ISTM 635: Business Information Security

Instructions

1. Please read the case carefully.
2. We will use this case to do in-class assignments related to various risk assessment tasks.
3. When required I will provide the worksheets that you can use to complete certain risks assessment tasks.
4. Make careful notes about your assumptions, information sources, and any other information you find necessary while completing these risks assessment tasks.
5. At the end of the semester you have to submit a complete qualitative risk assessment report.

Qualitative Risk Assessment

1. Identify and classify critical assets
2. Identify vulnerabilities and relevant threats
3. Estimate threat likelihood and impact if threat is carried out successfully
4. Estimate cybersecurity risk for critical assets

Deliverables

1. Qualitative Risk Assessment Report
2. Write a Security Baseline for Windows 10 workstations used by AMC
3. Write a network access policy for AMC. Develop Access Control List (ACL) rules for Windows Defender Firewall that will enforce this policy.

Introduction

The Aggie Medical Center (AMC) is a hospital, located in College Station, TX. It has 2 remote clinics and 2 labs in the Bryan and College Station. It has:

- A permanent administrative organization
- Both permanent and temporary personnel- Physicians, Surgeons, Medical staff, Maintenance staff, Administrative staff
- A small information technology (IT) department (three people) responsible for on-site computer and network maintenance and upgrades, and handling simple user help requests

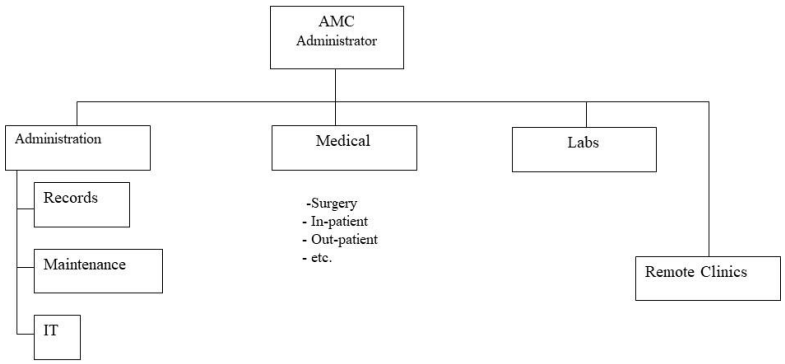

Figure 1: AMC Organization Chart (A high-level view)

In January 2020, AMC senior managers decided they wanted a comprehensive review of cybersecurity within their facility. Several new regulations would be coming out in the following year that would require documented cybersecurity risk assessments and proof of good cybersecurity practices. After some discussion and consultation with other medical facility managers, they decided to use your consulting firm. They assigned the initial planning and preparation to the assistant administrator, Nancy Perry, who will coordinate with your team, help you with data collection, and act as the liaison between your team and BMC.

Systems of Interest, Access Paths, and Key Components

Figure 2 shows a high-level map of the organization's IT infrastructure. A brief description of servers used by BMC is as follows-

- Patient Data Information Server (PDIS) - Database of most of the important patient information. Everyone who needs to has access (e.g., appointment scheduler, pharmacist, lab technicians, providers, etc.). Within PDIS, all information is cross-referenced. ABC Systems maintains PDIS for BMC.
- Financial Record Keeping Server (FRKS) - All of the insurance, billing records, payment schedules, and other related information are stored on this server.
- Personnel Management Server (PMS) – Salary, financial, demographics, work histories, assignments, skills, and disciplinary records of all employees are stored on this server.
- Medical Logistics Server (MLS) – This server has data on supplies, office property, and equipment. It also hosts the procurement application. It can be accessed from outside by pre-certified vendors.

All the servers can be accessed by authorized employees from their workstations within the BMC network. PDIS can also be accessed physicians from their home computers. Data can be entered and/or edited on the servers by authorized employees only. Workstations are located in all physicians' offices, treatment rooms (including emergency rooms), nursing stations, labs, and administrative offices. Support for the servers used by PDIS, FRKS, PMS, ECDS, and MLS is provided by an independent contractor, ABC Systems. In addition, ABC also does network management and maintenance for BMC. BMC also has a small, internal IT staff to provide on-site help desk support and basic system maintenance for the hospital, all clinics, and the labs. Internal IT personnel were provided with limited training from ABC Systems.

