Task 1: Developing an Incident Response Policy According to SAMA Cyber Security Framework, fill in the table to answer the following questions:

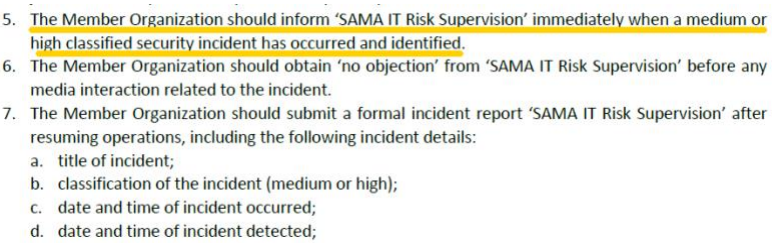
Task 1.1: Does the document clearly define the criteria for an incident? If so, show it. If not, define the criteria for an incident?

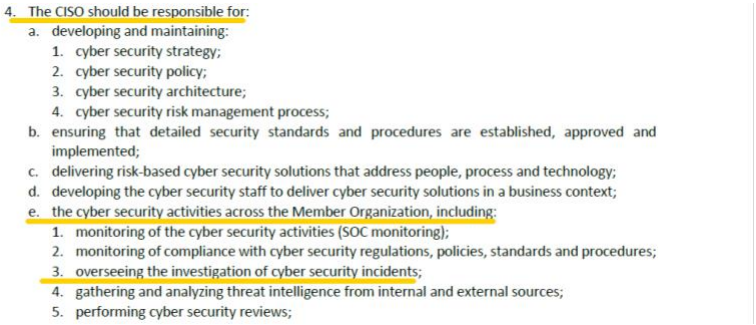
Task 1.2: Does the document clearly define severity level for incidents? If so, show it. If not, what information is the document missing?

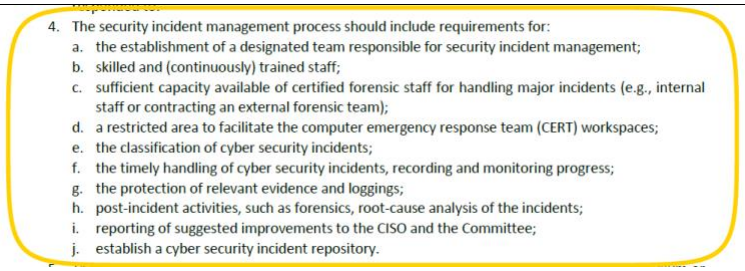
Task 1.3: Does the document define roles and responsibilities? If so, describe the response structure. If not, what information is the document missing?

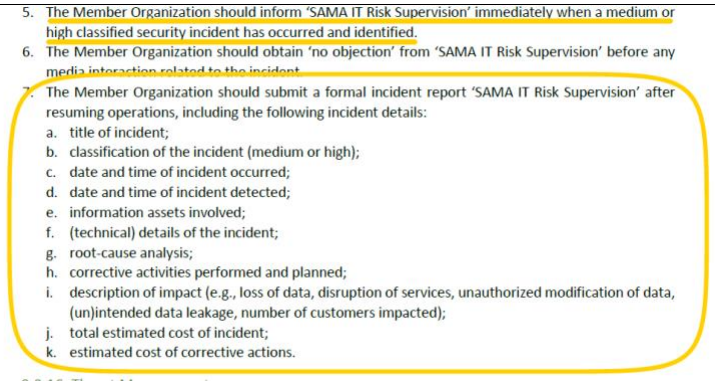
Task 1.4: Does the document include notification requirements? If yes, what laws are referenced and why? If no, what laws should be referenced?

Component	Availability (Choose Yes or No)	Reasons
The criteria for an incident	No	Definition of the criteria for SAMA cybersecurity incident: - A cybersecurity incident is an adverse event that may affect the member organization, the general public, the member Organization's customers or partners. - Unauthorized access, whether actual or suspected, to customer data or employee data, as well as the possibility of modification to it, and that data includes the financial account or credit card, which consists of the card numbers and names of their owners, the expiration of the card and service codes. - The actual or suspected event that negatively affects availability when the services provided to the Member Organization's customers are disrupted. - Actual or suspected events negatively affect the integrity of a Member Organization's intellectual property, either by modifying or acquiring it. - Actual or suspected event capable of sabotaging the working of networks within member organization, and computing services. - Actual or suspected events have not been identified in member organizations before, so it is necessary to classify the accident by the management urgently. - All member Organizations' employees and partners must report cybersecurity incidents, whether suspected or previously known.

		- The Cybersecurity Incident Policy must be applied equally to incidents within member organizations, and incidents of third parties.
Severity level for incidents	Yes	A severity level for incidents is existing in (Page:34, Section: 3.3.15 Cybersecurity Incident Management, Point: 5)  5. The Member Organization should inform 'SAMA IT Risk Supervision' immediately when a medium or high classified security incident has occurred and identified. 6. The Member Organization should obtain 'no objection' from 'SAMA IT Risk Supervision' before any media interaction related to the incident. 7. The Member Organization should submit a formal incident report 'SAMA IT Risk Supervision' after resuming operations, including the following incident details: a. title of incident; b. classification of the incident (medium or high); c. date and time of incident occurred; d. date and time of incident detected; But it does not Clearly define the incident definition severity levels. • **Incident Severity Levels.** - The definition of incidents for cybersecurity should include incident severity levels based on the legal impact, reputation, and operational impact of member organizations. - Cybersecurity incidents are any harmful event that threatens the information or information system. Accidents are classified according to their severity in relation to the impact on banks. The level of risk is set by the management or cybersecurity investigator. - The Member Organization should inform 'SAMA IT Risk Supervision' immediately when a medium or high classified security incident has occurred and identified. • **Level 1 Incidents:** - They are cybersecurity incidents that cause very great harm to customers, the public, or the business of the member organization, and violate the member organization's regulations or laws. - Level 1 incidents must be dealt with promptly when reported. - An internal notification is required for each Chief Executive Officer (CEO), Chief Operating Officer (COO), legal counsel, Chief Information Security Officer (CSO), and designated incident handler. - Such as actual or suspected exposure to the client's protected information, a denial of service attack (DOS), the theft of any device that contains legally protected information, theft of any media on any of the bank's devices and their containment of confidential information for customers, employees, or member organization's partners, a notification from a client or business partner that his data has been breached, or direct actions that violate local or legal regulations of the member organization. • **Level 2 Incidents:** - It exposes the member organization to danger or unauthorized access to non-critical information and systems, or threats to attack

		the systems, or any act considered a possible violation of the law or regulations. - The response time for level 2 incidents is within four hours. - An internal notification is required for each Chief Operating Officer (COO), legal counsel, Chief Information Security Officer (CISO), and designated incident handler. - Such as when malware is detected on an organization's systems. When the warning signs of a potential exploitation are detected. Notification by a third party of an imminent attack on the organization. • **Level 3 Incidents:** - They are situations that can be solved and contained by the owner of the information or HR personnel. Lack of evidence or suspicion of harm to the information, processes, or services provided to the customer. - The response time for level 3 incidents is within 24 hours. - An internal notification is required for each Chief Information Security Officer (CISO) and designated incident handler. - Such as detection or suspicion of malware on the workstation. The user's access to sites that are not within his authority. • **Report accidents:** - All employees are required to report any discovery of actual or suspected accidents, but they should not specify the level of severity, and this is for experienced employees.
Roles and responsibilities	Yes	Roles and responsibilities for incidents response exists in (Page:16-, Section: 3.1.4 Cyber Security Roles and Responsibilities, Point: 4-e-3) CISO:  4. The CISO should be responsible for: a. developing and maintaining: 1. cyber security strategy; 2. cyber security policy; 3. cyber security architecture; 4. cyber security risk management process; b. ensuring that detailed security standards and procedures are established, approved and implemented; c. delivering risk-based cyber security solutions that address people, process and technology; d. developing the cyber security staff to deliver cyber security solutions in a business context; e. the cyber security activities across the Member Organization, including: 1. monitoring of the cyber security activities (SOC monitoring); 2. monitoring of compliance with cyber security regulations, policies, standards and procedures; 3. overseeing the investigation of cyber security incidents; 4. gathering and analyzing threat intelligence from internal and external sources; 5. performing cyber security reviews; (Page:34, Section: 3.3.15 Cybersecurity Incident Management, Point: 4) Incident management process:

