Cybersecurity Risk Assessment Report

Aggieland Medical Center (AMC)

A Qualitative Risk Assessment for Critical Information Systems

Submitted By :

Ruchira Bhat (636000154)

Divya Shreshta Gajula (33004478)

Maitri Heerpara (635008347)

Chadani Acharya (534009207)

18 April 2025

ISTM 635 - Business Information Security

Section: 602

Confidential Information Statement:

This document contains sensitive information pertaining to the information systems, cybersecurity posture, and operational processes of Aggieland Medical Center (AMC). It has been prepared solely for academic purposes in the context of the ISTM 635 course. Unauthorized distribution, reproduction, or disclosure of this document or its contents is strictly prohibited outside the designated educational setting.

EXECUTIVE SUMMARY

Aggieland Medical Center (AMC), a regional healthcare provider with critical operations in College Station and satellite clinics across Bryan and Navasota, conducted a qualitative cybersecurity risk assessment to evaluate its exposure to cyber threats and inform risk mitigation strategies. The assessment followed the NIST SP 800-30 framework and began by identifying twelve essential business processes and ten key IT assets, ranging from core systems like the Patient-Data Information System (PDIS) to third-party managed infrastructure. Fourteen technical, administrative, and physical vulnerabilities were identified across these assets, including unpatched CVEs, misconfigured firewalls, excessive privilege inheritance, and a lack of business-continuity planning. These weaknesses were mapped to ten realistic threat scenarios such as ransomware attacks, supply-chain compromises, insider misuse, and social engineering.

Each threat scenario was evaluated for its likelihood of occurrence based on adversary motivation and exploitability, and for potential adverse impact on confidentiality, integrity, availability, legal compliance, and operational continuity. Cross-analysis revealed that four threats - unauthorized network intrusion (T1), email-based ransomware (T7), malware propagation via firewall misconfiguration (T8), and vendor console compromise (T9) pose very high overall risk to AMC's critical operations and regulatory standing. Recommended actions include strengthening patch and privilege management, implementing multi-factor authentication, improving incident response protocols, and enhancing vendor oversight. These targeted controls will enable AMC to better protect patient data, sustain healthcare delivery, and uphold compliance under evolving threat conditions.

TABLE OF CONTENTS

INTRODUCTION

In an increasingly digital healthcare environment, cybersecurity risks are no longer confined to the data center. they have real implications for patient care, operations, and trust. Recognizing this, Aggieland Medical Center (AMC), a regional hospital system based in College Station, Texas, initiated a qualitative cybersecurity risk assessment to understand where its most critical exposures lie. With two remote clinics, two labs, and a lean in-house IT team supported by an external contractor (ABC Systems), AMC operates with a complex but resource-constrained technology footprint that supports direct patient care, administrative operations, and compliance obligations.

The assessment was commissioned by AMC leadership not only as a proactive cybersecurity measure but also as a means to ensure that clinical systems remain reliable, patient data stays protected, and the organization can meet its regulatory commitments under HIPAA and related frameworks. Beyond technical scans, the process involved direct engagement with AMC staff, from department heads to clinicians and IT personnel to expose operational details that are not always reflected in logs or audit trails. Their input shaped our understanding of how systems are used, where safeguards might be falling short, and how risks manifest in the day-to-day flow of care and administration.

This report captures the findings and analysis from the full risk assessment process by combining technical data, staff input, and operational context into a structured evaluation of AMC's cybersecurity posture.. Following the structure outlined in NIST SP 800-30 Rev. 1, it identifies AMC's critical business functions and the IT systems that support them, catalogs vulnerabilities across technical, administrative, and physical domains, assesses threat scenarios and likelihoods, and evaluates the potential impact of compromise. Our goal is not just to list risks but to connect them to the workflows, people, and decisions that make AMC function. In doing so, we aim to provide leadership with actionable insight, not just into where threats exist, but how to prioritize them in a way that aligns with AMC's mission, capacity, and risk tolerance.

1. IDENTIFY KEY BUSINESS PROCESSES AND IT ASSETS

This step establishes the foundation for AMC's cybersecurity risk assessment by identifying its most critical business processes and the IT assets that support them. Understanding how technology enables clinical care, administration, and operations allows us to map vulnerabilities and assess risk exposure accurately.

1.1 IDENTIFY KEY BUSINESS PROCESSES

Objective:

The purpose of this step is to identify the critical business processes at Aggieland Medical Center (AMC) that are essential for its day-to-day operations and long-term strategic goals. Disruption to any of these processes due to cybersecurity threats can have serious operational, financial, legal, and reputational consequences.

What We Did:

The risk assessment team thoroughly reviewed AMC's operations and conducted interviews with key personnel, including senior managers, operational area managers, and IT staff. This enabled us to accurately map out the essential processes critical to AMC's daily and strategic functioning. Each identified business process was documented with specific activities and classified into one of three categories: Core, Support, or Management.

- Core processes are those directly involved in delivering healthcare services essential to AMC's primary mission.
- Supporting processes facilitate the smooth functioning of core processes without directly generating revenue.
- Management processes encompass activities related to governance, strategic decision-making, risk assessment, compliance, and operational oversight.

The identified business processes and their associated tasks are documented systematically for clarity and ease of reference in subsequent risk assessment stages.