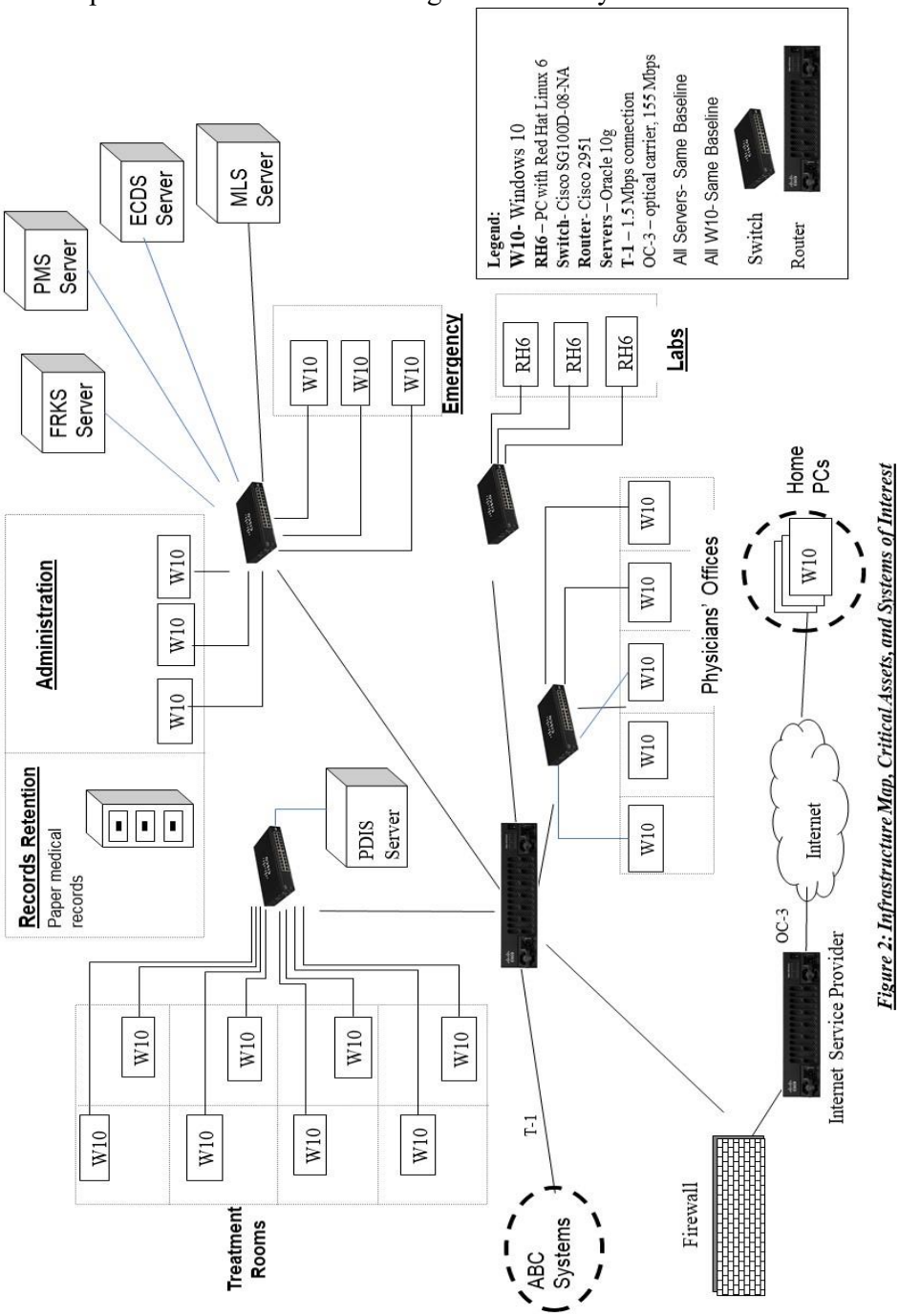

Figure 2: Infrastructure Map, Critical Assets, and Systems of Interest

The Aggie Medical Center (AMC)- Data Collection for Risk Assessment

The data collection part of the project has already been completed. Information was collected from the senior managers, general staff, and the IT staff. This information is provided in the following pages.

Data Collection: Senior Management

Table 1 describes some of the assets identified by senior managers. The assets they considered to be important are listed in the left column.

Table 1: Senior Management Assets

Important Assets	Other Assets
Patient Data Information System (PDIS) - Database of most of the important patient information. Everyone who needs to has access (e.g., appointment scheduler, pharmacist, lab technicians, providers, etc.). Within PDIS, all information is cross-referenced. ABC Systems runs PDIS for AMC. Paper medical records – Complete patient records are on paper. If lost, there's no way to re-create it. Patients can come in and pick up their records if going to another appointment within the facility. Financial Record Keeping System (FRKS) - All of the insurance, billing records, payment schedules, and other related information. Providers' credentials - Credentials of medical personnel.	Emergency Care Data System (ECDS) - Diagnosis, who saw patients, what was done, billing support, patient demographics, types of care, etc. Email - A common server with important information, historical data, etc. Personnel Management System (PMS) - Demographics, work histories, assignments, skills, disciplinary records. It has a lot of information that needs to be protected. Internet connectivity - Whatever it is we use to get to the Internet. Medical Logistics System (MLS) – Inventory of Supplies, real property, equipment, and medicines etc. Ordering is done through it.

Areas of Concern

Some of the discussion relative to PDIS is provided below, but it represents only a part of the conversation that occurred between your team and the senior management. *Table 2* shows the complete list of areas of concern for PDIS and the other important assets identified by senior managers.

Conversation about PDIS

- *"As far as our security strategy, PDIS and the other systems require unique user IDs and passwords, for which everyone receives training. Everyone knows patient information must be kept private. If patient information were revealed to someone who shouldn't have it, we could get sued."*
- *"I think our security training for all of our personnel is sufficient, although it could probably be improved."*
- *"The contract with ABC Systems requires the system to be up 24/7. It usually is, but apparently we have problems accessing it sometimes. I'm not sure why. I have heard complaints from the administrative group. They seem to have the most trouble."*
- *"PDIS is now central to our operations - we just can't function well without it. It provides access to all the information we need. If it's down or people can't get logged on, then data entry backs up and we run the risk of physicians not having the latest lab results or even changes in insurance coverage. We could get an incorrect patient diagnosis or treatment, with injury or illness as a result."*
- *"We're always looking for ways to improve the systems we use here. We've gotten quite efficient with TSPs at the management level for non-PDIS functions, and we'd like to extend that technology to the physicians and perhaps the nursing staff. We've asked ABC Systems to propose a plan for upgrading PDIS to allow TSP access. We asked them to include security concerns in their proposal."*
- *"Our IT staff does the day-to-day maintenance on PDIS. That's because ABC Systems' main office is 60 miles away and they're not large enough to keep people on site here. It was more cost-effective for us. ABC does provide adequate training for our IT people."*

Areas of Concern for Important Assets

Table 2 shows the areas of concern for those assets that the senior managers considered to be important.