		 4. The security incident management process should include requirements for: a. the establishment of a designated team responsible for security incident management; b. skilled and (continuously) trained staff; c. sufficient capacity available of certified forensic staff for handling major incidents (e.g., internal staff or contracting an external forensic team); d. a restricted area to facilitate the computer emergency response team (CERT) workspaces; e. the classification of cyber security incidents; f. the timely handling of cyber security incidents, recording and monitoring progress; g. the protection of relevant evidence and loggings; h. post-incident activities, such as forensics, root-cause analysis of the incidents; i. reporting of suggested improvements to the CISO and the Committee; j. establish a cyber security incident repository. Roles and responsibilities for incidents response structure are missing in this document: • **The incident response coordinator (IRC):** - It is the central point of contact for all actual or suspected incidents to investigate these incidents and also to record them. • **Designated incident handlers (DIHs):** - Senior staff with experience in crisis management, communication skills, and stamina in order to deal with cybersecurity incidents. • **The incident response team (IRT):** - It is a team responsible for further incident analysis, evidence handling, containment, elimination, recovery, notification, and post-incident activities. • **Computer Security Incident Response Team (CSIRT):** - It is the team that works side by side with the information security teams. Focuses on investigating computer security incidents. The InfoSec team implements security, monitoring, and policy configurations within a member organization. • **Incident response structure for roles and responsibilities:** - The accident was reported to the Incident response coordinator IRC. - The IRC informs the DIH, and they evaluate the accident report, and if it is not an actual accident, it will be sent back to the IRC for departmental follow-up. - If it evaluates as an accident, it is sent to the IRT, and here the incident response process further analysis, eradication and recovery, containment, notification, and post-incident activities.
Include notification requirements	Yes	Notification requirements are existing in (Page:34, Section: 3.3.15 Cybersecurity Incident Management, Point: 5,7)

		 5. The Member Organization should inform 'SAMA IT Risk Supervision' immediately when a medium or high classified security incident has occurred and identified. 6. The Member Organization should obtain 'no objection' from 'SAMA IT Risk Supervision' before any media interaction related to the incident. 7. The Member Organization should submit a formal incident report 'SAMA IT Risk Supervision' after resuming operations, including the following incident details: a. title of incident; b. classification of the incident (medium or high); c. date and time of incident occurred; d. date and time of incident detected; e. information assets involved; f. (technical) details of the incident; g. root-cause analysis; h. corrective activities performed and planned; i. description of impact (e.g., loss of data, disruption of services, unauthorized modification of data, (un)intended data leakage, number of customers impacted); j. total estimated cost of incident; k. estimated cost of corrective actions. • The law does not exist, but depending on the US referenced to Gramm-Leach-Bliley Act (GLBA). - It applies to any organization that deals with money and securities. • Member organization Financial Institution Customer Information: - Customers' member organizations must be notified of an accident of unauthorized access to their financial information; it must be presented clearly and explicitly. 1. Description of the accident. 2. Clarify the type of information accessed unauthorized. 3. Measures taken by the member organization to protect clients from further unauthorized access. 4. Phone number for additional information by a member organization. 5. Remind clients to report suspected identity theft incidents to the member organization.

Task 1.5: By using your answers above, write an IT security incident response policy to define criteria pertaining to an information security incident, to define roles and responsibilities, and to classify incidents by severity and assigned response and notification requirements.

IT security incident response Policy

OUTLINE:

1. Version Control

Version	data	Author by	Description
1.0	May 2017	Ahmed Al Sheikh Deputy Governor for Supervision	Saudi Arabian Monetary Authority SAMA

2. Introduction

1. The Information Technology (IT) Security Incident Response Policy defines the responsibilities of SAMA (“the Member Organizations”).

To maintain the protection of information assets and online services.
The stakes are high when it involves the confidentiality, integrity, and availability of information assets and applying new online services and new developments (e.g., Fintech, blockchain); while improving resilience against cyber threats.
The objective of the follows:
1-To create a common approach for addressing IT Security Incident Response Policy within the Member Organizations.
2-To achieve an appropriate maturity level of IT Security Incident Response Policy controls within the Member Organizations.
3-To ensure IT Security Incident Response Policy risks are properly managed throughout the Member Organizations.
4-Confidentiality – protected from unauthorized disclosure or (un)intended leakage of sensitive data.
5-Integrity – protected from unauthorized modification, which may include authenticity and non-repudiation.
6- Availability – protected from unauthorized disruption.
The policy incident response applicable to all or any Member Organizations regulated by SAMA, which include the following:

- All Banks operating in Saudi Arabia.
- All Insurance and/or Reinsurance Companies operating in Saudi Arabia.
- All Financing Companies operating in Saudi Arabia.
- All Credit Bureaus operating In Saudi Arabia.
- The Financial Market Infrastructure

Responsibilities of the member organization policy incident response IT security:

- SAMA is the owner and is responsible for periodically updating the policy. The Member Organizations are responsible for adopting and implementing the policy.
- SAMA is solely responsible for providing interpretations of the principles, objectives, and control considerations if required.

policy incident response IT security provides cybersecurity controls which apply to the information assets of the Member Organization, including:

- Electronic information.
- Physical information (hardcopy).
- Applications, software, electronic services, and databases.
- Computers and electronic machines (e.g., ATM).
- Information storage devices (e.g., hard disk, USB stick).
- Premises, equipment, and communication networks (technical infrastructure).

The Framework provides direction for cybersecurity requirements for Member Organizations and its subsidiaries, staff, third parties, and customers.

3. Policy Statement:

The IT Security Incident Response Policy defines the responsibilities of Member Organization. Staff when responding to or reporting security incidents. It delineates roles within the Computer Security Incident Response Team CISO should be responsible and descriptions which members of Member Organization administration should be involved in different kinds of security incidents.

● Criteria of information security incident

1. Includes defining the regulatory criteria for IT security incident response Policy for the Saudi Monetary Agency SAMA.

Policy Statement:

- A IT security incident is a negative event that will affect the bank, the overall public, the Member Organization customers or partners.
- Member Organization, IT security incident, is defined as follows:
- Unauthorized access, whether actual or suspected, to customer data or employee data, also as the possibility of modification to that, which data includes the financial account or credit card, which includes the card numbers and names of their owners, the expiration of the card and service codes.
- Actual or suspected event that negatively affects availability when the services provided to the Member Organization customers are disrupted.
- Actual or suspected event negatively affects the integrity of Member Organization intellectual property, either by modifying or acquiring it.
- Actual or suspected event capable of sabotaging the working of networks within Member Organization, and computing services.
- Actual or suspected event has not been identified in Member Organization ` before, so it's necessary to urgently classify the accident by the management.
- All Member Organization employees and partners are required to report cybersecurity incidents, whether suspected or previously known.
- The IT security incident response Policy must be applied equally to incidents within Member Organization and incidents of third parties.

● Roles and responsibilities

IT Security Officer—The IT Security Officer is responsible for assessing the initial scope of a security incident, assembling the Member Organization Incident Management Team, and appointing the Incident Manager.