TABLE 1: AMC - Business Processes Identified for Cybersecurity Risk Assessment					
Process ID	**Process Name**	**Activities-Tasks**	**Type of Process**		
			Core	**Support**	**Management**
BP-1	Patient Encounter / Clinical Care	– Register patient (walk-in, referral, or scheduled) – Retrieve/update chart in PDIS – Examination, diagnosis & treatment by physician / nurse – Document orders, progress notes, discharge instructions	X		
BP-2	Emergency Care Delivery (ECDS)	– Triage & stabilise patient – Enter vitals & diagnosis into ECDS – Order laboratory tests / radiology – Produce encounter report for billing & epidemiology	X		
BP-3	Medication Dispensing & Verification	– Provider prescribes via PDIS – Pharmacy System (RxS) checks allergies / contraindications – Dispense drug; update inventory & patient record	X		
BP-4	Laboratory & Diagnostic Testing	– Collect specimen – Perform test in remote lab – Upload results into PDIS / ECDS – Alert ordering provider of critical values	X		

BP-5	Revenue-Cycle & Insurance Billing (FRKS)	– Generate charges from clinical systems – Verify insurance, co-pay, pre-auth – Submit electronic claims & post remittance – Manage patient statements & collections		X	
BP-6	Medical Logistics & Procurement (MLS)	– Forecast supply needs – Issue purchase orders to pre-certified vendors (external access) – Receive & stock supplies/equipment – Reconcile invoices		X	
BP-7	Human Resources & Credential Management (PMS)	– On-board new hires / providers – Maintain salary, demographics, skills and disciplinary data – Verify licenses & certifications – Off-board & privilege revocation		X	
BP-8	Information-Release & External Relations	– Evaluate requests from press / insurers – Pull authorised data from PDIS – Apply Privacy-Act filters – Log & archive disclosures		X	

BP-9	IT Operations & User Support	– Help-desk ticket intake and triage – Account provisioning & workstation setup – Coordinate with ABC Systems for server/network maintenance – Patch and vulnerability management		X	
BP-10	Governance, Risk & Compliance	– Define cybersecurity and privacy policies – Conduct risk assessments – Oversee incident-response, audit and regulatory reporting			X
BP-11	Strategic & Financial Management	– Long-range planning, budgeting, capital projects – Contract oversight (e.g., ABC Systems SLA) – Performance review & quality-improvement initiatives			X
BP-12	Operational Risk Management	– Evaluating and managing threats to availability, integrity, and confidentiality of data systems			X

Outcome of this Step:

Twelve essential business processes were identified at AMC. These processes form the foundation for AMC's healthcare delivery, administrative support, and strategic management. Clear classification into Core, Support, and Management categories enables focused risk assessment in subsequent stages.

1.2 IDENTIFY IT ASSETS

Objective:

The primary goal of this step is to identify and document critical IT assets at Aggieland Medical Center (AMC). This step is vital as cyberattacks targeting these IT assets can severely disrupt the essential business processes dependent on them, affecting AMC's operational effectiveness, strategic objectives, and regulatory compliance. This aligns with the guidance provided in NIST Special Publication 800-30 at the Tier 3 level, which emphasizes detailed evaluation of system-specific cybersecurity risks.

What We Did:

The risk assessment team conducted a thorough inventory of AMC's IT assets. The identification was based on several key considerations:

- **Functionality:**

  The role of each asset in supporting AMC's business processes, particularly focusing on their operational criticality in healthcare delivery and administrative tasks.

- **Data Sensitivity:**

  Classification of data stored or processed by each IT asset, prioritizing assets handling protected health information (PHI), personally identifiable information (PII), and financial data, given their higher risk profiles.

- **Asset Utilization:**

  Identifying primary users and locations where these assets are deployed, ensuring comprehensive coverage across clinical, administrative, and IT management areas.

- **Prior Documentation & Interviews:**

  Leveraging prior risk assessments, vulnerability scans, and interviews with AMC's senior management, operational staff, and IT teams to verify accuracy and completeness of the IT asset inventory.

In this step, we identify the critical IT assets that support Aggieland Medical Center's key business processes. Each asset is evaluated at the system level and includes its role in healthcare delivery, data handling, and operational continuity. This identification is essential for understanding which systems, platforms, or infrastructure components, if compromised, could significantly disrupt AMC's ability to serve patients, comply with regulations, or maintain internal operations.

The assets listed span across electronic medical records (EMR) systems, financial and HR platforms, communication infrastructure, automation systems, and remote management tools. The justification for each asset reflects its business value, sensitivity of data handled, and potential impact in the event of unavailability, integrity failure, or confidentiality breach.

TABLE 2: AMC - Example of IT Assets at the system, component, hardware, and software levels

Asset ID	System	Components	HW	SW
IT-A	Patient-Data Information System (PDIS)	Database server; application server; workstations across physicians' offices, treatment rooms, labs and admin areas; Cisco ASA firewall; internal network (routers, switches, Wi-Fi)	Servers that host PDIS; workstations; Cisco ASA firewall; Cisco 2951 router; Cisco SG100D-08 switch; Wi-Fi APs; cabling	MS SQL Server (vulnerabilities CVE-2022-29143/-1636); operating system (Windows Server—implied by the MS-SQL stack); PDIS application software; ASA firmware
IT-B	Financial Record-Keeping System (FRKS)	Billing database; claim-submission module; staff workstations	Server that stores financial records; workstations; printers (for invoices/claims)	MS SQL Server (same CVEs as above); operating system (Windows Server); billing/insurance application (not named)
IT-C	Personnel Management System (PMS)	Employee/credential database; payroll-processing module	Server; HR workstations	Operating system (Windows Server); HR/credential-management software (not named)

IT-D	Pharmacy System (RxS)	Automated drug-dispensing unit; medication/payment interface to PDIS	Drug-dispensing kiosk; supporting server; pharmacy workstations	Pharmacy-management application (not named); operating system (implied Linux/embedded, not specified)
IT-E	Medical Logistics Server (MLS)	Procurement application; vendor VPN access for external suppliers	Server that hosts MLS; network gear enabling remote-vendor connection	Operating system (Linux implied by Red Hat reference for other servers); procurement software/VPN service (not named)
IT-F	Emergency-Care Data System (ECDS)	Real-time ER/trauma database; reporting/analytics engine	Server supporting ECDS; ER-area tablets/workstations (used for triage/entry)	Operating system (Windows Server implied); ECDS application (not named)
IT-G	Email System	Central email server; client email software on all workstations	Email-server hardware; user workstations	Sendmail 8.9.3 on Red Hat Linux 6 (server); email-client software (e.g., Outlook, not named)
IT-H	Network & Security Infrastructure	Cisco ASA firewall; routers; switches; Wi-Fi; internet gateway; network-monitoring tools managed by ABC Systems	Cisco ASA firewall; Cisco 2951 router; Cisco SG100D-08 switch; Wi-Fi APs; structured cabling; IT-staff workstations	ASA firmware; router/switch IOS; vulnerability-scanning and network-monitoring software run by ABC Systems (not named)