Table 2: Senior Management Areas of Concern for Important Assets	
Asset	**Areas of Concern**
PDIS	Personnel access information that they are not authorized to use: access is used inappropriately or legitimately accessed information is distributed inappropriately.
	Staff could intentionally enter erroneous data into PDIS.
	It's difficult to get and retain qualified personnel to help maintain PDIS.
	PDIS is not compatible with newer systems, leading to system crashes.
	The risk of an outside intrusion into PDIS is much higher than newer systems because of the need to bypass the firewall.
	Power outages, floods, and other external events can lead to a denial of access to PDIS. This essentially shuts the hospital down.
	Accidental loss of any important information is a concern.
Paper Medical Records	Medical reports are signed out to patients. Anyone can potentially view, alter or lose records.
	Medical records are left where they shouldn't be (in offices and labs).
	Data in medical records (e.g., physician SSN, credentials, etc.) could be used to "forge" a prescription.
	Roof leaks, water, fire, etc., could destroy the physical medical records.
	Accidental mishandling by staff can lead to the destruction of physical medical records.
FRKS	Staff could inadvertently or intentionally disclose confidential patient financial information to family or friends.
	Staff could change or delete the information for any patient once they've logged into the system. We could get the wrong bills sent or never send any at all. We could file incorrect insurance claims.
	Power outages can lead to a denial of access to FRKS. We'd have to deal with a potentially large backlog of data entry and verification to do billing and insurance.
	There's no physical security for the room where staff log on to FRKS. Anyone could wander in and see confidential information displayed on the workstations.
Provider Credentials	Deliberate modification of the records could result in our using an unqualified provider.

Security Requirements for Important Assets

The security requirements for the important assets as defined by senior managers are provided in *Table 3*. The security requirement that is the most important for the asset is shown in **bold**.

Table 3: Security Requirements from Senior Management Perspective	
Asset	**Security Requirements (Relative Ranking)**
PDIS	AVAILABILITY System availability is required 24/7. CONFIDENTIALITY Information should be kept confidential. Federal compliance with Privacy Act of 1974 – Anyone accessing can be prosecuted for passing data to others. INTEGRITY Only authorized users should be able to modify information.
Paper Medical Records	AVAILABILITY Records must be available 24/7. **INTEGRITY** Only authorized users should be able to add information to the files. CONFIDENTIALITY Information should be kept confidential. Federal compliance with Privacy Act of 1974 – Anyone accessing can be prosecuted for passing data to others.
FRKS, PMS, ECDS, & MLS	INTEGRITY Only authorized users should be able to add, modify, or delete information. **AVAILABILITY** System availability is required during regular administrative office hours. CONFIDENTIALITY Patient financial information should be kept confidential.
Provider Credentials	**INTEGRITY** Only authorized users should be able to modify information. CONFIDENTIALITY Information should be kept confidential. **AVAILABILITY** It's needed on an as needed basis to verify new, transferred, or temporary providers or to provide information for insurance purposes.

Administrative Data Collection: Operational Area Management

Asset Information

Table 4 describes the assets identified by the operational area managers. The assets are divided into what were considered to be important assets and all other assets.

Table 4: Operational Area Management Assets

Important Assets	Other Assets
Paper Medical Records - all patient information, lab results, etc. These are paper for now, but some data is now also in PDIS. PDIS - has everything: pharmacy, appointment history, patient history, billing, admissions, and all the ancillary stuff. 400 modules in it, a massive system. ECDS (Emergency Care Data System) - tracks what patient encounter was and the diagnosis; runs reports, trends, and population demographics; contains raw information for trending accidents; used for insurance and billing.	Pharmacy System - supports automated drug dispensing Medical Logistics System Providers' Credentials 32 or 33 other automated systems – not as important

Areas of Concern

Some of the discussion relative to PDIS is provided below. *Table 5* shows the complete list of areas of concern for PDIS and the other important assets identified by operational area managers.

Conversation about PDIS

- *"Everyone gets the same basic security training, but it only covers passwords. We should probably know something about managing security breaches or attacks. I wouldn't know what to do if I saw something out of the ordinary. My staff certainly wouldn't. I suppose we'd call our IT folks, but what they would do, I don't know."*
- *"We've got a lot of workstations out in the open, and they're not always watched. It wasn't too bad two years ago when they were fairly big, but now we're talking about going to these streamlined, lightweight TSPs with wireless connections so physicians can carry them around with them. That's to get around the fact that we can't get them to remember to log out, and PDIS won't let them log on from multiple workstations. The physicians complain they have to try and back track their patient schedule and figure out where they were last logged in. So what happens when they leave the TSP in the treatment room?"*
- *"All new employees get set up with new accounts. I did ask our IT people to check that process because I noticed when I started three months ago that I had a lot of privileges that I didn't think I was supposed to have. Apparently I inherited everything my predecessor had, and she had moved around a lot in AMC and picked up quite a few privileges. I really fouled up some of the records."*
- *"ABC Systems did a really good job setting things up, but I don't think they really understand what we're dealing with. PDIS is usually up and running, but the network seems to have problems. It drops connections on a daily basis. ABC says the connection can be reestablished within the contracted amount of time by our IT folks, but still, it's a continual annoyance, and sometimes the most recent patient data don't get to the physician in time. I mean, with the tight patient appointment schedule, you can't ask someone to sit in the corner and wait five minutes for data on drug allergies to come up. The physician will go with the record they have and move to the next patient. If necessary, the patient will have to wait a few hours for things to get caught back up and for the prescription to be verified."*

Areas of Concern for Important Assets

Table 5 shows the operational area managers' areas of concern for the important assets.