Incident reporting—All members of the Member Organization are required to report actual or suspected security incidents. All suspected security incidents should be reported to the Member Organization Customer Service Center at 798-874-8180

Incident manager—This role is designated by the IT Security Officer and can lead the response to the incident. This is often a technical role and can coordinate the work of log collection, evidence preservation, and analysis activities.

● Incident’s severity levels and assigned response and notification requirements

Incident response will be addressed, supported by the severity of the incident. Incident severity takes several factors into account:
incident severity levels supported the legal impact, reputation, and operational impact of member Organization. Sensitivity of the data involved, the number of end-users impacted, and its overall impact on the ability of the Member Organization to satisfy its mission. Incident severity also are used to determine who manages an incident, who is informed about an incident, and also the extent and immediacy of the response to the incident.

High:
A security incident will be considered “high” if any of the subsequent characteristics are present:

- IT security incidents cause very great harm to customers, the general public, or the business of the member organization, and violate the member organization’s regulations or laws.
  Poses a serious threat of financial risk or legal liability
- Threatens to reveal (or does expose) level 1 data as defined by the data classification Policy
- Threatens to propagate to or attack other networks, or organizations internal or external to the member organization’s
- Actual or suspected exposure to the client's protected information, a denial of service attack (DOS), the theft of any device that contains legally protected information, theft of any media on any of the bank's devices, and their containment of confidential information for patrons, employees or member organization’s partners, a notification.
- Threats to human life or property when received by the IT Security Office.

Medium:
A security incident are going to be considered “medium” if any of the following characteristics are present:

Threatens to impact (or does impact) a significant number of systems or people. The member organizations can still function, but a group, department, unit, or building could also be unable to perform its mission.
An internal notification is required for every Chief Operating Officer (COO), legal counsel, Chief Information Security Officer (CISO), and designated incident handler.
Systems impacted contain only level 2 and/or level 3 data
Impacts a non-critical system or service.
Low:
Low severity incidents haven't any characteristics from the “medium” or “high” categories and may include the following:
Only a small number of people or systems are impacted
Systems impacted contain only level 3 data
Little to no risk of the incident spreading or impacting other organizations or networks.
An internal notification is required for every Chief Information Security Officer (CISO)and designated incident handler.

Such as detection or suspicion of malware on the workstation. The user's access to sites that aren't within his authority.

- **notification requirements**

policy statement
•It applies IT Security Incident Response Policy to any organization that deals with money and securities.
•Member organization Financial Institution Customer Information:
-Customers' member organizations must be notified of an accident of unauthorized access to their financial information; it must be presented clearly and explicitly.
1. Description of the accident.
2. Clarify the type of information accessed unauthorized.
3. Measures taken by the member organization to protect clients from further unauthorized access.
4. Phone number for additional information by a member organization.
5. Remind clients to report suspected identity theft incidents to the member organization.
•The IT security team is responsible for initial assessment of an
incidents severity based on the scope, scale and risk of the incident.

4. Policy exceptions

1. Requests for exceptions to any information security policies could also be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the CISO for review and approval according to the exception procedures published by the CISO.

Frequency of Policy Review
The CISO must review information security policies and procedures annually, at a minimum. This policy is subject to revision based upon the findings of those reviews.
Chief Information Security Officer CISO:

identify solutions that enable consistency in compliance and aggregate and report on available compliance metrics.
develop, establish, maintain, and enforce information security policy and relevant standards and processes.
educate the member Organization community about individual and organizational information security responsibilities.
measure and report on the effectiveness of member Organization information security efforts; and
delegate individual responsibilities and authorities specified in this policy or associated standards and procedures, as necessary.

5. Policy enforcement clause

Compliance with this policy is mandatory, and it's to be reviewed periodically by the Information Security Officer. All member organizations shall ensure continuous monitoring. In case of ignoring or infringing the information security directives, member organization's environment can be harmed (e.g., loss of trust and reputation, operational disruptions or legal

violations), and also the fallible persons will be made responsible resulting in disciplinary or corrective actions (e.g., dismissal) and will face legal investigations.
A correct and fair treatment of employees who are under suspicion of violating security directives (e.g., disciplinary action) has to be ensured. For the treatment of policy violations, Management and Human Resources Department have to be informed and affect the handling of policy violations.

6. Administrative notations

https://www.sama.gov.sa/enUS/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

7. Policy definitions

Security incident:
A security incident is defined as any actual or suspected event which will adversely impact the confidentiality, integrity, or availability of data or systems used by the member organization' process, store, or transmit that data. Examples of events that would constitute a security incident include:

Unauthorized access to data by an outsider or insider not authorized to access that data
An endpoint (desktop, laptop, server, or mobile device) infected by malware. "Malware" may be a broad category encompassing Trojans, worms, viruses, ransomware, and other malicious programs
.Reconnaissance activities such as scanning the network for security vulnerabilities when scans are performed by outsiders or insiders not authorized to perform such scans
Denial of Service attacks (performed by outside or inside entities)
Web site defacements
Violations of member organization's IT security policies
Unpatched vulnerabilities on systems connected to the member organization's network
Discovery of an unregistered or non-centralized server in violation of the Server Hosting Policy.

Task 2: Creating Incident Awareness

Task 2.1: Write a brief explanation of why each of the listed events is considered high priority. Include at least one example per event.

Some events drain resources and can be expensive as they cause internal threats, external threats, human-initiated threats, technological threats, malicious threats, intentional or accidental threats to negatively affect the company, clients, business partners, or/and the public at large. All employees, contractors, consultants, vendors, and business partners are required to report known or suspected information security incidents.

Event#	Reasons	Example

a	Customer data at risk of exposure or compromise When an application, organization, or other individuals accidentally exposes personal data, this is known as sensitive data exposure. A data breach, in which an attacker gains access to and steals information, is not the same as sensitive data disclosure. When a database where information is stored is not properly protected, sensitive data is exposed. This may be due to a variety of factors, including weak encryption, no encryption, software bugs, or when someone mistakenly uploads data to the wrong database. In a sensitive data exposure, various forms of data may be exposed. Some of the types of information that can be left exposed include banking account numbers, credit card numbers, healthcare data, session tokens, Social Security numbers, home addresses, phone numbers, dates of birth, and user account information such as usernames and passwords. When data is left exposed in a database or server for everyone to see, it is known as data exposure. When systems and program configuration details are left unsecured online, sensitive data may be exposed. Unauthorized access to information is a security incident called a data breach. Hackers seek out personally identifiable information (PII) and other data to steal money, compromise identities, or sell on the dark web. Data may be targeted for theft, modification, or destruction. In today's world of technology, businesses store their customers' personal information electronically and on computers. Your consumer data can be at risk, despite the convenience of the software and devices we use. Customer data is information that a company uses to run its business. Data security and privacy are two key components of establishing trust between an organization and its customers (loss of customer trust). The consequences (impact): <u>Personal Information Hacking:</u> -It has a negative impact on confidentiality and integrity. We are constantly threatened by data breaches, resulting in a massive amount of personal user data being leaked and sold on the black	**Example 1**: Equifax, one of the largest credit bureaus in the United States of America, was breached on Sept. 7, 2017, due to an application vulnerability in one of their websites, leaving millions of personal records exposed to attackers and breaching of personal information (including Social Security numbers, birth dates, addresses, and in some cases drivers' license numbers). Equifax was also slow to report the breach. In February 2020, the US government indicted veterans of China's People's Liberation Army for hacking into Equifax and stolen sensitive data as part of a massive heist that also involved stealing trade secrets. **Example 2:** Adobe announced in early October 2013 that hackers had stolen around 3 million encrypted customer credit card information, as well as login data for an undetermined number of user accounts, as security blogger Brian Krebs reported. In August 2015, Adobe agreed to pay $1.1 million in legal costs and an undisclosed sum to customers to resolve allegations of Customer Records Act violations and unfair business practices. **Example 3:** SWVL Ride-Sharing Group Transport Company announced that its platform was hacked, targeting customers' information. The company's CEO reported that SWVL customers are our partners, and we have published the incident promptly on our website in order to keep our customers updated. The hacked data, as stressed by the CEO, are restricted to names,