IT-I	Workstation Fleet (Windows 7 / Windows 10 – clinical & administrative)	Desktop PCs in physicians' offices, treatment rooms, nursing stations, labs and admin areas; lightweight TSP thin-clients that clinicians carry between rooms	Desktop / thin-client hardware located throughout the hospital (no vendor model specified)	Windows 7 and Windows 10 operating-system images (both found vulnerable in the scan)
IT-J	ABC Systems Remote-Management Platform	Off-site management console; vulnerability-assessment tools; system & network monitoring tools; privileged user-provisioning/administration services	Servers hosted at ABC Systems' NOC that run the console and tools (specific models not stated)	Vulnerability-assessment software, monitoring/audit tools, patch-management utilities operated by ABC Systems

Understanding these assets allows us to map vulnerabilities, threats, and risks more effectively in subsequent steps of the cybersecurity risk assessment.

This table presents a detailed inventory of Aggieland Medical Center's IT assets, outlining the specific reasons for their inclusion in the cybersecurity risk assessment. Each asset listed is critical due to its role in maintaining healthcare service delivery, data security, operational continuity, and regulatory compliance.

TABLE 3: AMC - IT Assets Identified for Cybersecurity Risk Assessment		
Asset ID	**Asset Description**	**Justification**
IT-A	**Patient-Data Information Server (PDIS)** – central electronic medical-records database	– Supports *every* direct-care workflow and is the single source of truth for PHI. – Loss of availability stalls admissions, labs and prescribing; loss of confidentiality triggers Privacy-Act liability; loss of integrity can injure patients.
IT-B	**Financial Record-Keeping Server (FRKS)** – billing & claims	– Produces all invoices and insurance submissions; errors directly cut revenue and invite HIPAA/PCI findings. – Holds sensitive financial data whose exposure harms both AMC and patients.
IT-C	**Personnel Management Server (PMS)** – HR & credentialing	– Stores staff PII and licence data; tampering could let unqualified personnel practise, or enable identity fraud.
IT-D	**Pharmacy System (RxS)** – automated drug dispensing	– Interfaces with PDIS to check allergies and prescriptions; corrupted data could cause medication errors that jeopardise patient safety.
IT-E	**Medical Logistics Server (MLS)** – procurement & inventory	– Tracks every critical supply (PPE, reagents, implants). – A prolonged outage or falsified data can lead to stock-outs that halt surgery and bedside care.
IT-F	**Emergency-Care Data System (ECDS)** – real-time ER/trauma charting & analytics	– Guides life-critical decisions in the emergency department; outages or tampering can delay care or feed clinicians bad data. – Generates regulatory reports on population-health and accidents.

TABLE 3: AMC - IT Assets Identified for Cybersecurity Risk Assessment		
IT-G	**Email Server (Sendmail 8.9.3)** – internal & external messaging	– Primary communication path for treatment plans and scheduling. – Legacy OS and MTA versions contain known CVEs that make it a common ransomware/phishing entry point carrying PHI.
IT-H	**Network & Security Infrastructure** – core switches, routers, Wi-Fi, Cisco ASA	– Single backbone linking hospital, clinics and labs; mis-config or DoS simultaneously severs all clinical, billing and remote-access services.
IT-I	**Workstation Fleet (Win 7/10, clinical & admin)**	– First-line access to every other system; widespread shared logins and unpatched CVEs make them the easiest compromise vector.
IT-J	**ABC Systems Remote-Management Platform** – vendor VPN & patch console	– Third-party tool with privileged reach into IT-1 through IT-6; represents a classic supply-chain attack surface and single-SLA dependency.

Outcome of this Step:

A comprehensive and detailed inventory of AMC's critical IT assets was developed. Each asset was thoroughly documented with its associated system components, hardware (HW), and software (SW), clearly outlining their roles, functionalities, and dependencies. This structured approach provides an essential foundation for subsequent steps involving vulnerability identification, threat assessment, and risk evaluation.

2. IDENTIFY VULNERABILITIES

Objective:

To uncover and catalog all weaknesses, whether in technical controls, administrative processes, or physical safeguards, across Aggieland Medical Center (AMC) that could be exploited by threat agents. This includes not only system-level flaws (e.g., unpatched software, misconfigurations) but also gaps in governance, external

dependencies, business processes, and overall security architecture, in line with NIST's broad view of vulnerabilities.

What We Did:

1. **Reviewed Case Study Definition & Scope:** Adopted the provided definition of "vulnerability" as any weakness in systems, procedures, controls, or implementation that could be leveraged by an adversary. Expanded the scope to include organizational governance, third-party relationships (e.g., ABC Systems), business-process deficiencies (e.g., session management), and resiliency architecture (e.g., lack of BC/DR).
2. **Analyzed Technical Scan Results:** Examined AMC's vulnerability scan (page 5) to identify CVEs affecting Windows 7/10 workstations, Red Hat Linux 6 email servers, MS SQL Server, and network devices.
3. **Conducted Stakeholder Interviews & Workshops:** Engaged senior managers, operational leads, general staff, and IT personnel to document policy gaps (inadequate training, privilege provisioning), insecure user practices (shared passwords, missing auto-logout), and physical control lapses (unlocked server rooms, unsupervised TSPs) across pages 6–13.
4. **Mapped Weaknesses to Classification:** For each identified issue, determined whether it represented a technical, administrative, or physical vulnerability, per the assessment guidelines.
5. **Documented Findings in Table 4:** Compiled all 12 distinct vulnerabilities into the standardized format to support subsequent threat and risk quantification.