Table 5: Operational Area Managers' Areas of Concern	
Asset	**Areas of Concern**
Paper Medical Records	Too many people are entering the wrong data, resulting in incorrect records, and/or multiple files and records may exist for an individual.
	"Loose" control over records – No process to stop the patient from taking or modifying them. No mechanism to copy and release just what's needed. Integrity of record is compromised.
	Could get poor quality of care or patient death if contradictory medications are prescribed or allergies are not accounted for.
PDIS	Too many people have access to too much information. Role-based access builds over time and replacements inherit all of those access privileges.
	Too many people are entering the wrong data, resulting in incorrect records, and/or multiple files and records may exist for an individual.
	Connectivity is an issue, including problems with availability of and access to PDIS. The uptime requirement in the contract is for the servers, not for our connectivity.
	Loss of Internet connectivity. Systems are susceptible to malicious code and virus activity (in part due to the location/configuration of the firewall).
	Firewall limits connectivity. Timeliness of firewall support can affect system performance.
	ABC Systems fails to recognize the importance of the Internet to the medical staff to access current best practice information.
	Could get poor quality of care or patient death if contradictory medications are prescribed or allergies are not accounted for.
	ABC Systems has many customers. They do not recognize the importance of the hospital. Priorities of the hospital are not understood. They do not respond in a timely manner.
ECDS	Loss of Internet connectivity. Systems are susceptible to malicious code and virus activity (in part due to the location/configuration of the firewall).
	ABC Systems does not recognize the importance of the hospital/health care organization. Priorities of the hospital are not understood.
	Could get poor quality of care or patient death if contradictory medications are prescribed or allergies are not accounted for.
	Too many people are entering the wrong data, resulting in incorrect records, and/or multiple files and records may exist for an individual.

Security Requirements for Important Assets

The security requirements for the important assets identified by operational area managers are provided in *Table 6*. The security requirement that is the most important is shown in **bold**.

Table 6: Security Requirements for Important Assets	
Asset	Security Requirements (Relative Ranking)
Paper Medical Records	AVAILABILITY Access to records is required 24/7. Records must be available for patient encounters. INTEGRITY Must be complete. All information should be available for patient encounters. Accuracy CONFIDENTIALITY Can be viewed only by those with "need to know." Patient information is subject to the Privacy Act.
PDIS	INTEGRITY Must be complete and all information should be available for patient encounters. Accuracy AVAILABILITY Access to records is required 24/7. Records must be available for patient encounters. **CONFIDENTIALITY** Can be viewed only by those with "need to know." Patient information is subject to the Privacy Act.
ECDS	INTEGRITY Must be accurate and complete. **AVAILABILITY** Access to records is required 24/7. All information should be available for patient encounters. CONFIDENTIALITY Can be viewed only by those with "need to know." Patient information is subject to the Privacy Act.

Administrative Data Collection: Staff

This section includes the knowledge elicitation workshops held with general staff and information technology (IT) staff. Information from IT staff is labeled as "IT Staff." Asset Information. *Tables 7* and *8* describe some of the assets identified by general and IT staff. The assets are divided into what each considered being important assets and all other assets.

Table 7: General Staff Assets

Important Assets	Other Assets
Paper Medical Records - "that's what we are and what we do." Paper is currently more important. Outpatient Records has the most control – that's where they're stored and where they come back to. Otherwise, control is by whoever has them at the moment. PDIS - same type of data as paper medical records, lab results, mobility, admissions history, etc. External Relations – group of people that control the release of information. They ensure there's no compromise to data being released to the public or insurance companies. They use PDIS a lot for the information being released. Email (PDIS and General) - LAN and PDIS. LAN is for patient data email, but it is not as secure as PDIS email.	Medical Logistics System (MLS) Internet access

Table 8: IT Staff Assets

Important Assets	Other Assets
ABC Systems – manages all major changes, maintenance, and upkeep. We can't create a new network user without them. Our help desk calls their help desk if something major goes wrong. Connectivity (to Internet) - commercial ISP. AMC Help Desk - five PC technicians (not part of core IT staff). Users call in problems and we troubleshoot them. Functional Servers for other systems – some are on site. The group that has the system does day-to-day management. They have their own system administration.	Mr. Smith - senior IT person PDIS Personal computers - For access to all systems, email, etc. People can always move to another PC. There are 30+ functional systems

Staff Areas of Concern

Some of the discussion relative to PDIS is provided below. *Tables 9* and *10* show the complete list of areas of concern for PDIS and the other important assets identified by general and IT staff members.