	market, as well as when accessing client accounts, the attacker can use them to finance terrorism. -Hackers seek out personally identifiable information (PII) and other data to steal money, or compromise identities. -Data may be targeted for theft, modification, or destruction. - Leakage of personal information or photos may be very embarrassing for some people and could result in breakups and job loss in the long term. The potential consequences include psychological distress for the related parties and reputational damage. Companies' data Hacking: In the case of the company's data, the consequences could be serious. The most likely consequence is facing judicial claims leading to the company's indebtedness. If the company's sensitive data and information are hacked while no action was taken in such effect, it would impact the customers' loyalty. Hacking may have an indirect influence on sales in the long run, which results in more financial problems. - Reputational damage, the cost of responding to the breach, and the possible loss of future revenue. -With the rise in crime and a lack of security for public safety, quality customers will seek out another destination due to their mistrust. -Data hacking, sometimes, may help increase competition and create useful competitive effects for the competing companies against victim companies Indications of its occurrence: It can be noted when suspicious or unauthorized activity through the website or leakage of Customers' information or being used for other purposes. It's critical to comprehend why these things are permitted to occur, as well as realize how much is at stake when it comes to personal data and other confidential information.	phone numbers, and emails. The payment details and banking card data are completely secured using powerful and inaccessible protection systems. **Example 4:** British Airways announced that the company's security system is hacked, as some pirates attacked the company's website. Such an attack resulted in the theft of personal and financial data of the company's customers, including names, addresses, emails, and credit cards. The hack affected approximately 380k tickets purchase. Despite British Airways reiterated payment of damages to all hacking victims, the shares of IAG, the parent company, dropped by 3% at the closing morning trading following the hack at the London Stock Exchange. **Example 5:** Microsoft announced a security breach for customers' information in 2019. It was informed of such a problem by the Cybersecurity Researcher and Expert, Pop Dyachenko, working for Security Discovery.

b	b. Unauthorized use of a system for any purpose It occurs when an unauthorized individual or individuals use a computer or its data for unapproved or illegal purposes. Also, it occurs when someone uses another person's account or other methods to gain access to a website, software, server, service, or other systems. It can also happen if a user tries to access an area of a system they should not be accessing. A person is guilty when he knowingly uses, allows to be used, or accesses a computer, computer service, or computer network without authorization. Unauthorized Use of a computer can take several forms, such as downloading or copying personal identification information of other people stored on a department store network. Despite the fact that the computer is password locked, you manage to get access to the system and personal identifying details. Installed a program on your computer that registered all of your keystrokes, including email address names and passwords. After that, access your email account from an IP address. The consequences (impact): It affects confidentiality and integrity through: -Access to limited, confidential information and access to sensitive data for the sake of curiosity. - Changes, deletes, tampers with, damages, destroys, or adds to data stored on a computer. -It can result in criminal charges and/or disciplinary proceedings. -Access to the company's, employees', clients' property rights, slow down operations, impersonation , or espionage. -Theft of bank accounts and extort a victim. - Fraud to steal money or products. -Compromise systems and use them for unauthorized or illegal activity. - Deface websites or sabotage organizational systems. - Inflict physical damages – by gaining access to connected devices. Long-term effects of a successful data breach: -Harm to reputation and confidence. -Damage to business continuity. - Lower financial value or share price.	**Example 1:** Getting access to a bank computer and making an illegal bank transfer, etc. **Example 2:** Sage is a software company headquartered in the United Kingdom that specializes in accounting and human resource management. In the year 2016 was unauthorized used by a woman who works for the company to steal confidential customer information, including salary and bank account details. **Example 3:** someone guessing a username or password for an account that is not theirs before they gain access.

	- Costs of damage management, breach investigation, Government fines , Payment of damages to those affected, and communication costs. - Send damaging electronic messages to a computer device and injects a virus into a computer system. -Theft of password-protected data and the leakage of sensitive or personal information. -Wrongfully controlling or obtaining money, property, or data. - In certain cases, its effect may reach **availability**. A system outage may make it difficult for a business to maintain its productivity, causes the interruption or deterioration of computer services, or causes the denial of computer services to an authorized user of a computer or computer network. For example, it can disable governmental computer services and public safety infrastructure computer services. Indications of its occurrence: Organizations can keep track of their processes by keeping an eye on auditing activities. Detecting unauthorized use by these tools: 1-Scanning tools.2- IDS systems. 3- Software for monitoring audit records. 4- Software for network monitoring.	
c	c. DoS attack A denial-of-service attack (DoS attack) is a type of malignant attack performed by the attacker or group of attackers for disabling the targeted PC, PCs, or network services temporally or permanently. Usually, in such sort of attacks, the attacker's flood devices by the constant flow of requests beyond response capabilities or by sending customized requests to exhaust the targeted device's resources. Therefore, such devices are no longer capable of responding to good requests. Denial of service is typically accomplished by target URL with more requests than the server can handle in an attempt to overload systems and prevent any or all valid requests from being fulfilled. A DoS assault is similar to a crowd of people crowding a shop's entry door, making it difficult for legitimate customers to enter and thus disrupting trade. The consequences (impact) :	**Example 1:** January 2016: HSBC customers lost access to their online banking accounts two days before the UK tax payment deadlines due to the latest target of a sophisticated Dos attack. **Example 2:** SITES OF THE CLINTON AND TRUMP CAMPAIGN Anonymous, a multinational hacker group, conducted a denial-of-service attack on Donald Trump on April 1. The party, known as #OpTrump, attempted to take down the billionaire's hotel chain and presidential campaign websites, as well as his email servers. Anonymous hoped that by launching the attack, they would be able to

	-It is one of the most common threats that affect **availability**. This means that daily traffic on the website will be delayed or entirely disrupted during the attack time. -Despite the fact that DoS attacks seldom result in the theft or loss of sensitive information or other assets, they can cost the victim a lot of time and money to deal with because revenue will most likely be lost as a result of the attack. -There is the cost of remediation, and it is possible that impacted consumers will be paid. - If service providers fail to meet their SLAs, they can face financial and legal consequences. -Then there are intangibles like harm to a company's name or reputation, which can manifest in the form of lost business and declining stock prices down the road. -In addition, these attacks are damaging the satisfaction of their clients. Customers often turn to a different company because they are concerned about potential security problems or simply cannot afford to have an unavailable service. -DoS attacks primarily impact organizations and how they operate in a connected world. Consumers' ability to access resources and information is hampered as a result of the attacks. -DoS attacks are used by cybercriminals to extort money from businesses that rely on their websites being accessible. However, there have been instances where legal companies have paid underground elements to help them cripple rival websites. In addition, cybercriminals often use a combination of DoS attacks and phishing to target online bank customers. They use a denial-of-service attack to take down the bank's website and send out phishing emails instructing customers to go to a fake emergency site instead. How can processor DoS be discovered? • The increasing processor performance and exhaustion of power is the principle of DoS attacks. • Extraordinarily slow network performance. • Failure to access the requested website	derail Trump's presidential campaign and damage his image. **Example 3:** **Mafiaboy** On February 7, 2000, one of the first denial-of-service attacks made the news. A 16-year-old hacker known as Mafiaboy conducted one of the largest (if, not the largest) denial-of-service attacks of the time. Mafiaboy's attack caused the most important websites, including CNN.com, Amazon.com, eBay, and Yahoo, to be temporarily unavailable. The attack lasted about a week, and for the majority of that time, the targeted sites were unable to cope. Mafiaboy allegedly hacked into 50 networks and installed malware known as Sinkhole. The sinkhole was ordered to flood the targets with attack traffic. Following the attack, the Royal Canadian Mounted Police and the FBI in the United States conducted investigations. It didn't take long for the Canadian teen to be discovered boasting about his Exploits online, and he was arrested in April 2000. Michael Calce (aka Mafiaboy) was sentenced to 8 months "open custody" in a Canadian juvenile court in September 2001, which included time in a detention facility, restricted internet access, and one-year probation.

