Jordan Journal of Energy
Volume 1, Number 2, 2023

ISSN (Online): 2790-7678
ISSN (Print): 2790-766X

Jordan Journal of Energy (JJE)
Journal Homepage: http://dsr.mutah.edu.jo/index.php/jje
JEE an official peer review journal of Mutah University,

Developing a Cybersecurity Risk Management Framework for Non-Technical Losses in National Power Distribution Companies

Abdel Rahman Alzoubaidi[1]* , Asma Najdawi[2] , Mutasem Alzoubaidi[3]

[*1]Electrical Engineering department, Al Balqa Applied University, Amman, Jordan
[1]alzoubaidi@bau.edu.jo
[2] Greater Amman Municipality, Amman , Jordan
[2]najdawiasma@gmail.com
[3] HNTB corporation, Kansa City, Missori, United States
[3]malzoubaidi@hntb.com

Received 2nd July 2023; Accepted 16th August 2023

*Corresponding Author Email: alzoubaidi@bau.edu.jo

ABSTRACT. *Traditionally, power companies are the driving force behind a country's economy and disturbances in its services have severe effects. Advanced metering infrastructure (AMI) grids are vulnerable to network & web security attacks. The objective of this study is to pinpoint the risk mitigation measures that should be integrated into the electric power advanced metering grids of Jordan. The study investigates and proposes a Risk Management Framework (RMF) to minimize the risks of power fraudulent activity. AMI is vulnerable to electricity losses and hence the need to develop a system that would help mitigate this risk. To develop the RMF, we integrate security and privacy into the management activities, to assist in the organizational preparation of the processes and technologies needed for the ongoing energy system IT and OT convergence and digital transformation poses more cybersecurity concerns and essential requirements. We used the Quantitative Risk Management process utilizing the NIST RMF standards for financial risk impacts mitigation of energy losses in the AMI grid. The dependencies and influences between the dimensions considered are investigated, information gathering, and the collection of work data were carried out and used for quantitative analysis. This paper presents a pilot project study in collaboration with EDCO the developed and proposed RMF requirements, risk assessment and, finally recommends the implementation of the selected security controls for the AMI profile protection to mitigate the identified cyber risk.*

Keywords: Smart grid, AMI, Organizational Risk Management Framework (RMF), EDCO, security controls, SCADA security.

1. Introduction. In recent years, the great development in renewable energy resources and increasing of electric power demand poses new challenges on the distribution networks [1]. The present passive distribution networks (PDN) are of dual structure as they consist of substations and loads [2]. Nowadays, there is a need to convert the current PDN into an Active Distribution Network (ADN) of a ternary structure; distributed generations (DGs), substations and loads [3].

In recent years, the great development in renewable energy resources and increasing of electric power demand poses new challenges on the distribution networks [1]. The present passive distribution networks (PDN) are of dual structure as they consist of substations and loads [2]. Nowadays, there is a need to convert the current PDN into an Active Distribution Network (ADN) of a ternary structure; distributed generations (DGs), substations and loads [3]].

The future of electricity is on the Internet of Things (IoT) and recently the Internet of Everything (IoE). Traditional power grids are getting abandoned for smart and more efficient power grids [1]. According to the U.S. Department of Energy, energy reliability is one of the primary reasons behind the move toward smart grids. However, smart grids come with their challenges, such as the need to ensure cybersecurity [2]. As such, cyber security experts need to be involved in the development, and maintenance. Also, monitoring smart grids ensure maximum customer satisfaction and ensure that one of the primary sources of any country's security is maintained [3]. Energy is an essential resource for any country that wishes to ensure maximum security for its citizens, especially from external attacks [4,5,6,7].

The need to ensure cybersecurity in these smart grids is not a matter of convenience or mere speculation, given the recent attacks on various power grids by hackers. On December 23rd, 2015, in Ukraine, for example, the information systems of the three major energy distribution companies got hacked [8]]. Hackers allegedly sponsored by forces and states against the government in Ukraine successfully hacked the power grid and gained control. In the days after this, the country had no electricity, and cybersecurity professionals were the ones who helped to bring the electricity back online. The hack on Ukraine's power grid marked the first-ever successful hack on a power grid, and it marked the turning point in how countries viewed the need to have secure power grids [9,10]. The latter becomes more important with the move to use smart grids in most countries.

The example above about a hack in Ukraine's power grid for political reasons is an extreme one to show why cybersecurity is essential for any power grid. However, there are other lesser reasons why it is vital to protect power grids from intrusion. One such reason is to ensure that energy there is no theft. Smart grids work using advanced metering where the consumers are charged depending on their usage, and the electricity cuts itself off if the subscription of the consumer is depleted. However, malicious consumers and intruders might override such instructions and steal energy from the grid. In addition to this, using a smart grid requires that consumers share their personal information, and this information might get stolen [7] which poses a risk.

Jordan has appreciated the need to use smart grids in its energy distribution. To this end, the Jordan Electrical Power Company is responsible for distributing about 66% of the country's energy consumers, and it intends to use advanced metering systems. Given that energy theft is one of the significant cybersecurity issues that would face such a smart grid, it is crucial to assess the possible vulnerabilities and possible solutions to mitigate this risk [11,12,13,14].

In summary, the critical issue in this study is to investigate the advanced metering infrastructure from an energy theft perspective. Energy theft is one of the most important reasons to implement risk cybersecurity management for energy power distribution in Jordan. The study will also explore the control measures that power companies can take to manage cyber risk to reduce theft energy risk. It will also assess the physical and digital attack surface and vulnerabilities associated with each AMI then make recommendations for appropriate security requirements.

The organization of the rest of this paper are as a follow, in section 2 background, related work in section 3, RMF AMI pilot project in section 4, Finally, the results and conclusion are presented in section 5.

2. Background

2.1 Motivation

The Energy and Minerals Regulatory Commission (EMRC) is responsible for regulating and monitoring the energy sector, generation, transmission, distribution, and electricity supply. EMRC recorded 19,962 cases of electricity theft in 2018. Also, Law enforcement personnel at the EMRC recorded 10,443 cases of theft, while employees at the three electricity distribution companies discovered 6,768 cases [12,13,15]. This month's report on the largest electricity and water theft in the Kingdom, which will now get submitted to the Judicial Authority, stipulated that the thief must get fined 2.7 million JOD. Finally, last month, a joint force of the Public Service Directorate and Gendarmerie seized equipment worth 300 thousand JOD used to embezzle electrical power. The above formal reported issues constitute the driver motivations for conducting this empirical research. Conducting this empirical research will help provide a solution to mitigate the energy theft problem in the Kingdom of Jordan [12,13,15].

2.2 Project Description

The project objective is to conduct pilot project research to investigate electricity losses being the leading concern for power distribution companies for decades. Power distribution companies throughout the world are trying various new methods for detecting electricity non-technical loss. In combination with the innovation in information and communication, technologies Cyber Security threats, more unique and effective non-technical losses detection methods recommended by NIST aiming to implement RMF in the Jordanian power distribution companies to mitigate the risks affecting the smart grid infrastructure. The proposed development and implementation process of risk analysis solution allows for the practical consideration of potential risk determinations. For this pilot project, the Quantitative Risk Management process methodology is employed utilizing the NIST RMF risk mitigation of energy loss in AMI.