General Staff Conversation about PDIS

- *"Office space is very tight and we do share workstations. It takes forever to log on/log out. We found it was easier for one person to log on and just stay logged on all day."*
- *"I know we were told not to share passwords, but everyone knows and trusts each other so there's no problem. It's a little hard to keep patient information private because visitors can see the screens on the workstations. But that doesn't matter too much as the physicians and nurses all discuss their patients out in the open anyway. It's not as if we don't all know what's going on or who's here for what reason."*
- *"Actually, I've heard that certain staff members like to check out the medical records of people they're dating. And there was this one patient who got into the computer in the treatment room and looked up his wife's record. The doctor probably forgot to log out. They're always doing that. Logging out is even more complicated than logging in."*
- *"PDIS drops off at least four times a day. I don't know why. I just get dropped and get a message about the connection. I call IT and it's usually back up in 10 minutes, if IT answers. But then you have to do the whole log-in routine and meanwhile there's paperwork to be entered, patients calling, physicians asking questions about this or that, and we get behind."*
- *IT Staff Conversation about ABC Systems and PDIS*
- *"ABC Systems does run vulnerability assessment tools on PDIS. I know because we get all those long lists every other week. I don't know what they do with them, though. I mean, we're just trained to set up new user IDs and fix minor problems. The last three people that got a lot of training left for a job that paid four times as much. So management quit authorizing any training for those of us in IT. I used to be a medical administrator. Last month, they told me I was now in IT. Go figure."*
- *"I've never seen or heard of anyone sharing passwords. They were all told not to do that, although I'm not sure what we would do if we did catch them sharing passwords. I think I'm supposed to tell their boss."*
- *"PDIS actually got hacked last week. Well, at least I think it did. Something strange sure was going on. We called ABC Systems and they sent someone over a few days later. They said there was a problem with the firewall and they fixed it. We were supposed to have kept the logs for them, but no one ever told me that. We've started keeping those now, just in case. I've got a drawer full of disks."*

Areas of Concern for Important Assets

Table 9 shows the areas of concern for some of the staff's important assets. Note that the IT staff listed ABC Systems as an important asset, but did not identify any areas of concern. The analysis team sensed some resistance from the IT staff and did not pursue this during the workshop.

Table 9: Staff Areas of Concern

Asset	Staff Areas of Concern
PDIS	Doctors leave PDIS screens on after they have left treatment rooms. Patients and others could have access. Passwords, logouts, timeouts, and screen savers are inconsistently used.
	The configuration of facilities/layout allows inappropriate viewing of systems and medical records by patients and visitors.
	Inherent flaws and vulnerabilities in critical applications could be exploited.
	Doctors and staff discuss patient issues and information in public areas.
	There are networking/connectivity issues. Access to PDIS is often restricted due to system crashes.
	Instability of the local area network affects access to numerous systems and creates backlog.
	Access to the majority of systems is supported by ABC Systems. They are responsible for hardware and software maintenance. We're concerned about our lack of control.
	Hurricane evacuation procedures require movement of assets off of the first floor of all facilities due to flooding concerns.
External Relations	Unfamiliarity with all the regulations and legal issues sometimes results in confidential information being released to insurance companies and the press. Insurance representatives aren't above trying to trick information out of the staff.
	Someone from the insurance companies could use appointment records to see who keeps up with routine, preventative care as well as to look for confidential test results.
Paper Medical Records	Staff personnel could view medical records in unauthorized or inappropriate manner.
	Information is deliberately released to outside personnel.
	Misfiled paperwork could allow unauthorized personnel to view another's records.
	Accidental problems with data entry can affect the integrity of information.
	Loss of paper record can mean permanent loss of critical information.
Email	Medical personnel use email to discuss treatment plans for patients.
	Personnel might think that PDIS email is more secure – information is released because they believe it can't be viewed by unauthorized personnel.
	Instability of the LAN affects access to email. Medical personnel now rely heavily on email to schedule appointments, exchange patient information, and transmit records from home machines.
Connectivity to Internet	Connection fails frequently. This affects the medical personnel trying to research new treatments.
	Connections have been getting slower over the past six months.
Help Desk	Lack of adequate training for help desk personnel. ABC Systems trains them from the ground up – medical administrators are turned into computer technicians.
	There is a very small IT budget. There aren't enough of us to staff the help desk 24/7, which is what they seem to want.
FRKS, PMS, ECDS, & MLS	Some of the smaller systems use servers that we don't have responsibility for. Usually an untrained or barely trained person in that department maintains it. We can help, but not a lot.
	We don't know what security covers those other servers, but the information is replicated or moves to the servers and systems we do manage. We could be getting corrupted data.

Staff Security Requirements for Important Assets

The security requirements for important assets defined by general staff are provided in *Table 10*. The security requirement that is the most important is shown in **bold**.

Table 10: General Staff Security Requirements for Important Assets	
Asset	**Security Requirements (Relative Ranking)**
Paper Medical Records	AVAILABILITY Access to information is required 24/7. **INTEGRITY** They should be modified only by those with appropriate authority. CONFIDENTIALITY Privacy Act "need to know"
PDIS	AVAILABILITY Access to information is required 24/7. CONFIDENTIALITY "need to know" Privacy Act - Privacy statement is the first thing you see when you log in. INTEGRITY Information can only be modified by those with appropriate security keys.
External Relations	AVAILABILITY Be able to access information during regular office hours.
Email	AVAILABILITY Access to information is required 24/7. CONFIDENTIALITY Should only be seen by authorized or intended recipients.
ABC Systems	AVAILABILITY Support is required 24/7.
Connectivity to Internet	AVAILABILITY Access to information is required 24/7.
Help Desk	AVAILABILITY It's needed only during regular business hours, except for emergency room support, which is 24/7.
FRKS, PMS, ECDS, & MLS	AVAILABILITY Access to information is required 24/7. **INTEGRITY** The integrity of the information on the servers must be maintained. CONFIDENTIALITY The confidentiality of patient information and other confidential data must be supported.