TABLE 4: AMC - Vulnerabilities Present in the Organization						
IT Asset ID	**Vulnerability ID**	**Vulnerability**	**Classification**			**Details**
			Technical	**Administrative**	**Physical**	
IT-I	V1	Outdated Windows 7 OS on clinical & administrative workstations	X			CVE-2015-6131, CVE-2015-6127 (workstation scan results) – p. 5
IT-I	V2	Outdated Windows 10 OS on clinical workstations	X			CVE-2022-21851, CVE-2022-21922 (workstation scan results) – p. 5
IT-G	V3	Outdated Red Hat Linux 6 on email server	X			CVE-2000-0633, CVE-2000-0219 (email-server scan results) – p. 5
IT-A	V4	Outdated MS SQL Server used by PDIS	X			CVE-2022-29143, CVE-2021-1636 (PDIS/FRKS scan results) – p. 5
IT-H	V5	Firewall misconfiguration	X			“Systems are susceptible to

		permitting malware/virus propagation				malicious code … due to configuration of the firewall" – p. 9
IT-J	V6	AMC's reliance on ABC Systems for network and patch management introduces a supply chain attack surface — if ABC is breached, AMC is exposed.	X			Dependency on ABC Systems' off-site console, network-monitoring tools, and patch management creates a supply-chain attack surface when the vendor's infrastructure is compromised—"ABC Systems also does network management and maintenance for AMC" (Case Study, p. 3) .
IT-I	V7	Workstations do not auto-logout or enforce session time-outs		X		"Passwords, logouts, timeouts, and screen savers are inconsistently used" – p. 12

IT-I	V8	Shared passwords and weak session controls		X		"We were told not to share passwords … but everyone knows and trusts each other" – p. 11
IT-A	V9	Inadequate security training for PDIS users (incident recognition & response)		X		"Everyone gets the same basic security training, but it only covers passwords" – p. 8
IT-A	V10	Excessive privileges inherited during account provisioning in PDIS		X		"I inherited everything my predecessor had … I really fouled up some of the records." – p. 9
IT-A	V11	No Business Continuity / Disaster Recovery plan for PDIS		X		"The organization has no documented, reviewed, or tested business continuity or disaster recovery plans." – p. 18

IT-J	V12	Lack of vulnerability management and remediation		X		AMC collects vulnerability-scan results from ABC Systems but does not review or remediate them—"we usually file them in a drawer" (p. 22) .
IT-B	V13	No physical access controls on the FRKS server room			X	"There's no physical security for the room where staff log on to FRKS. Anyone could wander in." – p. 7
IT-A	V14	Unsupervised TSPs/workstations in open areas, allowing unauthorized viewing or tampering			X	"We've got a lot of workstations out in the open … what happens when they leave the TSP in the room?" – p. 8. No mention of

Outcome of this Step:

A comprehensive vulnerability register (Table 4) now exists, detailing twelve discrete weaknesses spanning:

- **Technical** flaws (unpatched CVEs, firewall misconfiguration),

- **Administrative** gaps (insufficient training, legacy account provisioning, no BC/DR), and
- **Physical** exposures (unsecured server rooms, open-area workstations).

This structured inventory provides the essential baseline for estimating threat likelihood, assessing potential impacts, and prioritizing remediation in the next phases of the cybersecurity risk assessment.

3. IDENTIFY THREATS

Objective:

In this step, the goal is to identify realistic threat events that could exploit known vulnerabilities in AMC's IT infrastructure. These threats, if realized, could negatively affect the confidentiality, integrity, or availability of critical systems, potentially disrupting healthcare delivery, exposing sensitive data, or impairing compliance with regulatory obligations such as HIPAA.

What We Did:

The cybersecurity risk assessment team performed a structured threat identification process using AMC's vulnerability data (from Step 2) as the foundation. This process incorporated the following key considerations:

- **Vulnerability Contextualization:**
  Each previously identified vulnerability was analyzed in the context of its associated IT asset, considering how that vulnerability could be exploited in real-world conditions.
- **Threat Agent Profiling:**
  Likely sources of threats were classified into categories such as external adversaries (e.g., hackers, cybercriminals), insiders (e.g., staff, former employees), or unintentional actors (e.g., patients, misconfigured systems). This profiling was guided by prior incidents reported in the AMC case, interviews, and documented risk factors.
- **Threat Event Definition:**
  Specific threat scenarios were defined based on the tactics, techniques, and procedures (TTPs) mentioned in the case file, national cybersecurity advisories (e.g., CISA), and recent threat intelligence relevant to AMC's technology stack.
- **Relevance Rating:**
  Each threat event was assessed for its relevance using the six-level scale provided in the case materials: Confirmed, Expected, Anticipated, Predicted, Possible, and N/A. This categorization was informed by direct incident reports, peer hospital advisories, public vulnerability databases, and staff interviews.

This step is critical to ensure that AMC focuses its cybersecurity efforts on the most plausible and potentially damaging threat scenarios, rather than generic or unlikely risks.

TABLE 5: AMC - Assessment Scale to Measure the Relevance of Threat Events	
Value	**Description**
Confirmed	The threat event / TTP has already occurred within AMC and is documented in service tickets, security-incident reports, or ABC Systems logs (e.g., the recent firewall breach reported by IT staff).
Expected	The threat event / TTP has been experienced by peer regional hospitals, clinics, or laboratories that share similar technology stacks (PDIS, Sendmail 8.x, Cisco ASA) and has been communicated to AMC through the Texas Hospital Association's security-information-sharing channel or ABC Systems advisories.
Anticipated	The threat event / TTP has been flagged by trusted healthcare-sector sources (bulletins, CISA KEV list, or the FBI's PIN notices) as currently targeting U.S. medical centers comparable in size and profile to AMC.
Predicted	Based on AMC's asset profile and known vulnerabilities (e.g., un-patched MS-SQL, legacy Sendmail), reputable threat-intelligence feeds or ABC Systems' risk forecasts assess that this threat event is likely to materialize against AMC within the next 12 months, even though no direct attempts have been detected yet.
Possible	The threat event / TTP has been described by credible industry analysts (e.g., Gartner, ISACs) or observed in other critical-infrastructure sectors, but there is no specific indication—from incidents, intelligence, or peer notifications—that it is presently directed at healthcare providers like AMC.
N/A	The threat event / TTP is not currently applicable to AMC's environment—for example, it targets cloud infrastructures or medical-device types AMC does not use, or credible intelligence indicates no adversary interest. Such events will be excluded from subsequent risk analysis unless conditions change.
TTP => Tactics, Techniques, and Procedures	