3. Related work

Previously various studies have been conducted on smart electricity grid protection against theft and other malicious activities associated with cybersecurity. These projects and studies have identified various vulnerabilities in smart grids and solutions to these vulnerabilities. Langer, Skopik, Smith, and Kammer stetter assessed cybersecurity issues that face smart grids as they evolve from the traditional forms of electricity grids to the new types of smart grids [3]. The researchers understood that smart grids are made of various ICT components that are all vulnerable to theft and other malicious activities. In their article, the researchers sought to provide a solution to assess any possible cybersecurity issues with these smart grids. The researchers recommended a two-stream risk assessment method to determine the various risks in a given smart grid. The research suggested covered both the existing components and the near future developments of any current system. Fig.1 represents the model that the researchers recommended.

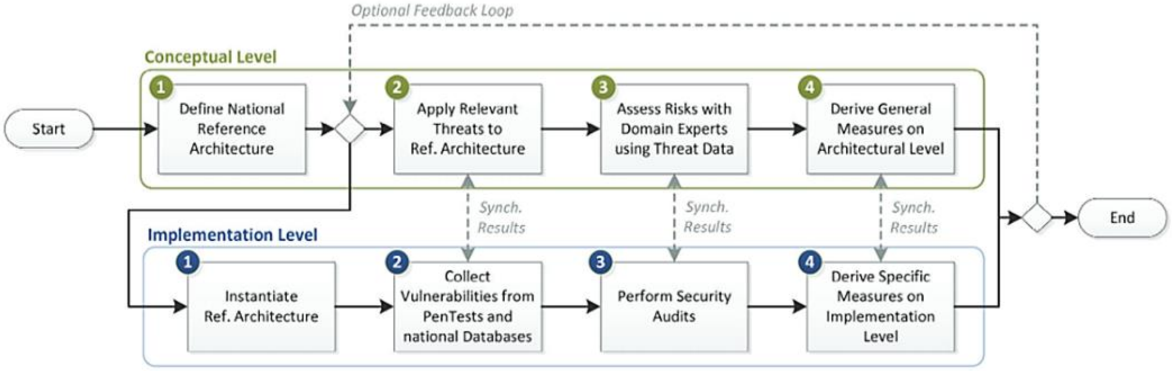
Optional Feedback Loop
Conceptual Level
Start
1 Define National Reference Architecture
2 Apply Relevant Threats to Ref. Architecture
3 Assess Risks with Domain Experts using Threat Data
4 Derive General Measures on Architectural Level
Synch. Results
Synch. Results
Synch. Results
End
Implementation Level
1 Instantiate Ref. Architecture
2 Collect Vulnerabilities from PenTests and national Databases
3 Perform Security Audits
4 Derive Specific Measures on Implementation Level

FIGURE. 1. Conceptual and implementation-based risk assessment in several interrelated steps [3].

The above method got implemented in Australia, and it was also evaluated in the course of the Austrian Research Project. The level of threats in smart buildings, e-mobility, customer premises, low-abvolt generation, medium-abvolt generation, grid test points, primary substation, secondary substation, grid service, and metering were all identified using this assessment process. Authentication, authorization, security mechanisms, integrity, availability, internal and external interfaces, confidentiality, data protection, system maintenance, and system monitoring were among the risks found. This method can be a great place to start while assessing the Jordan electricity grid risks.

In their research, Mathas et al. explored the problems of Advanced Metering Infrastructures (AMI) [5]. The scientific and industrial progression through installing smart meters has increased the demand side of technical and security risk management. Smart meters are an essential element of the AMI, where they enable two-way data communication between service users and utilities provider. The smart meter's real-time measurements generate a large volume of data that can be quickly transmitted to customers. Consumers may benefit from the smart meter's soundless functionality, but security issues and threats are significant problems and risks that should be tackled. Consumers will be unable to use the excellent features provided by smart meters if they are not properly prepared and risk-managed. The feasibility, investment, and need to preserve an acceptable degree of privacy through cybersecurity risk management must all be considered during implementation.

Khattak, Khanji, and Khan also understood the possibility of vulnerabilities in smart meters, given that the Internet of Electricity was getting appreciated by energy companies and governments [2]. Given the advanced metering infrastructure implementations, the researchers decided to investigate the cybersecurity concerns in the increasingly complex smart energy grids. The researchers identified the AMI security issues as smart meter security, data collector security, communication, and network security. The paper suggested the following security control and countermeasure. a) Having the smart meters encrypted that protecting the communication between devices and networks. It would also help to reduce the chances of data and information security getting compromised. b) Authentication mechanism serves the same purpose as smart grid encryptions and ensures that only authorized people have access to critical controls and information in the energy networks, c). The availability mechanism ensures that the availability of the AMI infrastructure does not get compromised through vulnerabilities such as network jamming and packet flooding, and d). Jamming prevention mechanism to help with preventing the jamming vulnerability technique that malicious people might use on the AMI devices and networks. This study is essential for this research since it gives direction on some of the vulnerabilities to look for when assessing the Jordan electric grid and possible solutions for these cybersecurity issues.

Yadav, Kumar, Sharma, and Singh conducted a study to determine the possible cybersecurity issues in smart grids and the possible solutions to these problems [11]. The researchers understood that given that smart grids rely on IoT, various cybersecurity issues must get addressed. The researchers identified the protection of consumer information, system availability, integrity and reliability, and confidentiality as some of the key cybersecurity issues that face the Smart grids. The researchers identified that the key goals of any smart grid cybersecurity are the availability of service, the confidentiality of data, and the integrity of the information shared. The researchers determined that the security of the smart grids would get compromised through 5 main methods, the use of malware, unauthorized access by internal users, the use of replay or repeat false messages, traffic analysis, and DoS attacks. The researchers suggested that the other cybersecurity measures for protecting networks ensure that the above methods do not work on a given smart grid. However, the researchers identified that this is only related to providing the users with efficient electricity availability, protecting their data, and focusing less on other security concerns.

Nonetheless, this is not the first study to identify energy theft as a possible issue in ensuring the cybersecurity of smart grids. Lopez, Sargolzaei, Santana, and Huerta also conducted a study to determine the threats and countermeasures present in smart grids when it comes to cybersecurity and identified energy theft as a possible threat facing smart grids [4]. According to researchers, the intention to steal energy from the grid will interrupt measurements before taking place, tampering with the stored data before, when, or after the measurements have been taken and stored in the meter. Also, one might modify the networks before or during the data logging by the meter. It is thus imperative to ensure that smart grids get protected against energy thefts. The use of theft detectors was the researchers' approach to the issue of energy theft. Theft detectors work by determining the average use of electricity per day against a certain predetermined threshold to assess whether electricity is stolen. If the average use is less than the minimum threshold per day, the assumption is that the energy is stolen.

McLaughlin, Pdkuiko, and McDaniel [6], and [1] went further than Lopez, Sargolzaei, Santana, and Huerta to demonstrate where energy theft might take place in a given smart grid [4]. McLaughlin, Pdkuiko, and McDaniel studied the phenomenon of energy theft in advanced metering structures and found vulnerabilities that help malicious people steal energy [6]. Byres, Franz, and Miller, on the other hand, investigated the phenomenon of vulnerabilities in the SCADA systems using attack trees [1]. When the two are combined, it becomes easy to see the various stages in which malicious persons might steal energy from the systems. Using the concepts developed by [6] and [1] to investigate energy theft would be helpful for this research since it creates a benchmark and a body of knowledge in which the research can progress. The studies by [6] and [1] were limited in that they did not focus on the specific circumstances surrounding Jordan's energy networks and the possible solutions for these energy theft vulnerabilities.