Summary of Technical Vulnerabilities Discovered by the Pen-Testers

Asset	Vulnerability	Description
Windows 10 OS	CVE-2020-5855	Unauthorized users who have physical access to the Windows 10 workstations can get shell access with administrative privileges
	CVE-2015-5628	Allows attackers to remotely execute their code on Windows 10 workstations
Red Hat Linux 6 OS	CVE-2009-4067	Unauthorized users who have physical access to the RH6 workstations to execute their own code on the machines, cause denial-of-service attack by using crafted USB device, or take full control of the system
	CVE-2019-19332	User (authorized or unauthorized) who is able to get access to "/dev/kvm" device could exploit this vulnerability to crash the systems resulting in a denial-of-service attack

Current Strategic Practices (SP) of AMC

The following tables summarize the survey information for each area of strategic practices. The information for each area is provided in two tables. First, a summary of the answers to the survey questions from each level of the organization is provided. Then, contextual information from each level relative to the area is provided. The comments sometimes contradict the survey answers. This can be expected as discussion can clarify the meaning of a question or counter any effort at white-washing the issue. Note that AMC did not feel it was necessary to remove attribution to the level of the organization. AMC personnel believe that their organization is open and honest enough not to misuse the information.

The following legends apply to the contents of the tables.

Legend
As perceived by personnel at this level:
yes – The practice is most likely used by the organization.
no – The practice is most likely not used by the organization.
unclear – It is unclear whether the practice is present or not.
blank – The question was not asked of this level.

Criteria:
Yes: 75% or more of respondents replied yes.

No: 75% or more of respondents replied no.

Unclear: Neither the yes nor no criteria were met.

Strategic Practices- Security Awareness and Training (SP1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes	No	No	Unclear
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Unclear	Yes	Unclear	Unclear
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Unclear	Unclear	Unclear	Unclear

Strategic Practices- Security Awareness and Training (SP1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We have training, guidance, regulations, and policies.	Personnel understand systems, but not incident management and/or recognizing and reporting anomalies.
Operational Area Management	Awareness training is required to gain account/access.	Lack of training for IT personnel Staff does not understand security issues
Staff		Who do you call with a problem? Who is responsible? Weakness in the training as it relates to PDIS, Medical Records, and other systems No understanding of my role or responsibility for security
IT Staff	100% security awareness training is done.	Awareness training is inadequate.

Strategic Practices- Security Strategy (SP2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
The organization's business strategies routinely incorporate security considerations.	No	Unclear		No
Security strategies and policies take into consideration the organization's business strategies and goals.	Unclear	Unclear		No
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Yes	Unclear		No

Strategic Practices- Security Strategy (SP2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		Lack the business sense, a proactive philosophy
Operational Area Management		Current protection strategy is not effective.
IT Staff		Lack of exposure to end-user activity

Strategic Practices- Security Management (SP3): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Management allocates sufficient funds and resources to information security activities.	Yes	Yes	Unclear	No
Security roles and responsibilities are defined for all staff in the organization.	Yes	Yes	Unclear	Unclear
The organization's hiring and termination practices for staff take information security issues into account.	Unclear	Yes	Unclear	Unclear
The organization manages information security risks, including assessing risks to information security taking steps to mitigate information security risks	No	No	Unclear	Unclear
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	No	Unclear		No

Strategic Practices- Security Management (SP3): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We are doing this risk evaluation, so that's a start.	I don't think we actually get those kind of reports; maybe we should.
Operational Area Management		Concerned about complacency – we've been very lucky so far.
IT Staff		Inadequate budget and staff. Out-of-date equipment and software

Strategic Practices- Security Policies and Regulations (SP4): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes	Yes	Unclear	Yes
There is a documented process for management of security policies, including creation, administration (including periodic reviews and updates), and communication	Yes	Yes	Unclear	Unclear
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes	Yes		No
The organization uniformly enforces its security policies.	Unclear	No	No	No

Strategic Practices- Security Policies and Regulations (SP4): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	Policies and procedures exist. Training guidance and regulations exist.	Consequences, or lack thereof, for violating policies and procedures are not well-known; we're not enforcing our own policies.
Operational Area Management	People know whom to call when a security incident occurs.	People don't always read or follow policies and procedures.
Staff		Poor communication of policies
IT Staff	There are established incident-handling policies and procedures.	Lack of follow-up on reported violations of security procedures Inability of IT staff to enforce procedures

Strategic Practices- Collaborative Security Management (SP5): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including protecting information belonging to other organizations understanding the security policies and procedures of external organizations ending access to information by terminated external personnel	Yes	Yes	Unclear	Yes
The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.	Unclear	Unclear		No

Strategic Practices- Collaborative Security Management (SP5): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		Distributed management of PDIS; lack of centralized control
Operational Area Management		Reliance on multiple organizations to support our networks
IT Staff	ABC Systems is responsible for security on their systems and networks; they are using good security practices (have a firewall, running Crack, etc.)	Lack of a single focal point for connectivity. Things get confused sometimes.

Strategic Practices- Contingency Planning/Disaster Recovery (SP6): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
An analysis of operations, applications, and data criticality has been performed.	Yes	Unclear		Unclear
The organization has documented, reviewed, and tested business continuity or emergency operation plans disaster recovery plan(s) contingency plan(s) for responding to emergencies	No	Unclear		Unclear
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	No	No		No
All staff are aware of the contingency, disaster recovery, and business continuity plans understand and are able to carry out their responsibilities	Yes	Unclear	No	Unclear

Contingency Planning/Disaster Recovery (SP6): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We do have a disaster recovery plans for natural disasters and some emergencies.	We don't have a business continuity plan.
Operational Area Management		Lack of business continuity and disaster recovery plans
Staff		I'm sure we have them, but I've never seen them and I'm not sure what I'm supposed to do.
IT Staff		Lack of contingency plans if the network stays down or we lose the servers

Current Operational Practices (OP) of AMC

The following tables summarize the survey information for each area of operational practices. The information for each area is provided in two tables. First, a summary of the answers to the survey questions from each level of the organization is provided. Then, contextual information from each level relative to area is provided. The comments sometimes contradict the survey answers. This can be expected as discussion can clarify the meaning of a question or counter any effort at white-washing the issue. Note that AMC did not feel it was necessary to remove attribution to the level of the organization. AMC personnel believe that their organization is open and honest enough not to misuse the information.
The following legends apply to the contents of the tables.