d	d. Unauthorized downloads of software, music, or videos A license is supplied with all legal software. This applies if the program is purchased for use on a single or several networked computers or preinstalled as part of a system. The unauthorized use of the program is described as violating the terms of the license. Unauthorized app downloads can be a major issue for some businesses. Attackers are actively searching for vulnerable targets to hack by tricking users into installing malicious files. This program raises the possibility of unauthorized access to confidential information. Without proper patching, upgrades, configurations, and security protocols, any program that is not authorized is likely to be handled. Without the knowledge of agency software, IT managers can't completely secure their data and information. Occur when: • Copying a legally obtained software program and installing it on more machines than the software license allows. • Gaining unauthorized access to secure software, also known as “cracking.” • Distributing counterfeit applications. • Preinstalling software programs on machines without having the software license that goes with it. The consequences (impact): -Legal & Monetary Everyone involved in the production and marketing of a film or song benefits financially from its sale. As a result, copyright law protects the product, preventing it from being copied, reused, or resold without their consent. If you did not pay for a song, movie, or other media file that has a copyright, then downloading that file is a crime. Materials that are potentially counterfeit or unlicensed can expose an organization to legal action. It may be expensive to remove and repair any damage that has occurred and reduce productivity with no vendor support. -Viruses & Spyware Illegal downloading exposes the device to a high risk of receiving viruses. Most illegal downloading is done through Peer-to-Peer (P2P) software, which helps users share their files with others. Since you	**Example 1:** Someone downloads unauthorized free software or videos using an insecure website, leading to the setup of malware. The malware will spy on his confidential information. **Example 2:** In Asia, many unlicensed copies of software programs such as Microsoft Word are distributed. **Example 3:** A copy of "CCleaner" software of Britain-based Piriform Company was downloaded in August 2017. Such copy included remote control tools that attempted reaching unregistered web pages that likely download additional unauthorized software. The accounts of software users were hacked.

	have no idea where you are getting the files from, you have no way of knowing whether the files are tainted with malware or spyware. When you download infected files to your computer, you risk losing data, getting a lot of pop-ups, having a poor Internet connection, and possibly losing your identity. Anti-virus software that is up to date will not always protect you from viruses obtained via peer-to-peer (P2P) software. - It's worth noting that some malwares are capable of remotely turning on an infected computer's microphone and video camera, giving cybercriminal eyes and ears into a victim's home or company. Furthermore, the threats associated with malware are severe; not only are there risks of data loss and identity theft but there are also serious copyright infringement risks. For preserving the environment's safety because unauthorized software may contain vulnerabilities, by exploitable by malware, and Systems running unauthorized software may introduce viruses, malware, Trojans and other malicious adware, spyware, and tracking cookies leading to the theft of information or loss of system availability. Not only does online access give cybercriminals and hackers the ability to target anybody, anywhere, at any moment, but it also allows them to hide their identities and illegal activities, allowing them to carry out further malicious attacks without fear of being investigated and prosecuted. It is the online downloads which are to expose consumers and small businesses to a high degree of cyber-attacks and resulting in debilitating personal and financial losses.	
e	e. Missing equipment According to IDC 201 study, 84 percent of IT businesses have registered equipment theft, with a recovery rate of just 3 percent. Laptops, hard disks, chargers, and keyboards are some examples of the equipment that people steal from offices. The consequences (impact): The effect will be on **availability**.	**Example 1:**APRIL 2008: MCDONALD'S LAPTOP. While eating at a McDonald's near the Ministry of Defense's Whitehall headquarters, an Army captain's laptop was stolen from under his chair. The data on the laptop, according to the MoD, was not sensitive and was completely encrypted. This is the most recent case of a Ministry of

	decrease productivity, increase spending to replace losses -Sale of lost hardware in the black market. -Theft of hardware, such as Hard Disk and USB, results in loss of **confidentiality**. -leads to a Ransomware attack. One of the Indicators of its occurrence: suspicious behavior by an employee such as: •a personal lifestyle that does not fit salary. • Unusual working hours. • Bad work performance. • Unjustified complaints about jobs. • Defensiveness while reporting on work. • An unexpected close relationship with, or unjustified favoritism by, a supplier or customer.	Defense laptop theft to be made public, and it occurred after the government tightened its regulations on workers bringing laptops home from work. Whitehall employees are no longer allowed to take unencrypted computers or drives containing personal information outside of the workplace. **Example 2:** JANUARY 2008: MILITARY RECRUITS A Royal Navy officer's laptop computer was stolen from his car in Edgbaston, Birmingham. It included the personal information of 600,000 people who had shown an interest in joining the Royal Navy, Royal Marines, or Royal Air Force had applied to do so. It included information such as passport numbers, Social Security numbers, and bank account numbers. **Example 3:** In healthcare environments, missing medical equipment reduces productivity, increases spending to repair losses, and can jeopardize patient safety. Every year, the healthcare industry loses millions of dollars due to lost or stolen equipment. More than $50,000 in stolen medical equipment was discovered on eBay last year after it vanished from United Memorial Medical Center in Batavia, New York. **Example 4:** UPS theft results in loss of availability. **Example 5:** If the server or keyboard is lost, it could result in the failure of the company's services and system.
f	f. Suspicious person in the Bank It occurs when a suspicious person at a bank commits a suspicious behavior through such as	**Example 1:** Milpitas (California) – On Jan. 2, 2015, a bank employee found a woman watching ATM customers.

	-Shoulder surfing: Attacks may be carried out from a short distance (by looking directly over the victim's shoulder) or from a longer distance. Attackers do not need any technical expertise to use this technique; all they need is a careful observation of the victims' surroundings and a familiarity with the typing pattern. This leads to the theft of sensitive information such as credit card passwords. -Stealing a bank's clientele using the "Tracking and Sneaking" method leading to financial losses. -With an increase in theft and a lack of security for public safety, quality customers will look for another place to visit (loss of clientele). -Theft of unattended properties from offices (material losses) or exposure to sensitive information on his property, such as his phone or flash memory. Indications of its occurrence: Indications include suspicious conduct, such as dubious movements or looks.	Police investigated and discovered that money had been fraudulently taken from several customers' accounts. **Example 2:**2021: Security forces in Alexandria managed to arrest a gang addicted to thefts by tracking banks' clientele. The gang's criminal activity was centered on stealing banks' clientele using the "Tracking and Sneaking" method after withdrawing cash. The city precincts were the gang's playhouse for undertaking their punishable activity. **Example 3:** He is mentioned in the movie hacker who robbed banks in 2017 because of his hate for the bank that expelled his mother. He entered the bank and pretended to be a new customer and wanted to ask about a commercial loan, and while he was talking with the employee, the pen tray fell on the ground, and during an assembly, he entered the flash memory, which was full of viruses, into the USB port in the computer case, which led to the complete disruption of the system.

Task 3: Analyzing an Occupant Emergency Response Plan and Assessing the Training and Testing of an Occupant Emergency Response Plan.