Perhaps, one of the best solutions offered to counter energy theft in smart power grids is provided by Sun, Hahn, and Liu [9]. According to Sun, Hahn, and Liu, various cyberattacks have happened that focused on AMI, including energy theft. The researchers concentrated on energy theft caused by network intruders from external interfaces including smart meters and information hackers. To address the issue of cyber-attacks, the researchers recommended using Anomaly and Intrusion detection systems (ADSs) [9]. These ADSs detect any type of anomaly or possible intrusions in the system and communicate them, alerting those people tasked with ensuring the security of the smart grid system. [1] presented a technique, This report, which focuses on the known sources of AMI threats, offers a holistic view as to how various security issues contribute to electricity theft being addressed. Future research should look at each of the known sources of threats in greater detail, and then apply suitable intelligent algorithms to evaluate data to create a model for timely decision support. [22]..

Summary

The above studies describe the research conducted in line with ensuring the cybersecurity of smart grids. The studies show the different methods and techniques used to detect security threats or possible intrusions and the solutions for ensuring that these security threats and possible intrusions repetition. Given that this study seeks to focus on Jordan, these papers will form a basis for the following research areas, including offering solutions to the vulnerabilities identified in Jordan AMI that may enable intruders to steal energy.

4. RMF AMI pilot project

This pilot project is ongoing research on the Jordanian Power Distribution Companies (PDC) to investigate electrical losses risk mitigation. due to cyber-attacks for the evolving national Smart Grid components implementation and grid digitalization. As a follow-up to our research field of interest, we are harnessing our studies to solve national problems in the field of cybersecurity for energy distribution in Jordan. This pilot research will propose and implement RMF for selected security controls to mitigate risks at the AMI. The RMF developed a risk-based approach process study that incorporates cybersecurity and privacy into the company management activities to aid in the organizational preparation of the processes and technology required to meet the energy system digitalization transformation requirements. The goal is to install smart grid AMI grid security controls on the electric grid for securing a designated region.

4.1 The Study Preparation

This research is carried out along with the agreement and authorization of the Electricity Distribution Company (EDCO) to provide the data and unclassified information and resources for a limited pilot project aimed at RMF implementation. The preliminary kick-off meeting is headed by the company's former General Director and attended by the director-general deputies for administrative, technical, and planning affairs and the concerned CEOs.

National PDCs, EDCO alike various worldwide, is facing electricity theft and bribery in electricity usage as the two most serious issues facing PDCs. The broadness, security, and privacy of these issues limited the scope of the study to a partial RMF controls selection and implementation; other issues and controls are considered for any future collaborative work.

Accordingly, data & information collection was achieved via several meetings with CEOs, department teams, staff, and published reports by national energy stakeholders to lay the floor to collect the data for the scope of this pilot project, making use of the company IT unclassified resources. EDCO has a mandate for distributing electrical energy purchased from the National Electric Power Company (NEPCO) to the southern part of Jordan, the Jordan valley, and many rural areas in the country, operating different transmission and distribution electricity voltages to end-user facilities. This pilot project's scope is restricted to investigating energy losses caused by SMI devices network equipment for a selected area in the company service coverage areas as a model to develop and recommend the RMF to be approved and implemented in phases to mitigate loss risk.

Typically, energy distribution companies, and EDCOs alike, have massive data gathered in their electricity distribution network databases to monitor, control, and manipulate, among other issues, it's Smart Grid electrical loss.

An electrical loss gets caused by resistance in the flow of electric current in electrical networks and transformers. The loss is influenced by the square of the value of the electrical load flowing through medium and low-voltage networks. The voltage at which the networks get operated also affects it. If the current and voltage increase, so the electrical loss increase. Table 1 represents the real electricity loss rates on medium and low voltage networks in EDCO electricity distribution company (2018-2020) [12,13,15].

Table 1 and Fig. 2. shows the company's electric loss rate for 2018 and 2019 was (11.88%), which was higher than the (11.32 %) allowed by the Electricity Sector Regulatory Authority for the tariff period (2018-2019) without penalties. It also shows; that in 2020 the electricity loss increased to (12.88%), consequently exceeding the allowed limits and resulting in financial losses. The loss rate on low voltage increased from (8.2%) in 2018 to (8.6 %) in 2019, while the percentage of loss on MV networks increased from (4.0 %) to (4.5 %) compared the year 2018, 2020 the MV increased to (5.58%). The increased MV and LV are the impact of COVID-19.

Table 1. Electricity loss rates on medium and low voltage networks

Total losses	MV	LV	Year
11.88%	**4.0%**	**8.2%**	**2018**
11.88%	**4.5%**	**8.6%**	**2019**
12.88%	**5.58%**	**5.55%**	**2020**

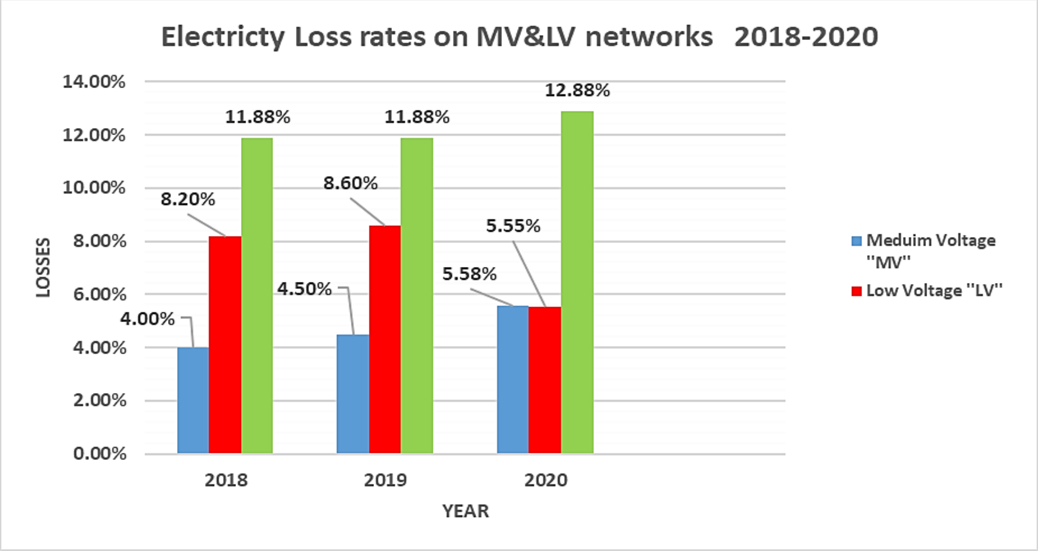

FIGURE. 2. Electricity loss rates on medium and low voltage networks

The company reported a loss rate of (12.88 %) in 2020, an increase from the previous year's loss rate of 11.88 %, and the reasons for this increase are due to the circumstances of the COVID-19, full and partial closures in the Kingdom of Jordan, which have directly affected the increase in electrical loss rates. That reduced the implementation plans to reduce non-technical losses, which led to an increase in the loss by (0.5%) and the most important of these procedures. Increased network tampering and attacks in 2019 were 569 cases, while in 2020, it increased to 710 cases. The latter was a result of customers' behavior and difficult financial circumstances. Also, it was caused by a lack of monitoring, decreased inspection, and detection due to closures and injuries to company staff. Particularly during the first phase of the pandemic, as this resulted in a decrease in the number of meters identified. It also caused an increase in cases of tampering, particularly given the company's inability to take any action, particularly at the stage of complete closure.