Legend
As perceived by personnel at this level:
yes – The practice is most likely used by the organization.
no – The practice is most likely not used by the organization.
unclear – It is unclear whether the practice is present or not.
blank – The question was not asked at this level.

Criteria:
Yes: 75% or more of respondents replied yes.

No: 75% or more of respondents replied no.

Unclear: Neither the yes nor no criteria were met.

Operational Practices- Physical Security Plans and Procedures (OP1.1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Unclear	Unclear	Unclear	No

Operational Practices- Physical Security Plans and Procedures (OP1.1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There are documented policies and procedures for managing visitors.	Yes	Yes	Unclear	Yes
There are documented policies and procedures for physical control of hardware and software.	Yes	Yes	Unclear	Yes

Operational Practices- Physical Security Plans and Procedures (OP1.1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		Not sure how often the plans are tested
Operational Area Management		Little challenging of people after hours Once sensitive data is printed and distributed, it's not properly controlled or handled.
Staff		If someone enters through the emergency room entrance, they can get anywhere. Storage space for sensitive information is insufficient.
IT Staff	Hardware security is very good.	

Operational Practices- Physical Access Control (OP1.2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes	Yes	Unclear	Unclear
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes	Yes	No	Yes

Operational Practices- Physical Access Control (OP1.2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff	We are required to lock up our offices at the end of the day.	Physical security is hampered by location/distribution of terminals need to share terminals shared office space sharing codes to cypher locks multiple access points to rooms
IT Staff	Hardware security is very good.	

Operational Practices- Monitoring and Auditing Physical Security (OP1.3): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Maintenance records are kept to document the repairs and modifications of a facility's physical components.				Yes
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.				No
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.		Unclear		No

Operational Practices- Monitoring and Auditing Physical Security (OP1.3): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		Never actually seen an overall audit report on maintenance/repairs
Staff		
IT Staff		We track repairs and modifications. Audit records are spotty. Not sure we ever review them.

Operational Practices- System and Network Management (OP2.1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes	Unclear		No
Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information).				Yes
The integrity of installed software is regularly verified.				Yes
All systems are up to date with respect to revisions, patches, and recommendations in security advisories.				Unclear
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Yes	Unclear	No	Yes
Changes to IT hardware and software are planned, controlled, and documented.				Yes
IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.				Yes
Only necessary services are running on systems – all unnecessary services have been removed.				Unclear

Operational Practices- System and Network Management (OP2.1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	There is a security plan. ABC Systems has one.	
Operational Area Management		Not sure everyone outside of IT understands they have responsibilities
IT Staff	We know what we're supposed to do. ABC Systems does all of the virus and vulnerability checking. They send us the results. Systems are protected well with passwords, authorizations, etc. We force users to change passwords regularly. ABC Systems has reported very few intrusions.	There's no documented plan. ABC Systems must keep up to date with security notices, but I'm not sure. I don't think we clean up inherited access rights very well. One of the managers brought a database system down last week with access rights he should not have had. We are looking into that.

Operational Practices- System Administration Tools (OP2.2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.				Unclear

Operational Practices- System Administration Tools (OP2.2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff	ABC Systems is supposed to run most of these tools from their site.	We run some of them and we're supposed to get updated versions and training, but that hasn't happened lately.

Operational Practices- Monitoring and Auditing IT Security (OP2.3): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.				Unclear
Firewall and other security components are periodically audited for compliance with policy.				Yes

Operational Practices- Monitoring and Auditing IT Security (OP2.3): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff	ABC Systems does all of the audits. ABC Systems runs monitoring tools.	I don't think ABC Systems reports unusual activity to anyone here – not sure if the response is according to our policy or theirs.

Operational Practices- Authentication and Authorization (OP2.4): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.		Unclear		Yes
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	Yes		Yes
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.				Yes

Operational Practices- Authentication and Authorization (OP2.4): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management	There are polices for access control and permissions.	But, we're not using role-based management of accounts and people inherit far too many privileges.
Staff		
IT Staff	Systems are protected well with passwords, authorizations, etc.	

Operational Practices- Vulnerability Management (OP2.5): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts keeping up to date with known vulnerability types and attack methods reviewing sources of information on vulnerability announcements, security alerts, and notices identifying infrastructure components to be evaluated scheduling of vulnerability evaluations interpreting and responding to the results maintaining secure storage and disposition of vulnerability data				Unclear
Vulnerability management procedures are followed and are periodically reviewed and updated.				Unclear
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.				Unclear

Operational Practices- Vulnerability Management (OP2.5): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff	ABC Systems does all of the vulnerability management and assessment activities. They do a good job.	We haven't been trained on what to do with those vulnerability reports. We usually file them in a drawer.

Operational Practices- Encryption (OP2.6): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).				Yes
Encrypted protocols are used when remotely managing systems, routers, and firewalls.				Yes

Operational Practices- Encryption (OP2.6): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff		

Operational Practices- Security Architecture and Design (OP2.7): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures history of security compromises results of security risk assessments				Unclear
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.				Yes

Operational Practices- Security Architecture and Design (OP2.7): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff		They're already building PDIS II and no one ever talked to us about what it should have for security. Maybe ABC Systems already knows.