TABLE 6: AMC - Threats to IT Assets					
Asset ID	**Vulnerability ID**	**Threat ID**	**Threat Event**	**Threat Agent/Source**	**Threat Relevance**
IT-H	V5	T1	Unauthorized network intrusion ("PDIS actually got hacked last week")	External adversary (unknown hacker)	**Confirmed** – already occurred and documented (p 12)
IT-I	V8	T2	Unauthorized disclosure of patient records ("staff … check out the medical records of people they're dating")	Trusted insider (staff member)	**Confirmed** – insider misuse observed (p 12)
IT-I	V7	T3	Unauthorized access to workstation ("one patient … looked up his wife's record")	External user (patient)	**Confirmed** – patient exploited session (p 12)
IT-A	V11	T4	Extended denial-of-service of PDIS following ransomware or data-destruction with no recovery plan	External adversary (ransomware group)	**Predicted** – based on un-patched CVEs and absence of BC/DR, likely within 12 months (p 18, p 5)
IT-A	V10	T5	Accidental data corruption ("I … inherited everything … I really fouled up some of the records")	Privileged insider (new administrator)	**Confirmed** – mis-provisioning incident (p 8)

IT-A	V9	T6	Social-engineering attempt for PHI (“insurance representatives … trying to trick information out of staff”)	External adversary (insurance representative)	**Possible** – described by staff but not directed at AMC (p 13)
IT-G	V3	T7	Ransomware/phishing infection via email - malicious payloads carrying PHI (Protected Health Information)	External adversary (cybercriminal)	**Expected** – seen in peer hospitals on Sendmail stacks. Report on Harbor Medical Group Ransomware Attack (June 2019) only adds to it.
IT-H	V5	T8	Malware propagation across AMC network through misconfigured firewall	External adversary (malicious actor)	**Predicted** – firewall msconfig opens malware vectors within 12 months (p 9). The Akira ransomware group has exploited a vulnerability (CVE-2020-3259) in Cisco ASA and FTD devices, allowing attackers to extract sensitive data from memory, including usernames and passwords.
IT-J	V6	T9	Supply-chain compromise via ABC Systems remote-management platform	External adversary (vendor-targeting group)	**Anticipated** – flagged by HHS/CISA advisories on third-party consoles (p 3, p 13, p 18)

IT-J	V12	T10	Exploitation of un-remediated vulnerabilities due to ignored scan reports	External adversary (cybercriminal)	**Predicted** – unpatched CVEs filed away, likely targeted in next year (p 22)

NOTE:

- Details of *Asset ID* are provided in *Table 3*.
- Details of *Vulnerability ID* are provided in *Table 4*.
- Explanation of *Threat Relevance* measures is provided in *Table 5*.

Outcome of this Step:

We developed Table 6: Threats to IT Assets, which identifies 10 distinct threats mapped to specific vulnerabilities and IT assets within AMC's infrastructure. The table includes adversarial threats (e.g., ransomware, phishing, privilege misuse), accidental threats (e.g., data entry errors, inherited permissions), and supply-chain risks. Each threat is supported with a defined threat agent/source and a documented relevance score, some of which are backed by page references from the original AMC case.

This threat identification forms the basis for evaluating likelihood and impact in the next phase of the risk assessment, helping AMC prioritize its security controls and mitigation strategies effectively.

4. ESTIMATE THREAT LIKELIHOOD

In this step, we evaluate the likelihood that each identified threat will be initiated by its corresponding agent. This is determined by combining the adversary's motivation (capability, intent, and targeting) with the ease of exploiting the associated vulnerability, based on CVSS 3.1 metrics.

4.1. ADVERSARIAL THREATS

Objectives:

The objective of this step is to assess the motivation of adversarial threat agents who may attempt to exploit identified vulnerabilities in AMC's IT systems. Understanding adversary motivation, including their capability, intent, and targeting focus is critical for estimating how likely it is that a threat event will be initiated.

What We Did:

We conducted a qualitative assessment of each threat agent's motivation using the framework provided in NIST SP 800-30. The process involved:

- **Threat Agent Classification:** Each threat was linked to a specific agent type (e.g., external adversary, trusted insider, patient, vendor).
- **Motivation Criteria Evaluation:** The three key factors **capability**, **intent**, and **targeting** were rated based on evidence such as system logs, interview insights, known CVEs, and national advisories (e.g., CISA).
- **Motivation Score Assignment:** Using the lookup matrix in Table 7B, the ratings were converted into a qualitative motivation score (Very High, High, Moderate, Low, or Very Low).
- **Source Documentation:** Page references were cited for each data point used in the scoring process to ensure transparency and traceability.

TABLE 7A: AMC - Assessment of Threat Agent/Source's Motivation

Threat ID	Threat Agent/Source Description	Source of Information	Capability*	Intent*	Targeting *	Motivation Score**
T1	External adversary (unknown hacker responsible for PDIS breach)	Staff interview (p 12)	Very High	Very High	Very High	Very High
T2	Trusted insider (staff member checking unauthorized records)	Staff interview (p 12)	Moderate	Moderate	Moderate	Moderate
T3	External user (patient who accessed spouse's record)	Staff workshop notes (p 12)	Very Low	Low	Low	Low
T4	External adversary (ransomware group targeting PDIS)	Vulnerability & BC/DR findings (pp 5, 18)	High	Very High	Very High	Very High

T5	Privileged insider (new user with accumulated access who corrupted records)	Interview with admin staff (p 8)	Moderate	Very Low	Very Low	Low
T6	External adversary (insurance representative)	Staff interviews (p 13)	Low	Moderate	High	Moderate
T7	External adversary (cybercriminal) group via email server)	Email-server CVEs & industry advisories (p 5)	High	Very High	High	Very High
T8	External adversary (malicious actor exploiting firewall misconfig)	Firewall findings (p 9)	Moderate	High	Moderate	Moderate
T9	External adversary (vendor-targeting group via ABC Systems console)	ABC Systems dependency (p 4)	Very High	High	High	Very High
T10	External adversary (cybercriminal exploiting unremediated CVEs)	Vulnerability management audit (p 22)	High	Very High	High	Very High

NOTE:

- Details of Threat ID are provided in Table 6.
- ***Assessment Scales** for Threat Agent/Source **Capability**, **Intent**, and **Targeting** is provided in ***APPENDIX A***.