During the year 2019, the company worked to make all possible efforts to reduce electrical losses in all its forms through the following:

- Identifying the electrical feeders and areas in which the electrical loss exceeded the performance indicators and determining the necessary measures to reduce the losses on these feeders and regions. The company has implemented several major projects to improve the performance of electrical networks and contribute to reducing electrical loss in the company according to the loss reduction plan.
- To prevent tampering and misuse, the company conducted procedures for the detection and inspection of subscriptions, as well as prosecutions of cases of tampering, in cooperation with the Commission's judicial police and security authority (Public Security and the Gendarmerie), and filed an invitation with the courts. In 2019, there were 892 cases, and in 2020, there were 882 cases.

4.2 Security Control

The presented recommendations are a cornerstone step to studying losses by specifying criteria for cyber-physical and knowledge networks in smart grids. Cybersecurity controls for protections, safeguards, or defensive measures (processes, protocols, applications, procedures, or even other intentions) intended to protect a system or its resources from cyberattacks[17,18,24].

Also, to investigate and characterize principles that define selected cybersecurity controls applied to AMI to protect the smart grid, essential for the RMF development and implementation in the allocated region.

Security controls can be classified as management, technical and operational controls. Management controls apply to problems that management must deal with, and focuses on security policy, preparation, guidelines, and requirements that influence the set of organizational and technological controls to reduce risk and protect the purpose of the company. The proper use of device hardware and software protection capabilities are examples of technical controls, steps that perform in parallel to protect critical and sensitive data, information, and I.T. system functions [16]. Establish automated protection against unauthorized access or misuse, aid in identifying security breaches, and support application and data security standards. Operational controls are mainly concerned with implemented and executed processes by those responsible for the system's use. Operating controls aim to enhance the security of a specific technique or group of systems and are often based on management and technical controls [25].

The smart grid is a complicated system of systems, and to secure its mission of efficient power delivery, it needs more than one layer of security controls. Physical fences and surveillance cameras are only a few of the security controls available, as are encryption algorithms and digital certificates. Applying these security controls on the smart grid prevents the unauthorized disclosure of information, ensures that the information was not modified by an unauthorized source, and ensures that the services and information are available when a user or system requires them. Confidentiality, Integrity, and Availability (CIA) are the priorities of every physical or information security program.

The fact that the smart grid would include both legacy and advanced technologies is an added challenge, making defining the specifically required security controls, and where to put those security controls a difficult decision. The evolving nature of information flow in a smart grid network, as well as new applications for that information, further complicates the security landscape [26].

4.3 Security Controls for AMI

Smart Electricity Meters (SEMs) installation at both client's end and substations is part of Smart Grids' modern digitalization of energy usage and costing scheme, which is controlled by the AMI. The latter supports the bidirectional data connectivity between SEMs and utilities, allowing for the development of a smart grid for the PDCs. The AMI is controlled and managed via instructions in real-time transmission the consumption data, and pricing information to both the utility company and the consumer. The SEM, customer gateway, verbal communication network, and headend are all components of AMI networks. Energy-related data is recorded and communicated by SEMs. Typically, they get arranged to record and supply customers' power usage and billing data at regular intervals, typically every minute.

The client gateway connects the AMI network to customer systems and appliances. This network acts as a connection between the SEM and the AMI headend, permitting transmitted data to flow in both directions. Normally such connections are implemented utilizing Virtual Private Networks (VPN), Fiber, or wireless connections communication technologies owned, controlled, and managed by a third party. AMI security standards, threat sources, and SEM attacks all aim to manipulate data and are major cyber security concerns, although it jeopardizes revenue and customer privacy. Moreover, it is also capable of harming the overall operations of the power grid. Fortunately, the presence of these assaults and other criminal actions such as unauthorized procurement processes, sale, and manipulated equipment by company employees, involvement with consumers, typically via third parties, to commit energy thefts, and the illegitimate purchasing and selling of reserved vouchers. The existence of compromised data in the AMI indicates this. AMI Communications Network serves as a link between the SEM and the AMI headend, allowing data to flow back and forth.

As a result, the protection methods to cope with AMI data, similar to those used to secure data in general, are justified based on access control, analysis and feedback, authentication, authorization, availability, confidentiality, integrity, non-repudiation, privacy, and accountability.

Confidentiality, integrity, availability, and non-repudiation are the four basic AMI specifications (CIAN). However, the continued operation of CIAN is jeopardized due to cyber-attacks, which usually seek to disrupt the AMI for energy theft. Risks to AMI's CIAN mitigation occur in two ways: Viz ensuring the AMI's security requirements are maintained. Furthermore, automatically restored after any security breach or through diligent identification of threat sources [18]. Finally, the eventual following is that relevant models and algorithms are used to manage the parameters of the required systems. It is worth noting that an indication of a violation or threat indicates you have failed to meet all the CIAN's requirements; additionally, analyzing the threats and attackers offers more useful information for proper device management and surveillance [24].

Control is defined as an operation, process, method, or another measure that eliminates damage by avoiding or stopping a security breach, mitigating the risk it can inflict, or finding and revealing it such that corrective action is taken.

When analyzing the smart grid and security to identify Smart Grid Security Controls, it is crucial to determine what needs to be protected and why protection is so critical. The global power grid comprises various technologies and components, and electric utilities have evolved several business practices to ensure the reliable delivery of electricity [19].

AMI Security Profile provides a collection of baseline controls for safeguarding the AMI components. The controls are the outcome of a four-phase procedure that entails the following: 1) smart grid use cases assessment 2) risk assessment, 3) domain analysis, and 4) analyzing and adapting national authority-specified controls. The collection of security measures is comprehensive. Aside from its definition, each step includes an explanation for adoption and, where applicable, future improvements or supplementary guidelines [24].

4.4 Risk Management Framework Methodology

Research methodologies used for cyber security risk are the study of the documents of the act’s norms, international standards, procedures, international legislation, content analysis, comparative methods, and statistical and graphical presentation methods. Information gathering and the collection of work data were carried out by using the statistics of operational plans, risk analyses, and operational procedures. This contribution is the result of the above method in the form of a pilot project research methodology. This interactive research methodology has two parts: investigation and achievement, to establish the practice's progress based on the learning of individuals and workgroups. This pilot study provides the research team and others with a better insight into the problem and potential solutions. The NIST Special Publications 800-53 Rev.4 & Rev.5 to control the security and privacy of information systems, organizations' standard and compliance framework are continuously updated that attempts to flexibly define standards, controls, and assessments based on risk, capabilities, and cost-efficiency, [31]. The NIST SP 800-53 rev4, NIST SP 800-82, and AMI security profile structures, as well as the associated practice standard and controls for risk reduction, provided the theoretical basis for this proposed risk management approach. The selected used rules to perform a quantitative risk analysis, plan risk responses; and apply controls to mitigate risks for this pilot case project are presented in Table 2.

This section includes the pilot project chosen security controls guidelines from the Industrial management and Automation Systems Security measures (IACS) and NIST. IACS is an important part of the smart grid because it tracks and controls industrial processes in the entire power supply chain, from generation to disruption. As shown in Table 2, their safety is critical to the proper functioning of the power grid. Although this pilot project does not include all the smart grid's command and control areas, the security principle remains the same. When implementing a control command, the control system must know that the command is transmitted from an authorized and authenticated source [24].

TABLE 2. Cybersecurity NIST controls specified in power systems' standards.

