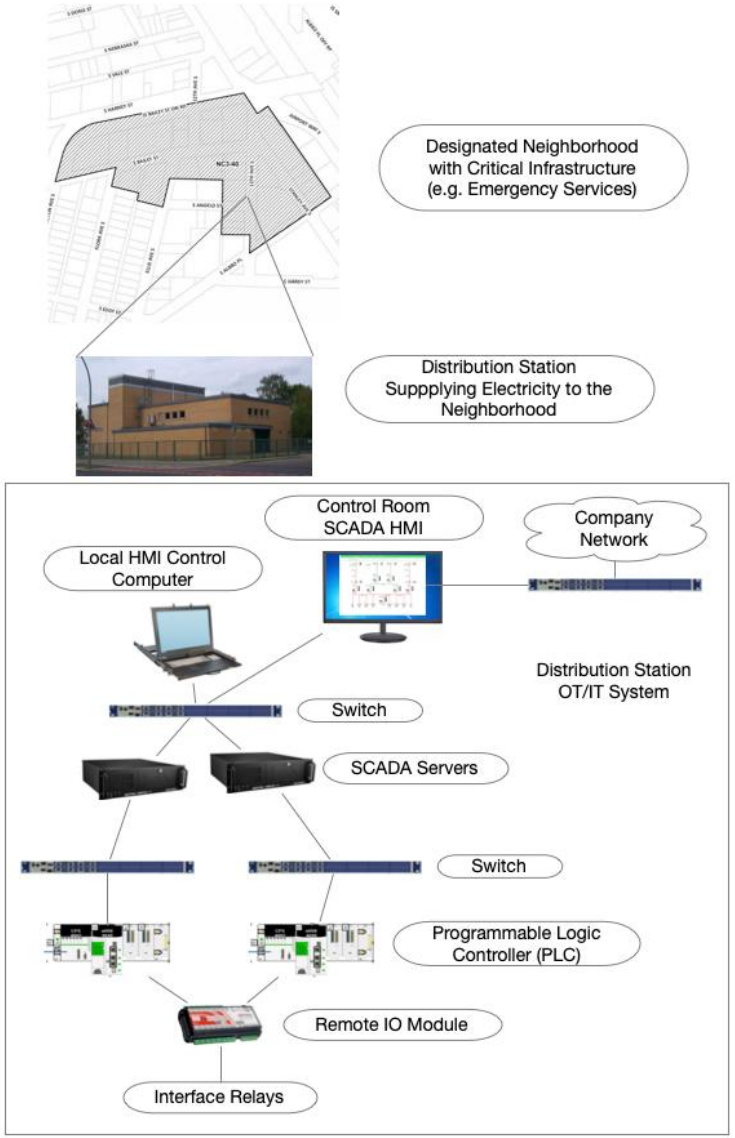
THANK YOU FOR YOUR ATTENTION!

Hisham Choueiki, Ph.D., P.E.
hchoueiki@naruc.org

ANNEX
RISK REGISTER EXAMPLE

Identify all the high-risk power grid assets. For this example, it will be a neighborhood distribution station because it is supplying electricity to an emergency services facility.

Step 1
OT/IT Assets
Control Room SCADA HMI
Local HMI Control Computer
Company Network Switch
Switch 1
SCADA Server 1
SCADA Server 2
Switch 2
Switch 3
PLC 1
PLC 2
Remote IO Module



For each power grid asset, identify each IT asset.

Step 2	
OT/IT Assets	**Vulnerability**
Control Room SCADA HMI	Old Operating System
	Old SCADA
	Old Hardware
	Accessible from company network
Local HMI Control Computer	Old Operating System
	Old SCADA
	Old Hardware
Company Network Switch	None
Switch 1	None
SCADA Server 1	Old Operating System
	Old SCADA
SCADA Server 2	Old Operating System
	Old SCADA
Switch 2	None
Switch 3	None
PLC 1	None
PLC 2	None
Remote IO Module	None

For each IT asset, identify all the IT asset's vulnerabilities.

Step 3		
OT/IT Assets	**Vulnerability**	**Risk**
Control Room SCADA HMI	Old Operating System	Stolen data
	Old SCADA	Take over control Shutdown electricity
	Old Hardware	Failure Loss of control
	Accessible from company network	Take over SCADA Loss of control Shutdown electricity
Local HMI Control Computer	Old Operating System	Stolen data
	Old SCADA	Take over control Shutdown electricity
	Old Hardware	Failure Loss of control
Company Network Switch	None	Take over SCADA Loss of control Shutdown electricity
Switch 1	None	None
SCADA Server 1	Old Operating System	Stolen data
	Old SCADA	Take over control Shutdown electricity
SCADA Server 2	Old Operating System	Stolen data
	Old SCADA	Take over control Shutdown electricity
Switch 2	None	None
Switch 3	None	None
PLC 1	None	None
PLC 2	None	None
Remote IO Module	None	None

For each vulnerability, name and describe each risk.