- ****Motivation Score Scale**- This score is obtained from the Look-Up **Table 7B**.

TABLE 7B: AMC - Look-Up table to estimate the qualitative value of Threat Agent/Source's Motivation

Capability	Intent	Targeting	Motivation Score	Motivation Score Explanation
Very High	Very High	Very High	Very High	Adversary is almost certain to initiate the threat event
Very High	Very High	High	Very High	Adversary is almost certain to initiate the threat event
Very High	Very High	Moderate	High	Adversary is highly likely to initiate the threat event
Very High	Very High	Low	Moderate	Adversary is likely to initiate the treat event
Very High	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very High	High	Very High	Very High	Adversary is almost certain to initiate the threat event
Very High	High	High	Very High	Adversary is almost certain to initiate the threat event
Very High	High	Moderate	High	Adversary is highly likely to initiate the threat event
Very High	High	Low	Moderate	Adversary is likely to initiate the treat event
Very High	High	Very Low	Moderate	Adversary is likely to initiate the treat event

Very High	Moderate	Very High	High	Adversary is highly likely to initiate the threat event
Very High	Moderate	High	High	Adversary is highly likely to initiate the threat event
Very High	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event
Very High	Moderate	Low	Moderate	Adversary is likely to initiate the treat event
Very High	Moderate	Very Low	Moderate	Adversary is likely to initiate the treat event
Very High	Low	Very High	Moderate	Adversary is likely to initiate the treat event
Very High	Low	High	Moderate	Adversary is likely to initiate the treat event
Very High	Low	Moderate	Moderate	Adversary is likely to initiate the treat event
Very High	Low	Low	Low	Adversary is unlikely to initiate the threat event
Very High	Low	Very Low	Low	Adversary is unlikely to initiate the threat event
Very High	Very Low	Very High	Moderate	Adversary is likely to initiate the treat event
Very High	Very Low	High	Moderate	Adversary is likely to initiate the treat event
Very High	Very Low	Moderate	Low	Adversary is unlikely to initiate the threat event

Very High	Very Low	Low	Low	Adversary is unlikely to initiate the threat event
Very High	Very Low	Very Low	Low	Adversary is unlikely to initiate the threat event
High	Very High	Very High	Very High	Adversary is almost certain to initiate the threat event
High	Very High	High	Very High	Adversary is almost certain to initiate the threat event
High	Very High	Moderate	High	Adversary is highly likely to initiate the threat event
High	Very High	Low	Moderate	Adversary is likely to initiate the treat event
High	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
High	High	Very High	High	Adversary is highly likely to initiate the threat event
High	High	High	High	Adversary is highly likely to initiate the threat event
High	High	Moderate	High	Adversary is highly likely to initiate the threat event
High	High	Low	Moderate	Adversary is likely to initiate the treat event
High	High	Very Low	Moderate	Adversary is likely to initiate the treat event
High	Moderate	Very High	High	Adversary is highly likely to initiate the threat event

High	Moderate	High	High	Adversary is highly likely to initiate the threat event
High	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event
High	Moderate	Low	Moderate	Adversary is likely to initiate the treat event
High	Moderate	Very Low	Moderate	Adversary is likely to initiate the treat event
High	Low	Very High	Moderate	Adversary is likely to initiate the treat event
High	Low	High	Moderate	Adversary is likely to initiate the treat event
High	Low	Moderate	Moderate	Adversary is likely to initiate the treat event
High	Low	Low	Low	Adversary is unlikely to initiate the threat event
High	Low	Very Low	Low	Adversary is unlikely to initiate the threat event
High	Very Low	Very High	Low	Adversary is unlikely to initiate the threat event
High	Very Low	High	Moderate	Adversary is likely to initiate the treat event
High	Very Low	Moderate	Moderate	Adversary is likely to initiate the treat event
High	Very Low	Low	Low	Adversary is unlikely to initiate the threat event

High	Very Low	Very Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Very High	Very High	Very High	Adversary is almost certain to initiate the threat event
Moderate	Very High	High	High	Adversary is highly likely to initiate the threat event
Moderate	Very High	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Very High	Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	High	Very High	High	Adversary is highly likely to initiate the threat event
Moderate	High	High	High	Adversary is highly likely to initiate the threat event
Moderate	High	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	High	Low	Moderate	Adversary is likely to initiate the treat event
Moderate	High	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Very High	High	Adversary is highly likely to initiate the threat event
Moderate	Moderate	High	Moderate	Adversary is likely to initiate the treat event

Moderate	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	Very High	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	High	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Low	Very Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Very Low	Very High	Moderate	Adversary is likely to initiate the treat event
Moderate	Very Low	High	Moderate	Adversary is likely to initiate the treat event
Moderate	Very Low	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Very Low	Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Very Low	Very Low	Low	Adversary is unlikely to initiate the threat event

Low	Very High	Very High	Moderate	Adversary is likely to initiate the treat event
Low	Very High	High	Moderate	Adversary is likely to initiate the treat event
Low	Very High	Moderate	Moderate	Adversary is likely to initiate the treat event
Low	Very High	Low	Low	Adversary is unlikely to initiate the threat event
Low	Very High	Very Low	Low	Adversary is unlikely to initiate the threat event
Low	High	Very High	Moderate	Adversary is likely to initiate the treat event
Low	High	High	Moderate	Adversary is likely to initiate the treat event
Low	High	Moderate	Moderate	Adversary is likely to initiate the treat event
Low	High	Low	Low	Adversary is unlikely to initiate the threat event
Low	High	Very Low	Low	Adversary is unlikely to initiate the threat event
Low	Moderate	Very High	Moderate	Adversary is likely to initiate the treat event
Low	Moderate	High	Moderate	Adversary is likely to initiate the treat event
Low	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event