NIST SP 800-53 Rev.4	NIST SP 800-82	Security Profile for AMI
Access control	Access control	Access control
Audit and accountability	Audit and accountability	Audit and accountability
Awareness and training	Awareness and training	System and communication protection
Identification and authentication	Identification and authentication	System and information integrity
System and communications protection	System and communications protection	System development and maintenance
System and information integrity	System and information integrity	Information and document management

Security measures and practices specific to IACS

Table 3 shows general implementation standards for security controls and procedures, IACS adoption, smart grid adoption, and AMI adoption.

TABLE 3; general application standards within an AMI smart grid security control

NIST SP 800-53
NIST SP 800-82
Security Profile for AMI

4.5 NIST SP 800-53 rev4

Security and Privacy controls for AMI data systems and organizations lay out a foundation of controls for securing information systems in government, based on a variety of statutory and regulatory documents, guidelines, and business criteria. Policy formulation and management, awareness and training, contingency planning, incident response, staff protection, systems procurement, and other security aspects are addressed by the controls, which are organized into 18 families that represent unique security topics. Furthermore, it devotes a substantial portion of its material to illustrating the control selection process, which can be used as part of a risk management strategy.

4.6 NIST SP 800-82

Limiting physical access to IACS networks and reducing access to IACS networks (e.g., through network isolation, DMZ, multilayer, access control), protecting against vulnerabilities, detecting security incidents, maintaining a multidisciplinary security unit, successful networking and information sharing, fault tolerance, graceful decay, device restoration, and defense-in-depth are some of the Key protection priorities identified in NIST SP 800-82. As an outcome, an IACS defense strategy can include IACS-centric policies and procedures, knowledge and training, security across the life cycle of IACS components (from design to disposal), a multi-layered network with critical operations performed in the most protected subnetwork, and other elements derived directly from security objectives. The paper goes through each of these points in detail.

4.7 Electricity Regulatory Framework in Jordan

Jordan has laws and regulations governing the responsible use of nuclear energy and general electricity. The safe use of nuclear energy issues in April, has provisions for authorization, disposal of radioactive material, emergency preparation requirements, administrative sanctions, inspection, safeguards, safety responsibilities, liabilities and punishment, enforcement, and physical protection. It is important to follow the stipulated regulations when dealing with nuclear energy sources, given their toxicity and lethality in case they are not handled well. These are enforced with the help of the Jordan Nuclear Regulatory Commission, which was established in 2007. The rules used to regulate the nuclear energy climate in the country follow the IAEA safety standards, and EU, USDOE, CNSC, IRSN, and KINS commissions to ensure the responsible use of nuclear energy[14].

The general Electricity Law concerns the illegal use of the electrical system, unlawfully connecting, stealing electrical power, or even assisting a person in such activities will result in imprisonment from 6 months to two years. Other Punishments that one might also face include fines of less than two thousand dinars but not more than 10,000 dinars or both imprisonment and a fine. Sabotage will result in imprisonment for a period of one month to one year or a fine of fewer than 500 dinars (not more than 2,000 dinars) or both imprisonment and fine. Negligence results in one week's imprisonment to three months or a fine of not more than 500 dinars or both imprisonment & fine.

These general electric laws are regulated with the help of the EMRC. Electricity tariffs, payment fees, service fees, disbursements, royalties, and link charges to the transmission and distribution system are all determined by the Electricity Regulatory Commission, which was instituted in 2001.

5. Results and conclusion

Figure the RMF framework proposed in this pilot project results from an actual initiation process in which the company team and the researcher (research team) worked together consciously. Losses for real-time data processing over three years. The RMF, as well as the assessment processes for cybersecurity-related threats and mitigation management methodologies, as well as active project team participation, aids the study in becoming more successful in risk management methodology adjustments.

Because of the pilot project's limitations, development and implementation are limited to; General application requirements measures and procedures that specify cybersecurity areas and controls, with the adoption of a smart grid and Security Profile for AMI profile summarized in appendix A [29].

Adapted from NIST 800-53 shows a set of guidelines for conducting security and privacy control assessments for information systems. We recommend systematic assessments, performed in phases for the system implementation. The access control family catalog procedure to assess the security controls and control enhancements in NIST Special Publication 800-53, Rev. 4 & Rev. 5 protection and privacy controls.

The implemented procedures are adaptable and customizable, allowing the company to conduct security and privacy control assessments that aid internal risk management processes and are coherent with the company's acceptable risk tolerance, aiming to develop effective protection and privacy evaluation plans with this information.

5.1 Future Work

The recent annual 2021 report of The National Electric Power Company (NEPCO) stated that the Company's accumulated losses amounted to JD 5,135,023,755 as of 31 December 2021, which exceeds 75% of the paid-in capital. This report is another strong motivation fueling the researcher to undergo this vital research challenge that needs continuous risk assessment, identification & mitigation. Also, Jordan's PDC undergoing digital transformation activities ought to improve its cybersecurity strategies. A Risk Management Plan is needed to guide the project team and managers during the implementation and development of the RMF cyclical process to incorporate principles of security and risk management into the organization's system policies and procedures. A defined document for the RMF Plan that collects all necessary and valuable information for the researcher to manage the appropriate risks, including the RMF objectives and tolerances, the identified methods, strategies, and procedures to detect, assess, plan responses, monitor and control risks, utilizing the defined models to use.

To expand the RMF development and implementation with continuous improvements, extra information from the company team may be required to identify the security requirements and utilize a systematic asset assessment required for RMF practices by acquiring knowledge and encouraging them to engage in the risk management process' phases and feel their contribution in the improvements through effective engagement.

A risk Monitoring and Control process for implementing risk mitigation plans, controlling identified risks, monitoring risks, identifying potential risks, and evaluating the efficacy of risk management systems that have been put in place.

A further direction is to study SCADA security risks associated with data communication networks utilizing Virtual Private Network (VPN) connectivity to connect the AMI and SEMs grids. VPN data communication security on the public network is based on the CIA triad concept in network security. To investigate when VPN may be used, and when to recommend the use of VPN to have protected communication based on anonymity communication. Also SCADA, OT (Operational Technology), and IT (Information Technology) systems have become increasingly interconnected, creating new cybersecurity threats and vulnerabilities.

5.2 Research limitations

As predicted, some challenges arose during the pilot project's implementation and creation of the RMF methodology due to the adoption of a new practice. These challenges were due to the following factors: novelty, the timing of the research study during COVID-19 together with staff working remotely from home; restricted time available; and public awareness of the importance of cybersecurity and risk management. As an innovative approach, the suggested technique, method, and procedures were placed on the project team.

Acknowledgment. This work has been carried out during a sabbatical leave granted to the author Abdel Rahman Alzoubaidi from Al-Balqa' Applied University (BAU) during the academic year 2021-2022. I would like to thank the EDCO power distribution company general manager, deputies, and engineers for their support and assistance in providing the data & information to complete this project.

REFERENCES

[1] B. S. Munir, A. Trisetyarso, M. Reza and B. S. Abbas, Application of Artificial Neural Networks for Power System Oscillation Prediction, *ICIC Express Letters*, vol. 13, no. 9, pp. 815-822, 2019.

[2] L. M. W. G. Fan Zhang, An Integrated Wide Area Protection Scheme for Active Distribution Network Based On Fault Component Principle, *IEEE Transaction on Smart Grid*, vol. 10, no. 1, pp. 392-402, 2019.

[3] V. F. Martins and C. L. T. Borges, Active distribution network integrated planning incorporating distributed generation and load response uncertainties, *IEEE Transactions on Power Systems*, vol. 26, no. 4, pp. 2164-2172, 2011.