Task 3.1: Attach the plan you used or reference it if you found it online.

https://www.dm.usda.gov/beprepared/docs/USDA_Headquarters_Occupant_Emergency_Plan_6282019v2.pdf

Task 3.2: When was the plan last updated?

The effective date of this OEP is June 2019. This document supersedes all previously recognized OEPs for the USDA HQ complex. This OEP will be reviewed and updated on an annual basis.

Task 3.3: Summarize the key components of the plan.

we have in Occupant Emergency Plan of USDA Headquarters Facility the key component is

(Response plans)

Legally the Federal Government has a corporate responsibility to ensure a functional Occupant Emergency Program across its facilities. The motive of the Occupant Emergency Program is to develop an Occupant Emergency Plan (OEP) and an Occupant Emergency Organization (OEO). The OEP and OEO avail a functional, systematic, and rapid response in the event an emergency or disaster arises from a broad scope of hazards at stake. The Occupant Emergency Organization (OEO) function coordinates emergency response conveyance to safeguards casualties or victims in case of a disaster while sustaining normal operations in place. The OEO has a systematic incident command system controlled by an incident commander who has the inclusive duty to develop the OEP and coordinate all emergency responses in case of emergency. In collaboration with the public information officer, safety officer, liaison officer, and the Employees Needing Assistance (ENA) officer, the incident commander ensures the systematic coordination of activities and responses to carry out an Occupant Emergency Plan (OEP).

During emergency incidents, the incident commander relies on supervisors who control the general staff to execute essential response obligations. Under the available staff, operations, planning, logistics, and finance coordinate executions are systematically initiated. The operations section chief (OSC) executes personnel-related tasks with the help of the emergency command unit. The emergency command unit works jointly with warden units, emergency response team (ERT) units, and the staging unit to ensure the generally coordinated functionalities are viable, on time and realistic based on the nature of emergence. Also, the security unit is integral in providing supervised security restrictions and aid when applicable. In collaboration with the security liaison officer (SLO), technical security unit (TSU), and the operational security officer (OSO), an emergency is collectively evaluated, and a crisis is enacted with an efficient operation.

The planning section is obligated in joint evaluation, collection, and emergency dissemination reports to report the actual status of an emergency. A documentation unit is schemed to ensure complete documentation of relevant information from a crisis is captured for future reference. The resource unit ensures swift distribution of basic needs such as food and personal supplies are in reliable circulation throughout the emergency response exercise. A situation unit is also necessary to ensure feasible situational awareness concerning an emergency is given to the general public on a timely schedule. Also, a logistics section is required for the occupant emergency plan. It is liable to facilitate effective incident management for functionalities such as security, food, communication, and medical service needs needed during an emergency response. A service branch and support branch coordinate to implement command and control of emergency needs. The logistics section ensures a supply unit (SU) responds to the emergency scene to evaluate the status of the OSC. A facilities unit incepts oversight on security control in coordination with technical security units to enhance an efficient emergency operation plan.

A finance section ensures that vending, contracts, claims, and compensation functionalities are well documented based on the overall cost analysis of an emergency incident. The finance section integrates viable coordination across the human resource, time unit, compensation unit, and procurement unit to capture an emergency incident's operational records and financial documentation. Additionally, tenant agency functionality is integral in the occupant emergency plan, where all personnel are liable to enact emergency measures in line with the operation headquarters stipulations. The mission area reporting coordinator (MARC),

agency area coordinator (AAC), and the employees needing assistance (ENA) monitor execute operations, planning, logistic and financial functionalities in line with the occupant emergency plan. Additionally, during emergencies based on the nature of an incidence, an evacuation or shelter-in-place can be utilized provided that emergency procedures are embraced. have complete emergency contact information number of USDA Security Office, USDA Security Control Center, Manager: Duane Williams, Emergencies, Customer Service Center Hotline, Federal Protective Service, Hazardous Materials Information (Gas-Electric-Bomb Threat).
Specific emergency procedures differ by incident type, affecting the USDA Headquarters buildings (South/Whitten).
In an emergency incidence, occupants have two basic defensive actions that can be utilized, including evacuation or shelter-in-place. Generally, before taking defensive actions during an emergency, the occupants should ensure they secure their valuables, place, and lock exposed records in desk drawers, and any other important materials if necessary. The evacuation procedures require a quick response notification, which can be achieved by vibrating bells or activating fire strobes on all floors. In case the emergency is a non-fire incident, the use of public-address speakers will be viable. Once the building alarm has been sounded during duty hours, no employee will enter the facility. During non-duty hours, employees will be required to seek help from the security control center (SCC) and indicate their location within the incident facility. Additionally, all occupants will be required to swiftly assemble at emergency assembly areas to enhance swift accountability and response during an emergency. As a result, occupants must adhere to OEO instructions to ease the emergency response operation.

In shelter-in-place (SIP), notifications are given through a public address system notifying the occupants about the emergency response and safety mitigation. A SIP can be utilized when there is a biological explosion, or criminal disturbance occurs. However, the SIP in occupant response is not mandatory because one should think before opting to SIP based on the emergency intensity in line with OEO stipulations. Additionally, in an emergency, other viable emergency procedures can be incepted based on the incident variables. The need for attaining employee accountability is integral; all the operation and command units must coordinate to ensure that every employee is accounted for during the response plan. In incidences of an elevator entrapment, occupants are urged to stay calm and use the proposed channel through the operations center operator to mitigate the risk. Additionally, basic medical emergency aid is essential. Medical emergency response will vary based on the incident, such as in a fire outbreak, an exit is blocked by smoke, bomb threat, active shooting, gas leak, earthquake, or natural disaster. Therefore, throughout the emergency response plan, emergency communication channels define the intent to which an emergency response will be based on reliability, efficiency, and resilience.
The United States Department of Agriculture uses the agriculture-Automated Warning and Information Response System (Ag-AWaIRS) for communicating with personnel during an emergency. This system serves as a primary means of notification during an Evacuation.
include (Public Address System, Alert Desktop Messaging (Pop-up), E-mail Messaging, Short Messaging Service (Text Messaging), Phone Calls, Mobile Notifier Application, Hearing Impaired Paging System (HIPS).

In your opinion, does the plan provide adequate instructions?

Occupant Emergency Plan USDA Headquarters Facility provides detailed instruction on components of Response plans that include authority, plan activation; the EOP should be activated at a level proportional to the information available on the incident. Starting there and setting up an Incident Management Post may incur high costs. So, identify roles and responsibilities to activate and deactivate the plan then not done predetermined thresholds and specific circumstances for activation that will help avoid confusion, delay, and possible human error., notification, communication, evacuation, relocation, coordination with public authorities, and security. And Describes evacuation and shelter-in-place procedures in the event of emergency or disaster caused by a wide range of threats and hazards, including natural or human-made disasters, terrorist events, technological risks, and medical emergencies.

But don't have all components of contingency plans, Recovery plans, and Resumption plans.

Task 3.4: What type of exercises would you recommend to test the occupant emergency response plan?

Although an organization could perform tests, training, and practices

should consider having a program in place that addresses all three

should routinely determine the need for a tabletop exercise for an OEP by considering Program is to develop, implement, and institutionalize a comprehensive all-hazard program to improve the ability to manage and execute the OEP effectively. The TT&E program provides documentation that may include test results, feedback forms, participant questionnaires, and any other documents resulting from the event.

The USDA Headquarters Building overall objectives for conducting a tabletop exercise

As part of the TT&E program, need for a tabletop exercise

because ensures all OEO personnel are familiar with notification and evacuation procedures.

Ensures all OEO personnel are sufficiently trained to carry out Department operations and functions in an emergency environment

ensures that tabletop exercises are scheduled within a reasonable timeframe after a training event so that the personnel participating in the tabletop Annually or As Needed.