Low	Moderate	Low	Low	Adversary is unlikely to initiate the threat event
Low	Moderate	Very Low	Low	Adversary is unlikely to initiate the threat event
Low	Low	Very High	Low	Adversary is unlikely to initiate the threat event
Low	Low	High	Low	Adversary is unlikely to initiate the threat event
Low	Low	Moderate	Low	Adversary is unlikely to initiate the threat event
Low	Low	Low	Low	Adversary is unlikely to initiate the threat event
Low	Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Very High	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	High	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Moderate	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Low	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very High	Very High	Moderate	Adversary is likely to initiate the treat event

Very Low	Very High	High	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	Moderate	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	Low	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	High	High	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Moderate	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Low	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very Low	Moderate	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	Moderate	High	Low	Adversary is unlikely to initiate the threat event
Very Low	Moderate	Moderate	Low	Adversary is unlikely to initiate the threat event
Very Low	Moderate	Low	Low	Adversary is unlikely to initiate the threat event

Very Low	Moderate	Very Low	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Very High	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	High	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Moderate	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Low	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very Low	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	Very Low	High	Low	Adversary is unlikely to initiate the threat event
Very Low	Very Low	Moderate	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very Low	Low	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event

What We Did:

We evaluated each identified vulnerability's technical exploitability using the CVSS 3.1 framework (see Table 8) and the scales used below Table 8. For every vulnerability (V1–V14), we classified its:

- Attack Vector (AV): where the attacker must be (Network, Local, Physical).

- Attack Complexity (AC): how difficult it is to reliably exploit (Low vs. High).
- Privileges Required (PR): what level of access the attacker needs (None, Low, High).
- User Interaction (UI): whether a user must take an action (None vs. Required).
- Scope (S): whether successful exploitation affects only the vulnerable component or other resources.

We then plugged these metrics into the CVSS 3.1 exploitability formula (via the NVD calculator) to generate a numerical Exploitability Sub-score (0–3.9). Finally, we translated each sub-score into a qualitative category - Very High, High, Moderate, or Low, so that we could combine it with adversary motivation and impact assessments in our overall likelihood analysis.

TABLE 8: AMC - Ease of Exploitability Assessment

Vulnerability ID	Attack Vector (AV)	Attack Complexity (AC)	Privilege Required (P)	User Interaction (UI)	Scope (S)	Exploitability Score (CVSS 3.1)
V1	Network	Low	None	None	Unchanged	Very High [3.9]
V2	Network	Low	None	None	Unchanged	Very High [3.9]
V3	Network	Low	None	None	Unchanged	Very high [3.9]
V4	Network	Low	Low	None	Unchanged	High [2.8]
V5	Network	Low	None	None	Unchanged	Very High [3.9]
V6	Network	High	High	None	Changed	Moderate [1.3]
V7	Physical	Low	None	None	Unchanged	Low [0.9]
V8	Local	Low	Low	None	Unchanged	Moderate [1.8]
V9	Network	Low	None	Required	Unchanged	High [2.8]

V10	Local	Low	High	None	Changed	Moderate [1.5]
V11	Network	High	None	None	Unchanged	High [2.2]
V12	Network	High	None	None	Unchanged	High [2.2]
V13	Physical	Low	None	None	Unchanged	Low [0.9]
V14	Physical	Low	None	None	Unchanged	Low [0.9]

NOTE:

- Details of *Vulnerability ID* are provided in *Table 4*.
- ***Exploitability Score*** Calculator CVSS V3.1 is available at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator. OR use *the spreadsheet model* to calculate this score.
- Exploitability Score ranges between 0 and 3.9.
- ***Qualitative Exploitability Score*** Scale:

  Very High when CVSS 3.1 Exploitability Score range is [3-3.9]

  High when CVSS 3.1 Exploitability Score range is [2-3]

  Moderate when CVSS 3.1 Exploitability Score range is [1-2]

  Low when CVSS 3.1 Exploitability Score range is [<1]

CVSS Exploitability Definitions (Supporting Table 8)

To support interpretation of Table 8, the following CVSS v3.1 metric definitions are provided across five supporting tables:

Table A: Attack Vector (AV)

Value	Definition
Network	A vulnerability exploitable with Network access means the vulnerable component is bound to the network stack and the attacker's path is through OS layer 3 (the network layer). Such a vulnerability is often termed 'remotely exploitable' and can be thought of as an attack being exploitable one or more network hops away (e.g.

	across layer 3 boundaries from routers).
Adjacent Network	A vulnerability exploitable with Adjacent Network access means the vulnerable component is bound to the network stack, however the attack is limited to the same shared physical (e.g. Bluetooth, lEEE 802.11), or logical (e.g. local IP subnet) network, and cannot be performed across an OSI layer 3 boundary (e.g. a router).
Local	A vulnerability exploitable with Local access means that the vulnerable component is not bound to the network stack, and the attacker's path is via read/write/execute capabilities. In some cases, the attacker may be logged in locally in order to exploit the vulnerability, or may rely on User Interaction to execute a malicious file.
Physical	A vulnerability exploitable with Physical access requires the attacker to physically touch or manipulate the vulnerable component, such as attaching a peripheral device to a system.

Table B: Attack Complexity (AC)

Value	Definition
Low	Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success against the vulnerable component.
High	A successful attack depends on conditions beyond the attacker's control. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected.

Table C: Privileges Required (PR)

Value	Definition
None	The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files to carry out an attack.
Low	The attacker is authorized with (i.e. requires) privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. Alternatively, an attacker with Low privileges may have the ability to cause an impact only to non-sensitive resources.
High	The attacker is authorized with (i.e. requires) privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

Table D: User Interaction (UI)

Value	Definition
None	The vulnerable system can be exploited without interaction from any user.
Required	Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited, such as convincing a user to click a link in an email.

Table E: Scope (S)

Value	Definition
Unchanged	An exploited vulnerability can only affect resources managed by the same authority. In this case the vulnerable component and the impacted component are the same.

Changed	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case the vulnerable component and the impacted component are different.

Outcome of this Step:

Ten threat agents were assessed for motivation across different scenarios. Most external adversaries scored very high, especially those associated with ransomware, email-based phishing, or vendor compromise. Insider threats showed more varied scores depending on intent and access. These motivation scores will be combined with exploitability scores in the next step to estimate the overall likelihood of threat initiation.