[4] X. Chen, Y. Li, M. Zhao, A. Wen and N. Liu, A coordinated strategy of protection and control based

[5] C. Chandraratne, W. L. Woo, T. Logenthiran and R. T. Naayagi, Adaptive Overcurrent Protection for Power Systems with Distributed Generators, *2018 8th International Conference on Power and Energy Systems* (ICPES), 2018.

[6] J. Ma, X. Xiang, R. Zhang, J. L. a. P. Li and J. S. Thorp, Regional protection scheme for distribution network based on logical information, *IET Generation, Transmission & Distribution*, vol. 11, no. 17, pp. 4314-4323, 2017.

[7] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel and K. Vu, Wide-Area Protection and Power System Utilization, *Proceedings of the IEEE*, vol. 93, no. 5, pp. 997-1003, 2005.

[8] M. N. Alam, S. Chakrabarti, A. Sharma and S. C. Srivastava, An Adaptive Protection Scheme for AC Microgrids Using μPMU Based Topology Processor, *2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe* (EEEIC / I&CPS Europe), 2019.

[9] Shalini, S. R. Samantaray and A. Sharma, Enhancing Performance of Wide-Area Back-Up Protection Scheme Using PMU Assisted Dynamic State Estimator, *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5066-5074, 2019.

[10] E. J. Holmes, *Protection of Electricity Distribution Networks*, 3rd Edition, 2011.

[11] E. J., Byres, M., Franz, & D. Miller. (2004, December). The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the international infrastructure survivability workshop (pp. 3-10). Citeseer.

[12] A. M., Khattak, S. I., Khanji, & W. A. Khan, (2019, January). Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In International Conference on Ubiquitous Information Management and Communication (pp. 554-562). Springer, Cham.

[13] L., Langer, F., Skopik, P., Smith, & M. Kammerstetter, (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid. computers & security, 62, 165-176.

[14] C., Lopez, A., Sargolzaei, H., Santana, & C. Huerta (2015). Smart Grid cybersecurity: An overview of threats and countermeasures. Journal of Energy and Power Engineering, 9(7), 632-647.

[15] C. M., Mathas, K. P., Grammatikakis, C., Vassilakis, N., Kolokotronis, V. G., Bilali, & D. Kavallieros, (2020, August). The threat landscape for smart grid systems. In Proceedings of the 15th

International Conference on Availability, Reliability, and Security (pp. 1-7).

[16] S., McLaughlin, D., Podkuiko, & P. McDaniel, (2009, September). Energy theft in the advanced metering infrastructure. In International Workshop on Critical Information Infrastructures Security (pp. 176-187). Springer, Berlin, Heidelberg.

[17] M., Nabil, M., Ismail, M., Mahmoud, M., Shahin, K., Qaraqe, & E. Serpedin, (2019). Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. In Deep Learning Applications for Cyber Security (pp. 73-102). Springer, Cham.

[18] S., Saini, R. K., Beniwal, R., Kumar, R., Paul, & S. Saini, (2018). Modeling for improved cybersecurity in Smart distribution system. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(2), 56-59.

[19] C. C., Sun, A., Hahn, & C. C., Liu, (2018). Cybersecurity of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, 45-56.

[20] L., Streltsov, (2017). The system of cybersecurity in Ukraine: principles, actors, challenges, accomplishments. European Journal for Security Research, 2(2), 147-184.

[21] S. A., Yadav, S. R., Kumar, S., Sharma, & A. Singh, (2016, February). A review of possibilities and solutions of cyber-attacks in smart grids. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 60-63). IEEE.

[22] Ro'ya daily newspaper, https://en.royanews.tv/news/14184/The-shocking-consequences-of-electricity-theft-in-Jordan, retrieved 8/3/2021 Published: 2018-05-06 10:31

[23] Alghad daily newspaper, https://alghad.com/jordans-biggest-power-theft/, retrieved 8/3/2021

[24] Jordan Regulation Commission. 2020. https://web.archive.org/web/20120617064232/http://www.jnrc.gov.jo/About.html

[25] Jordan time's daily newspaper,https://www.jordantimes.com/news/local/15511-power-theft-cases-reported-first-10-months-year-%E2%80%94-emrc retrieved 8/3/2021

[26] Gueltoum Bendiab, Konstantinos-Panagiotis Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis, Stavros Shiaeles: Advanced Metering Infrastructures: Security Risks and Mitigation, https://doi.org/10.1145/3407023.3409229, The 15th International Conference on Availability, Reliability, and Security (ARES 2020), Dublin – Ireland

[27] A. k., Masood "Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasures," May 2019, https://www.researchgate.net/publication/333305127_Smart_Meter_Security_Vulnerabilities_Threat_Impacts_and_Countermeasures

[28] I., Mkpong-Ruffin, D., Umphress, J., Hamilton, & J. Gilbert (2007, October). Quantitative software security risk assessment model. In Proceedings of the 2007 ACM workshop on Quality of protection (pp. 31-33).. DOI: 10.1145/1314257.1314267.

[29] J., Yao, P., Venkitasubramaniam, S., Kishore, L. V., Snyder, & R. S., Blum, (2017, March). Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks. In 2017 51st Annual Conference on Information Sciences and Systems (CISS) (pp. 1-6). IEEE.

[30] R. W., Habash, V., Groza, & K., Burr, (2013). Risk management framework for the power grid cyber-physical security. Current Journal of Applied Science and Technology, 1070-1085.

[31] Y., Guo, C. W., Ten, S., Hu, & W. W., Weaver, (2015, February). Modeling distributed denial of service attack in advanced metering infrastructure. In 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT) (pp. 1-5). IEEE. DOI: 10.1109/ISGT.2015.7131828

[32] M. A., Faisal, Z., Aung, J. R., Williams, & A., Sanchez, (2012, May). Securing advanced metering infrastructure using intrusion detection system with data stream mining. In Pacific-Asia Workshop on Intelligence and Security Informatics (pp. 96-111). Springer, Berlin, Heidelberg.

[33] A. O., Otuoze, M. W., Mustafa, O. O., Mohammed, M. S., Saeed, N. T., Surajudeen-Bakinde, & S., Salisu. (2019). Electricity theft detection by sources of threats for smart city planning. IET Smart Cities, 1(2), 52-60.

[34] R., Leszczyna. (2019). Standards with cybersecurity controls for smart grid A systematic analysis. International Journal of Communication Systems, 32(6), e3910.DOI:10.1002/dac.3910. https://onlinelibrary.wiley.com/doi/10.1049/iet-smc.2019.0045

[35] DHS Sensitive Systems Policy Directive 4300A Version 13.1 July 27th, 2017. https://www.dhs.gov/

[36] P., McDaniel, & S., McLaughlin, (2009). Security and privacy challenges in the smart grid. IEEE Security & Privacy, 7(3), 75-77.

[37] e., Fernandes, J., Jung, and A. Prakash. 2016. Security Analysis of Emerging Smart Home Applications. In 2016 IEEE Symposium on Security and Privacy (S.P.). IEEE, 636–654.

[38] A., Hansen, J., Staggs, and S., Shenoi. 2017. Security analysis of an advanced metering infrastructure. International Journal of Critical Infrastructure Protection, 18, pp.3-19. https://doi.org/10.1016/j.ijcip.2017.03.004

[39] NIST Special Publication 800-53A Assessing Security and Privacy Controls in Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations http://dx.doi.org/10.6028/NIST.SP.800-53Ar4.