Also, Functional exercises allow personnel with operational responsibilities to validate tests and validates communications equipment to ensure both internal and external operability and Ensures occupants understand procedures associated with the "All Clear" command and re-entry into the facility and exercise the deliberate and pre-planned movement of occupants to SIP locations and exercise the purposeful and pre-planned evacuation of occupants to rally points, including a scenario, a tracking form, and an after-action report.

However, senior-level teams and operational-level teams should initially participate in separate tabletop exercises because of their different levels of responsibility. The exercise should apply to the roles and responsibilities of personnel within the EOP.knowledge of the roles and responsibilities identified in the plan being exercised is current.

The Occupant Emergency Program and plan are reviewed and updated Annually or As Needed.

Corrective maintenance also may be necessary following an exercise or incident, a change in occupant status, or other facility or occupant-related activities reveal or create deficiencies in the program.

Task 3.5: What type of training would you recommend in order to educate personnel regarding the occupant emergency response plan?

Training enables staff to maintain and enhance their skills proficiencies and to remain current with advances.

The scheduling of training events that support OEP should be coordinated closely with other events in a TT&E program. Itis roles and responsibilities training sessions typically precede tests for ensures roles and responsibilities before exercising the plan itself.

is typically split between a presentation into their roles and responsibilities and activities that allow personnel to demonstrate their understanding of the subject matter, including types of potential emergencies, reporting procedures, alarm systems, evacuation plans, and shutdown procedures.

Task 4: Regulatory Compliance for Institutions

Task 4.1: List US Acts that Medical Insurance Companies should comply with, and explain why?

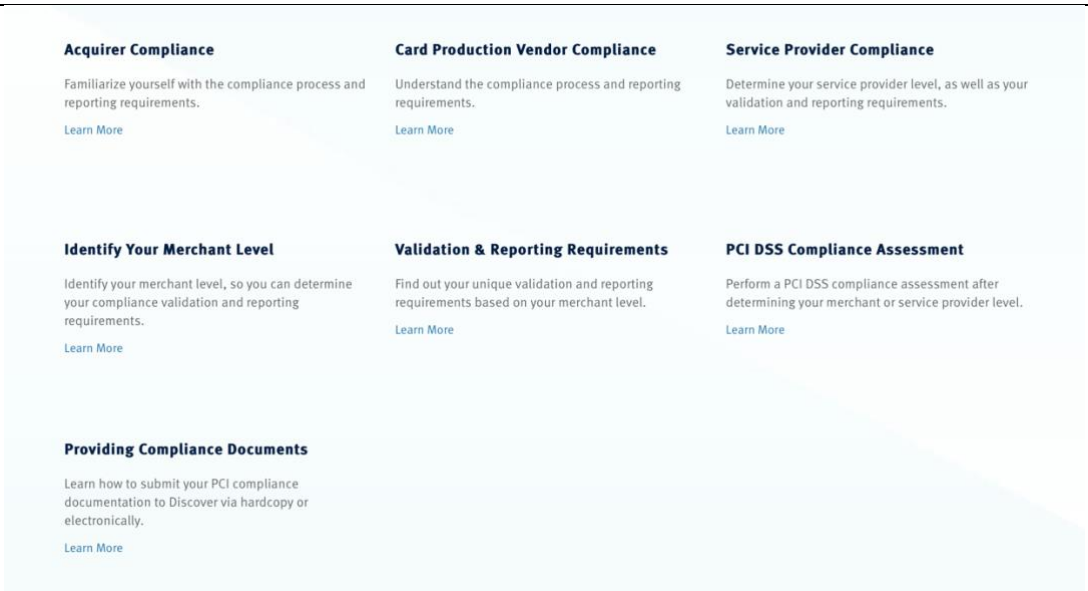
US Acts	Reason
Act 1: **Health Insurance Portability and Accountability Act (HIPPA)**	The main objective of this law is to protect a person's privacy and ensure that patient privacy is maintained. Complying with HIPAA can improve the efficiency in the healthcare industry and ensure that the health information is shared in a secure manner. Medical Insurance Companies should comply with HIPAA for the following reasons, become a HIPAA compliant is not optional for medical practices or their business associates today (Anyone who handles health records must adhere to HIPAA). The penalties for non-compliance with this act increased from $25K to $1.5M per violation annually. The patients can freely discuss their health concerns with the doctors and be transparent if they know

	that their health information is protected. Promotes Personal, Societal Values and supporting the values and human rights such as respect and dignity.
Act 2: Health Information Technology for Economics and Clinical Health (HITECH) Act	HITECH addresses the privacy and security concerns associated with the electronic transmission of health information. HITECH gives patients the right to access their protected health information (PHI) electronically. And notify the patients in case of any data breaches related to patients' PHI. And any data breach for 500 or more patients' information must be reported to the U.S Department of Health and Human Services (HHS). Complying with HITECH Act can protect patient information and avoid severe legal consequences. The HITECH Act enforces penalties as high as $250K for first incidents and $1.5M for repeat incidents. And additional loss may occur due to notify patients affected by a breach, through investigations, audits, and other legal issues. HITECH does not allow the individual to raise a lawsuit against a provider. Instead, a state attorney general is required to bring the action on their behalf.
Act 3: Gramm-Leach-Bliley Act (GLBA)	The main objective of this Act is to explain how the companies share and protect their customers' sensitive information, and how they protect this information from unauthorized access. The penalties for non-compliance with the GLBA are the following, First, the institution will be subject to a civil penalty for each violation of not more than $100K. Then, the officers and directors of the institution will be subject to, and personally liable for, a civil penalty of not more than $10K for each violation. Finally, and the institution and its officers and directors will also be subject to fines by Title 18 of the United States Code or imprisonment for not more than five years, or both.

Task 4.2.: All major credit card companies have dedicated online portals to explain the way that they keep card member information safe and secure. The following are the links to the security portals for several major credit card companies: Discover Card: https://www.discovernetwork.com/en-us/business-resources/fraud- security/pci-rules-regulations/ and JCB Card: www.global.jcb/en/products/security/pci-dss/. Describe how they document and address PCI DSS compliance.