Operational Practices- Incident Management (OP3.1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes	Unclear	Unclear	Yes
Incident management procedures are periodically tested, verified, and updated.	Unclear	No	Unclear	No
There are documented policies and procedures for working with law enforcement agencies.	No	No	No	Unclear

Operational Practices- Incident Management (OP3.1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		Never even considered dealing with law enforcement for security problems until just now.
Operational Area Management	Procedures exist for incident response.	Not everyone is aware of the procedures.
Staff		I don't know if I'm supposed to do anything or what to look for. Who do we call?
IT Staff		I suppose we should call law enforcement if the system really gets attacked. But who calls – us or ABC Systems?

Operational Practices- General Staff Practices (OP3.2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Staff members follow good security practice, such as securing information for which they are responsible not divulging sensitive information to others (resistance to social engineering) having adequate ability to use information technology hardware and software using good password practices understanding and following security policies and regulations recognizing and reporting incidents	Unclear	Unclear	No	Yes
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Unclear	No	Unclear	Yes
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	Unclear	No	Yes

Operational Practices- General Staff Practices (OP3.2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		Fairly certain people share passwords and accounts
Operational Area Management		I've heard they have so much trouble logging in and out and moving from machine to machine that they just don't bother.
Staff	We get "don't share passwords" type of training.	Physical layouts, insufficient equipment, cramped space – all leads to sharing passwords, accounts, machines, whatever. We all trust each other.
IT Staff	All staff are trained on passwords.	

Cybersecurity Risk Assessment of AMC
[Printed Report Due on Monday, March 16th2019, 5 pm]

- **Title Page**- This page contains the name of the group, course ID, section number, the name of team members, and the Aggie Honor Code signed by each team member.
- **Table of Contents Page**
- **Executive Summary**- No more than a page. Contains a summary of your project goals, your assessment of the cybersecurity risks that AMC faces, and your recommendation to minimize those risks
- **Asset Identification**- A brief explanation of your task in this phase of the project and the list of assets identified by your team.
- **Asset Classification**- A brief explanation of your task in this phase of the project and the ranking of assets identified by your team in the previous step. Refer to the appropriate appendix for explanation of the asset value scores. [NOTE: you will lose points if the measurement scale for scoring the financial, operational, and legal scales are not clearly defined in the appendix].
- **Vulnerability and Threat Identification**- A brief explanation of your task in this phase of the project. Provide (in table format) the threat statements for each asset. Based on your project guidelines, you should have at least 4 threat statements for each assets, and these statements should include at least two technical vulnerabilities (with CVE IDs) and two non-technical vulnerabilities (due to gaps in administrative and physical controls). Refer to the appropriate appendix for explanation of the vulnerabilities. For each threat statement, refer to the appropriate appendix for related tree analysis. [NOTE: You will lose additional points if the non-technical vulnerabilities identified in this phase are not supported by evidence from the case, i.e. you *assume* these vulnerabilities to exist without any evidence from the case].
- **Cybersecurity Risk Estimation**- A brief explanation of your task in this phase of the project. Provide (in table format) the cybersecurity risk associated with each threat statements for each asset. This section should also contain the scores of Likelihood and FIV for each threat statement. Refer to the appropriate appendix for explanation of these scores.
- **Cyber Security Risk Management Strategy**- Provide cybersecurity risk management strategy for each threat statement. Where the strategy is to mitigate or eliminate risk, provide specific controls that need to be implemented. Where possible (of if information available online) provide the cost of implementing these controls.
- **Appendices- Measurement Scales**
    - **Appendix A**- Measurement scales used for Asset Classification (in terms of financial, operational, and legal impacts of asset failure). [NOTE: You will lose points if you do not describe/define/explain the financial criteria, key business processes, and the law used for legal impact].
    - **Appendix B-** Provide the Vulnerability-Threat identification tree(s) in this appendix. Also, provide a brief description of the vulnerabilities in this section.
        - **For the technical vulnerabilities-** Provide their CVE ID, a link to the NVD page where information is available for this vulnerability, a brief description of the vulnerability, Exploitability Score, Impact Score, and Vector information (e.g., *Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)*.
        - **For the non-technical vulnerabilities-** Provide evidence from the case that this vulnerability exists, a brief description of the vulnerability, calculated Exploitability Score, calculated Impact Score, and Vector information (e.g., *Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)*.
    - **Appendix C**- Measurement Scale for scoring Threat Likelihood (in terms of CVSS V3 Exploitability Scores).
    - **Appendix D**-
        - Estimation of Final Impact Value (as a function of Asset Value Scores and CVSS V3 Impact Score). [NOTE: You will lose additional points if the score range for asset value and CVSS V3 score range is not the same (i.e. 0-10)].
        - Measurement Scale used for scoring FIV for a Threat Statement (in terms of FIV values)
    - **Appendix E**- Cybersecurity Risk Matrix and Risk Management Strategy for various cybersecurity risk values
    - **Appendix F**- Any assumptions made by the project team
    - **Appendix G**- Baseline for hardening Windows 10 workstations used by AMC employees
    - **Appendix H**- Network Access Policy and corresponding ACL for Windows Defender Firewall
- **References**
- **Glossary-** Provide a brief explanation of terms and abbreviations to explain them to a reader who is not an expert in information systems and/or cybersecurity
- **Team Work-** Provide (in table format) the contribution of each group member to the project

Additional Suggestions

1. Number and label each table and figure
2. Number the pages
3. Proof read for grammatical and/or spelling mistakes
4. Format the report to improve its readability