[40] The National Electric Power Company (NEPCO) annual 2021 report, https://www.nepco.com.jo/store/docs/web/2021_en.pdf , accessed 25nov2022.

[41] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, retrieved, Nov. 22 from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

APENDIX A

A catalog of procedures to assess the security controls and control enhancements in Special Publication 800-53.

FAMILY: ACCESS CONTROL

AC-1	**ACCESS CONTROL FOR EMPLOYEES**
	Assessment Objective: Determine if the organization
AC-1(a)(1)	
AC-1(a)(1)[1]	develops and documents an access control policy that addresses:
AC-1(a)(1)[1][a]	purpose;
AC-1(a)(1)[1][b]	scope;
AC-1(a)(1)[1][c]	roles;
AC-1(a)(1)[1][d]	responsibilities;
AC-1(a)(1)[1][e]	management commitment;
AC-1(a)(1)[1][f]	coordination among organizational entities;
AC-1(a)(1)[1][g]	compliance;
AC-1(a)(1)[2]	defines personnel or roles to whom the access control policy are to be disseminated;
AC-1(a)(1)[3]	disseminates the access control policy to organization-defined personnel or roles;
AC-1(a)(2)	
AC-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the access control policy and associated access control controls;
AC-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
AC-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
AC-1(b)(1)	
AC-1(b)(1)[1]	defines the frequency to review and update the current access control policy;
AC-1(b)(2)[2]	reviews and updates the current access control policy with the organization-defined frequency;
AC-1(b)(2)	
AC-1(b)(2)[1]	defines the frequency to review and update the current access control procedures; and
AC-1(b)(2)[2]	Reviews and updates the current access control procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine** [SELECT FROM Access control policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with access control responsibilities; organizational personnel with information security responsibilities]	

AC-2(12)	**ACCOUNT MONITORING / ATYPICAL USAGE**
	Assessment Objective: Determine if the organization
AC-2(12)(a)	
AC-2(12)(a)[1]	defines atypical usage to be monitored for information system accounts;
AC-2(12)(a)[2]	monitors information system accounts for organization defined atypical
AC-2(12)(b)	
AC-2(12)(b)[1]	defines personnel or roles to whom atypical usage of information system accounts are to be reported; and
AC-2(12)(b)[2]	Reports atypical usage of information system accounts to organization-defined personnel or roles.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system monitoring records; information system audit records; audit tracking and monitoring reports; other relevant documents or records]. **Interview:** [SELECT FROM organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities]. **Test:** [SELECT FROM: Automated mechanisms implementing account management functions]	

AC-3(7)	**ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL**
	Assessment Objective: Determine if the organization
AC-3(7)[1]	the organization defines roles to control information system access;
AC-3(7)[2]	the organization defines users authorized to assume the organization-defined roles;
AC-3(7)[3]	the information system controls access based on organization-defined roles and users authorized to assume such roles
AC-3(7)[4]	the information system enforces a role-based access control policy over defined:
AC-3(7)[4][a]	subjects, and
AC-3(7)[4][b]	Objects.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Access control policy; role-based access control policies; procedures addressing access enforcement; security plan, information system design documentation; information system configuration settings and associated documentation; list of roles, users, and associated privileges required to control information system access; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers]. **Test**: [SELECT FROM: Automated mechanisms implementing role-based access control policy].	
AC-7	**UNSUCCESSFUL LOGIN ATTEMPTS**
	Assessment Objective: Determine if the organization
AC-7(a)	
AC-7(a)[1]	the organization defines the number of consecutive invalid logon attempts allowed to the information system by a user during an organization-defined time period;
AC-7(a)[2]	the organization defines the time period allowed by a user of the information system for an organization-defined number of consecutive invalid logon attempts;
AC-7(a)[3]	the information system enforces a limit of organization-defined number of consecutive invalid logon attempts by a user during an organization-defined time period;
AC-7(b)	
AC-7(b)[1]	the organization defines account/node lockout time period or logon delay algorithm to be automatically enforced by the information system when the maximum number of unsuccessful logon attempts is exceeded;
AC-7(b)[2]	the information system when the maximum number of unsuccessful logon attempts is exceeded, automatically:
AC-7(b)[2][a]	locks the account/node for the organization-defined time period;
AC-7(b)[2][b]	locks the account/node until released by an administrator; or
AC-7(b)[2][c]	Delays next logon prompt according to the organization-defined delay algorithm.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with information security responsibilities; system developers; system/network administrators]. **Test:** [SELECT FROM: Automated mechanisms implementing access control policy for unsuccessful logon attempts].	

AC-14	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**
	Assessment Objective: Determine if the organization
AC-14(a)	
AC-14(a)[1]	defines user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions;
AC-14(a)[2]	identifies organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
AC-14(b)	documents and provides supporting rationale in the security plan for the Information system, user actions not requiring identification or authentication.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Access control policy; procedures addressing permitted actions without identification or authentication; information system configuration settings and associated documentation; security plan; list of user actions that can be performed without identification or authentication; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: System/network administrators; organizational personnel with information security responsibilities]	

AC-18(5)	**WIRELESS ACCESS | ANTENNAS/TRANSMISSION POWER LEVELS**
	Assessment Objective: Determine if the organization
AC-18(5)[1]	selects radio antennas to reduce the probability that usable signals can be received outside of organization-controlled boundaries; and
AC-18(5)[2]	Calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [SELECT FROM: System/network administrators; organizational personnel with information security responsibilities]. **Test:** [SELECT FROM: Wireless access capability protecting usable signals from unauthorized access outside organization-controlled boundaries].	

FAMILY: AWARENESS AND TRAINING

AT-1	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**
	Assessment Objective: Determine if the organization
AT-1(a)(1)	
AT-1(a)(1)[1]	develops and documents an security awareness and training policy that addresses:
AT-1(a)(1)[1][a]	purpose;
AT-1(a)(1)[1][b]	scope;
AT-1(a)(1)[1][c]	roles
AT-1(a)(1)[1][d]	responsibilities;
AT-1(a)(1)[1][e]	management commitment;
AT-1(a)(1)[1][f]	coordination among organizational entities;
AT-1(a)(1)[1][g]	compliance;
AT-1(a)(1)[2]	defines personnel or roles to whom the security awareness and training policy are to be disseminated;
AT-1(a)(1)[3]	disseminates the security awareness and training policy to organization-defined personnel or roles;
AT-1(a)(2)	
AT-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
AT-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
AT-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;

AT-1(a)(2)	
AT-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
AT-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated
AT-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
AT-1(b)(1)	
AT-1(b)(1)[1]	defines the frequency to review and update the current security awareness and training policy;
AT-1(b)(1)[2]	reviews and updates the current security awareness and training policy with the organization-defined frequency;
AT-1(b)(2)	
AT-1(b)(2)[1]	defines the frequency to review and update the current security awareness and training procedures; and
AT-1(b)(2)[2]	Reviews and updates the current security awareness and training procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].	

AT-2	**SECURITY AWARENESS TRAINING**
	Assessment Objective: Determine if the organization
AT-2(a)	provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users;
AT-2(b)	provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes; and
AT-2(c)	
AT-2(c)[1]	defines the frequency to provide refresher security awareness training thereafter to information system users (including managers, senior executives, and contractors); and
AT-2(c)[2]	provides refresher security awareness training to information users (including managers, senior executives, and contractors) with the organization-defined frequency
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records]. **Interview: [**SELECT FROM: Organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities; organizational personnel comprising the general information system user community]. **Test:** [SELECT FROM: Automated mechanisms managing security awareness training]

AT-2(2)	**SECURITY AWARENESS TRAINING| INSIDER THREAT**
	Assessment Objective: Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].