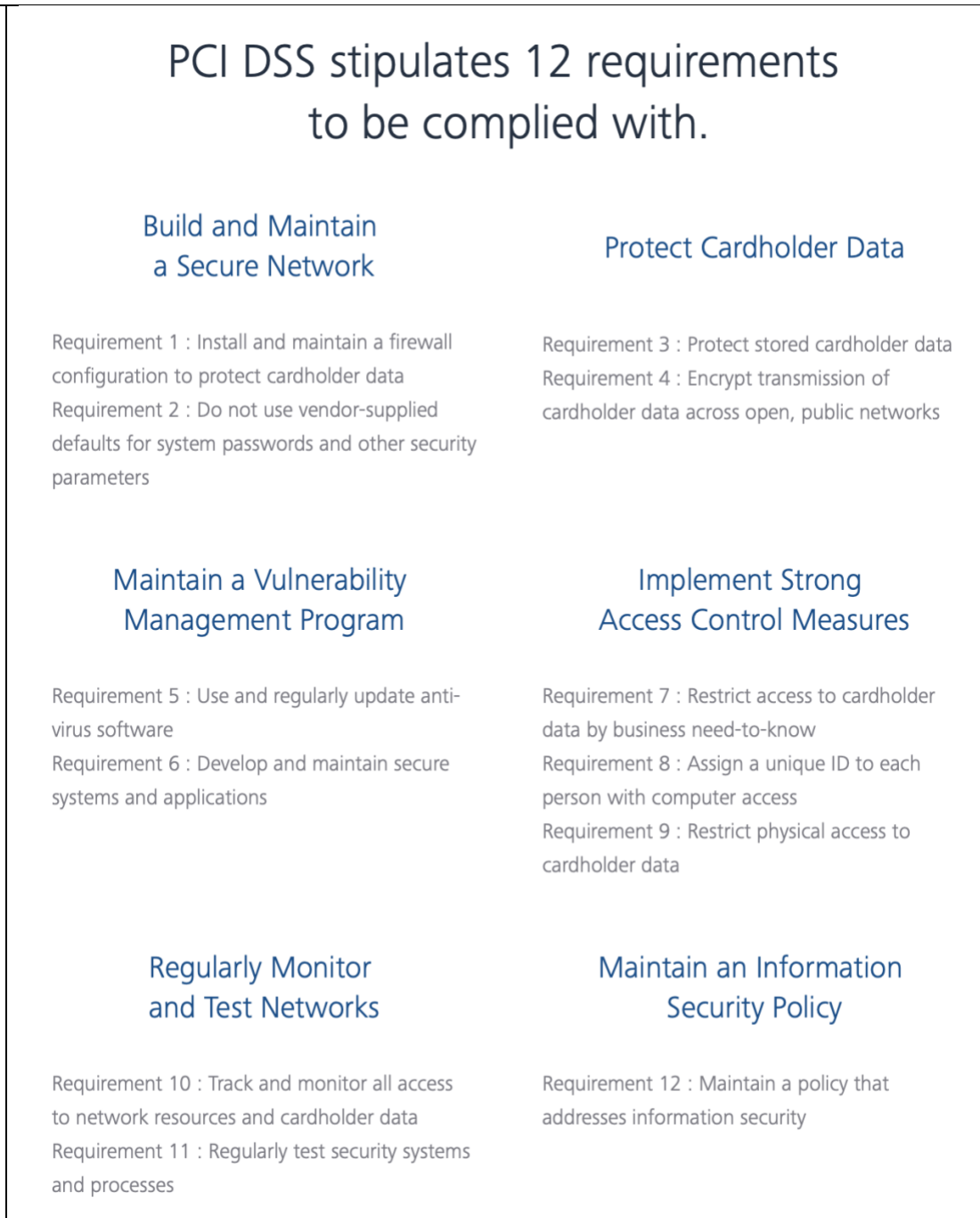
	How they document and address PCI DSS compliance.
Document#1	The main objective of the Discover company is to ensure the safety of customer data through PCI compliance. So they required all merchants, acquirers, resellers, and service providers that process, store or transmit cardholder data on the Discover® network to be PCI-compliant. Also, they enforce the merchants that accept Discover® Global Network to comply with the PCI DSS at all times and report the evidence of compliance to the company or your third-party acquirer. Moreover, they enforce the acquirers that process Discover transactions to report their annual compliance status, as a service provider, if you store, process, or transmit

	Discover Cardholder data on the Discover network, administer the DISC program and help secure the payment card transaction process. The Discover company has developed the Discover Information Security & Compliance (DISC) program to ensures the processing of cardholder data on the Discover® Global Network is secured and to help its partners implement and maintain the needed information security requirements. The Discover company has developed the Discover Information Security & Compliance (DISC) program to implement and maintain the required data security requirements and procedures for its partners. This program is aligned with the PCI security standards to help safeguard this data and limit data compromises. **DISC for Merchants, Acquirers & Service Providers** • Discover requires an additional requirement that each new implementation of payment applications by merchants and their agents is compliant with the Payment Card Industry Payment Application Data Security Standard (PA-DSS). And the PIN entry on POS terminals must comply with Payment Card Industry PIN Security Requirements. • Discover strongly recommends that acquirers ensure their merchants, service providers and agents use payment applications that have been validated as compliant with the PCI Payment Application Data Security Standard (PA-DSS). • Acquirers and their Agents who store, process, transfer, or otherwise handle PIN numbers as part of a credit or debit card authorization process must comply with Payment Card Industry PIN Security Requirements • Software-Based PIN Entry on COTS (SPoC) Solutions enable EMV contact and contactless transactions with PIN entry on the merchant's consumer device using a secure PIN entry application in combination with a Secure Card Reader for PIN (SCRP). Discover strongly recommends all SPoC solutions be PCI certified (PCI Software-Based PIN Entry on COTS) and listed on the PCI SSC website. • Contactless Payments on COTS (CPoC) Solutions enable merchants to accept contactless payments using a commercial off-the-shelf (COTS) mobile device (e.g., smartphone or tablet) with near-field communication (NFC). Discover strongly recommends all CPoC solutions be PCI certified (PCI Contactless Payments on COTS) and listed on the PCI SSC website. • Issuers can only use the Approved Vendor by DISC to provide goods and services related to the production of Cards. They helped merchants, acquirers, and service providers by providing them with some resources to maintain PCI compliance.

<table>
<tr>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>Document#2</td>
<td>They have published on their website the importance of being a PCI DSS compliant and introducing some benefits of the PCI DSS, which can show their commitment regarding been PCI compliant.

Also, they have present the PCI 12 requirements, to guide the others on how to be a PCI compliant,</td>
</tr>
</table>



They have developed the JCB Data Security Program, and it is a program for Licensees to ensure that they meet the PCI Data Security Standard (PCI DSS). JCB requires Licensees to ensure that the Licensees themselves, TPPs, IPSPs and Merchants with access to cardmember data and transaction data comply with the JCB Data Security Program.

	The JCB have present three ways can be used to validate the compliance of PCI DSS, 1. Self-Assessment Self-Assessment can be done by answer the Self-Assessment Questionnaire to determine your current level of compliance with the PCI DSS, 2. Security Scan A PCI SSC Approved Scanning Vendor (ASV) performs a remote network security scan of your network and web applications to evaluate system vulnerabilities and misconfigurations to attempted intrusions over the Internet. 3. On-site review A PCI SSC Qualified Security Assessor (QSA) performs an on-site review of your information security including interviews, document inspection, and audit of system controls. And JCB company develop a metric that can help to determine the due Date of PCI DSS Compliance and Compliance Validation Procedures,

Starting April 1, 2018

		Compliance with PCI DSS	Number of JCB transactions (per year)		Compliance Validation Procedures		
					Self-Assessment	Security Scan	On-Site Review
Merchants (including IPSPs)	E-commerce Transaction, MO/TO Transaction, Phone Call Service Transaction	Mandatory (On and after April 1, 2018)	Merchants excluding IPSPs	One million or more	-	Quarterly	Yearly
				Less than one million	Yearly	Quarterly	-
			IPSPs	Regardless of the number	-	Quarterly	Yearly
	Attended Transaction, Cardmember Operated Terminal Transaction	Mandatory (On and after April 1, 2020)	One million or more		-	Quarterly	Yearly
			Less than one million		Yearly	Quarterly	-
TPPs		Mandatory (On and after April 1, 2018)	One million or more		-	Quarterly	Yearly
			Less than one million		Yearly	Quarterly	-
Acquirers		Mandatory (On and after April 1, 2018)	Regardless of the number		-	-	-
Issuers		Mandatory (On and after April 1, 2018)	Regardless of the number		-	-	-

Task 4.3: Which regulation should we have to prevent what happened to Almaajel Group as it reported in the news/video (مجموعة المعجل)? Explain.

Which regulation should we have to prevent what happened: Sarbanes-Oxley (SOX) Act. This regulation can protect investors from fraudulent financial reporting by corporations. And this act has created strict new rules for accountants, auditors, and corporate officers and record-keeping requirements. This Act result that a new criminal penalty has been added for violating securities law. Any Corporate officers who knowingly certify false financial statements can go to prison.

References:

- Santos, O. (2019). *Developing cybersecurity programs and policies* (18th ed., pp. 368-410). Larry Sulky.