Step 4				
OT/IT Assets	**Vulnerability**	**Risk**	**Financial**	**Operational**
Control Room SCADA HMI	Old Operating System	Stolen data	Low	Low
	Old SCADA	Take over control Shutdown electricity	High	High
	Old Hardware	Failure Loss of control	Moderate	High
	Accessible from company network	Take over SCADA Loss of control Shutdown electricity	High	High
Local HMI Control Computer	Old Operating System	Stolen data	Low	Low
	Old SCADA	Take over control Shutdown electricity	High	High
	Old Hardware	Failure Loss of control	Moderate	High
Company Network Switch	None	None	None	None
Switch 1	None	None	None	None
SCADA Server 1	Old Operating System	Stolen data	Low	Low
	Old SCADA	Take over control Shutdown electricity	High	High
SCADA Server 2	Old Operating System	Stolen data	Low	Low
	Old SCADA	Take over control Shutdown electricity	High	High
Switch 2	None	None	None	None
Switch 3	None	None	None	None
PLC 1	None	None	None	None
PLC 2	None	None	None	None
Remote IO Module	None	None	None	None

For each risk, describe the financial and operational impact should the risk occur.

For each risk, determine the risk score by evaluating the impact and likelihood should the risk occur.

Step 5					
OT/IT Assets	**Vulnerability**	**Risk**	**Impact**	**Likelihood**	**Score**
Control Room SCADA HMI	Old Operating System	Stolen data	1	4	4
	Old SCADA	Take over control Shutdown electricity	5	4	20
	Old Hardware	Failure Loss of control	4	3	12
	Accessible from company network	Take over SCADA Loss of control Shutdown electricity	5	3	15
Local HMI Control Computer	Old Operating System	Stolen data	1	4	4
	Old SCADA	Take over control Shutdown electricity	5	4	20
	Old Hardware	Failure Loss of control	4	3	12
Company Network Switch	None	None	1	1	1
Switch 1	None	None	1	1	1
SCADA Server 1	Old Operating System	Stolen data	1	4	4
	Old SCADA	Take over control Shutdown electricity	5	4	20
SCADA Server 2	Old Operating System	Stolen data	1	4	4
	Old SCADA	Take over control Shutdown electricity	5	4	20
Switch 2	None	None	1	1	1
Switch 3	None	None	1	1	1
PLC 1	None	None	1	1	1
PLC 2	None	None	1	1	1
Remote IO Module	None	None	1	1	1

Step 6				
Priority	**OT/IT Assets**	**Vulnerability**	**Risk**	**Score**
1	Control Room SCADA HMI	Old SCADA	Take over control Shutdown electricity	20
1	Local HMI Control Computer	Old SCADA	Take over control Shutdown electricity	20
1	SCADA Server 1	Old SCADA	Take over control Shutdown electricity	20
1	SCADA Server 2	Old SCADA	Take over control Shutdown electricity	20
2	Control Room SCADA HMI	Accessible from company network	Take over SCADA Loss of control Shutdown electricity	15
3	Control Room SCADA HMI	Old Hardware	Failure Loss of control	12
3	Local HMI Control Computer	Old Hardware	Failure Loss of control	12
4	Control Room SCADA HMI	Old Operating System	Stolen data	4
4	Local HMI Control Computer	Old Operating System	Stolen data	4
4	SCADA Server 1	Old Operating System	Stolen data	4
4	SCADA Server 2	Old Operating System	Stolen data	4
5	Company Network Switch	None	None	1
5	Switch 1	None	None	1
5	Switch 2	None	None	1
5	Switch 3	None	None	1
5	PLC 1	None	None	1
5	PLC 2	None	None	1
5	Remote IO Module	None	None	1

Prioritize the risks by risk score.

For each risk that matches or exceeds the utility's risk tolerance, define protection measures, their costs, and the risk score reduction (i.e., residual risk) they can achieve.

Step 7					
Priority	**OT/IT Assets**	**Vulnerability**	**Risk**	**Score**	**Protection**
1	Control Room SCADA HMI	Old SCADA	Take over control Shutdown electricity	20	Upgrade SCADA New SCADA
1	Local HMI Control Computer	Old SCADA	Take over control Shutdown electricity	20	Upgrade SCADA New SCADA
1	SCADA Server 1	Old SCADA	Take over control Shutdown electricity	20	Upgrade SCADA New SCADA
1	SCADA Server 2	Old SCADA	Take over control Shutdown electricity	20	Upgrade SCADA New SCADA
2	Control Room SCADA HMI	Accessible from company network	Take over SCADA Loss of control Shutdown electricity	15	Install Firewall
3	Control Room SCADA HMI	Old Hardware	Failure Loss of control	12	Replace Computer
3	Local HMI Control Computer	Old Hardware	Failure Loss of control	12	Replace Computer

Once the protection measure is selected, it must be monitored to ensure that it is performing as expected, thus implying that the investment was appropriate.

Step 8					
Priority	**OT/IT Assets**	**Vulnerability**	**Risk**	**Score**	**Protection**
1	Control Room SCADA HMI	Old SCADA	Take over control Shutdown electricity	20	Upgrade SCADA
1	Local HMI Control Computer	Old SCADA	Take over control Shutdown electricity	20	Upgrade SCADA
1	SCADA Server 1	Old SCADA	Take over control Shutdown electricity	20	New SCADA
1	SCADA Server 2	Old SCADA	Take over control Shutdown electricity	20	New SCADA
2	Control Room SCADA HMI	Accessible from company network	Take over SCADA Loss of control Shutdown electricity	15	Install Firewall
3	Control Room SCADA HMI	Old Hardware	Failure Loss of control	12	Replace Computer
3	Local HMI Control Computer	Old Hardware	Failure Loss of control	12	Replace Computer

Three-phased approach for investment effectiveness assessment by GNERC