AT-3(1)	**ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS**
	Assessment Objective: Determine if the organization

AT-3(1)[1]	defines personnel or roles to be provided with initial and refresher training in the employment and operation of environmental controls;
AT-3(1)[2]	provides organization-defined personnel or roles with initial and refresher training in the employment and operation of environmental controls
AT-3(1)[3]	defines the frequency to provide refresher training in the employment and operation of environmental controls; and
AT-3(1)[4]	provides refresher training in the employment and operation of environmental Controls with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. **Interview**: [SELECT FROM: Organizational personnel with responsibilities for role-based security training; organizational personnel with responsibilities for employing and operating environmental controls]	

AT-2(2)	**SECURITY AWARENESS TRAINING| INSIDER THREAT**
	Assessment Objective: Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. **Interview**: [SELECT FROM organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].

FAMILY: AUDIT AND ACCOUNTABILITY

AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING**
	Assessment Objective: Determine if the organization
AU-6(a)	
AU-6(a)[1]	defines the types of inappropriate or unusual activity to look for when information system audit records are reviewed and analyzed;
AU-6(a)[2]	defines the frequency to review and analyze information system audit records for indications of organization-defined inappropriate or unusual activity;
AU-6(a)[3]	reviews and analyzes information system audit records for indications of organization-defined inappropriate or unusual activity with the organization-defined frequency;
AU-6(b)	
AU-6(b)[1]	. defines personnel or roles to whom findings resulting from reviews and analysis of information system audit records are to be reported; and
AU-6(b)[2]	Reports findings to organization-defined personnel or roles.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities].	

FAMILY: IDENTIFICATION AND AUTHENTICATION

IA-2	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**
	Assessment Objective: Determine if the organization: Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated	

documentation; information system audit records; list of information system accounts; other relevant documents or records].
Interview: [SELECT FROM: Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers].
Test: [SELECT FROM: Organizational processes for uniquely identifying and authenticating users; automated mechanisms supporting and/or implementing identification and authentication capability]

IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**
	Assessment Objective: Determine if
IA-3[1]	the organization defines specific and/or types of devices that the information system uniquely identifies and authenticates before establishing one or more of the following:
IA-3[1][a]	a local connection;
IA-3[1][b]	a remote connection; and/or
IA-3[1][c]	a network connection; and
IA-3[2]	
IA-3[2][a]	a local connection
IA-3[2][b]	a remote connection; and/or
IA-3[2][c]	a network connection

POTENTIAL ASSESSMENT METHODS AND OBJECTS:
Examine: [SELECT FROM: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers].
Test: [SELECT FROM: Automated mechanisms supporting and/or implementing device identification and authentication capability].]

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

SC—1	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**
	Assessment Objective: Determine if the organization
SC-1(a)(1)	
SC-1(a)(1)[1]	develops and documents a security awareness and training policy that addresses:
SC-1(a)(1)[1][a]	purpose;
SC -1(a)(1)[1][b]	scope;
SC-1(a)(1)[1][c]	roles
SC -1(a)(1)[1][d]	responsibilities;
SC -1(a)(1)[1][e]	management commitment;
SC -1(a)(1)[1][f]	coordination among organizational entities;
SC -1(a)(1)[1][g]	compliance;
SC-1(a)(2)	
SC-1(a)(1)[2]	defines personnel or roles to whom the security awareness and training policy are to be disseminated;
SC-1(a)(1)[3]	disseminates the security awareness and training policy to organization-defined personnel or roles;
SC-1(a)(2)	
SC-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SC-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
SC -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SC -1(a)(2)	
SC -1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SC -1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated

SC -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SC -1(b)(1)	
SC -1(b)(1)[1]	defines the frequency to review and update the current security awareness and training policy;
SC -1(b)(1)[2]	reviews and updates the current security awareness and training policy with the organization-defined frequency;
SC -1(b)(2)	
SC -1(b)(2)[1]	defines the frequency to review and update the current security awareness and training procedures; and
SC -1(b)(2)[2]	Reviews and updates the current security awareness and training procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].	

FAMILY: SYSTEM AND INFORMATION INTEGRITY

SI—1	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**
	Assessment Objective: Determine if the organization
SI-1(a)(1)	
SI -1(a)(1)[1]	develops and documents a security awareness and training policy that addresses:
SI -1(a)(1)[1][a]	purpose;
SI -1(a)(1)[1][b]	scope;
SI-1(a)(1)[1][c]	roles
SI -1(a)(1)[1][d]	responsibilities;
SI -1(a)(1)[1][e]	management commitment;
SI -1(a)(1)[1][f]	coordination among organizational entities;
SI -1(a)(1)[1][g]	compliance;
SI-1(a)(2)	
SI -1(a)(1)[2]	defines personnel or roles to whom the security awareness and training policy are to be disseminated;
SI -1(a)(1)[3]	disseminates the security awareness and training policy to organization-defined personnel or roles;
SI -1(a)(2)	
SI-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SI-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;
SI -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SI -1(a)(2)	
SI -1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;
SI -1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated
SI -1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;
SI -1(b)(1)	
SI -1(b)(1)[1]	defines the frequency to review and update the current security awareness and training policy;
SI -1(b)(1)[2]	reviews and updates the current security awareness and training policy with the organization-defined frequency;
SI -1(b)(2)	
SI -1(b)(2)[1]	defines the frequency to review and update the current security awareness and training procedures; and
SI -1(b)(2)[2]	Reviews and updates the current security awareness and training procedures with the organization-defined frequency.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness and training policy and procedures; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].	

FAMILY: Maintenance

MA-6	**TIMELY MAINTENANCE**
	ASSESSMENT OBJECTIVE: **Determine if the organization:**
MA-6[1]	defines information system components for which maintenance support and/or spare parts are to be obtained;
MA-6[2]	defines the time period within which maintenance support and/or spare parts are to be obtained after a failure;
MA-6[3]	
MA-6[3][a]	obtains maintenance support for organization-defined information system components within the organization-defined time period of failure; and/or
MA-6[3][b]	obtains spare parts for organization-defined information system components within the organization-defined time period of failure
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Information system maintenance policy; procedures addressing information system maintenance; service provider contracts; service-level agreements; inventory and Availability of spare parts; security plan; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with information system maintenance responsibilities; organizational personnel with acquisition responsibilities; organizational Personnel with information security responsibilities; system/network administrators]. **Test:** [SELECT FROM: Organizational processes for ensuring timely maintenance].	

MA-6(2)	**TIMELY MAINTENANCE/PREDICTIVE MAINTENANCE**
	ASSESSMENT OBJECTIVE: **Determine if the organization:**
MA-6(2)[1]	defines information system components on which predictive maintenance is to be performed;
MA-6(2)[2]	defines time intervals within which predictive maintenance is to be performed on organization-defined information system components; and
MA-6(2)[3]	performs predictive maintenance on organization-defined information system Components at organization-defined time intervals.
POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine: [SELECT FROM: Information system maintenance policy; procedures addressing information system maintenance; service provider contracts; service-level agreements; security plan; maintenance records; list of system components requiring predictive maintenance; other Relevant documents or records].** **Interview: [SELECT FROM: Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities. System/network administrators].** **Test: [SELECT FROM: Organizational processes for predictive maintenance; automated mechanisms Supporting and/or implementing predictive maintenance].**	