4.2. ASSESS LIKELIHOOD OF THREAT INITIATION FROM ADVERSARIAL THREAT AGENTS/SOURCES

Objective:

The objective of this step is to determine how likely it is that an identified adversarial threat agent will initiate an attack against AMC's vulnerable IT assets. This assessment helps prioritize threats by combining adversary motivation with technical exploitability, allowing for a realistic evaluation of attack probability.

What We Did:

We calculated the **Likelihood of Threat Initiation** using two key inputs for each adversarial threat:

- **Motivation Score:** Based on the factors capability, intent, and targeting using Table 7A and the look-up matrix in Table 7B.
- **Ease of Exploitability:** Derived from CVSS v3.1 metrics, calculated in Table 8.

We then mapped each combination of motivation and exploitability into a qualitative likelihood score using the reference Look-Up Table 10. This enabled us to estimate how likely each threat agent is to act on their opportunity to exploit the system.

TABLE 9: AMC - Likelihood of Threat Initiation

Asset ID	Vulnerability ID	Threat ID	Motivation Score for Threat Agent/Source	Ease of Exploitability Score	Likelihood of Threat Initiation Score
H	V5	T1	Very High	Very high	Very High
I	V8	T2	Moderate	Moderate	Moderate
I	V7	T3	Low	Low	Very Low
A	V11	T4	Very High	High	Very High
A	V10	T5	Low	Moderate	Low
A	V9	T6	Moderate	High	Moderate
G	V3	T7	Very High	Very High	Very High
H	V5	T8	Moderate	Very High	High
J	V6	T9	Very High	Moderate	High
J	V12	T10	Very High	High	Very High

NOTE:

- Details of *Asset ID* are provided in *Table 3*.
- Details of *Vulnerability ID* are provided in *Table 4*.
- Details of *Threat ID* are provided in *Table 6*.
- Motivation Scores are assessed in *Table 7*.
- Ease of Exploitability Scores are assessed in *Table 8*.
- ***Likelihood of Threat Initiation*** score is estimated using the Look Up *Table 10.*

TABLE 10: AMC - Look-Up table for estimating the Likelihood of Threat Initiation					
Ease of Exploitability	**Motivation of the Threat Agent/Source**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Very Low	Low	Moderate	Moderate

Outcome of this Step:

All ten adversarial threats identified earlier were scored for their likelihood of initiation. The results ranged from **Very Low** to **Very High**, with six threats categorized as **Very High**, indicating an urgent need for remediation. These likelihood scores will be combined with impact assessments in subsequent steps to calculate the overall risk associated with each threat event.

4.3 ASSES THE LIKELIHOOD OF ADVERSE IMPACT

Objective:

The objective of this step is to assess how severely each threat event—if successfully executed—would affect Aggieland Medical Center's (AMC) IT assets, operations, and business processes. This includes evaluating the potential impact on patient care, data confidentiality, regulatory compliance, financial performance, and overall mission continuity.

What We Did:

We reviewed each of the 10 identified threat events and evaluated their potential consequences using qualitative impact criteria outlined in NIST SP 800-30. The assessment considered multiple impact categories including harm to individuals (e.g., PHI exposure), operational disruptions (e.g., halted diagnostics or prescriptions), and reputational or legal consequences (e.g., HIPAA violations or ransomware payments). We referenced prior case documentation, interview transcripts, system role definitions, and Appendix B's non-adversarial threat examples to ensure comprehensive reasoning. Each threat was then assigned an adverse impact score of Very High, High, Moderate, Low, or Very Low based on the magnitude and scope of its potential damage.

TABLE 11: AMC - Assessment of the Likelihood of Adverse Impact from a Threat event				
Asset ID	**Vulnerability ID**	**Threat ID**	**Adverse Impact Score***	**Justification for the Adverse Impact Score**
IT-H	V5	T1	Very High	Unauthorized network intrusion can fully compromise PDIS, halting clinical operations (harm to operations), causing loss of patient data (harm to assets), and triggering regulatory fines for PHI exposure
IT-I	V8	T2	High	Unauthorized disclosure of patient records leads to PHI leakage (harm to individuals), reputational damage, and HIPAA non-compliance penalties
IT-I	V7	T3	Moderate	A patient's one-off access to another's record poses limited, localized confidentiality harm (harm to individuals) and is unlikely to disrupt broader operations
IT-A	V11	T4	Very High	Extended DoS of PDIS (no DR/BC) will stop admissions, diagnostics, and prescribing (harm to operations), with no quick recovery and major patient-safety implications
IT-A	V10	T5	Moderate	Accidental data corruption can mislead clinicians (harm to individuals) and require

				time-consuming data restoration, but is generally recoverable
IT-A	V9	T6	Moderate	Social-engineering attempts risking PHI exfiltration (harm to individuals) are likely to cause targeted data loss but not broad system outages
IT-G	V3	T7	Very High	Ransomware/phishing on the email server can encrypt critical communications and PHI (harm to operations & assets), forcing payment to restore access
IT-H	V5	T8	High	Malware spread via a misconfigured firewall can disrupt multiple systems (harm to operations), propagate loss of integrity, and require network-wide remediation
IT-J	V6	T9	Very High	A supply-chain breach through ABC Systems' console can grant attackers deep access to all critical servers (harm to operations & assets) and exfiltrate large volumes of PHI
IT-J	V12	T10	High	Exploitation of unremediated CVEs can lead to targeted system compromise (harm to operations & assets) but may be contained if detected before widespread propagation

NOTE:

- Details of *Asset ID* are provided in *Table 3*.
- Details of *Vulnerability ID* are provided in *Table 4*.
- Details of *Threat ID* are provided in *Table 6*.
- ***Adverse Impact *Score*** Scale:

  Very High=> If the threat event is initiated or occurs, it is almost certain to have adverse impacts.

  High=> If the threat event is initiated or occurs, it is highly likely to have adverse impacts.

  Moderate=> If the threat event is initiated or occurs, it is likely to have adverse impacts.

  Low=> If the threat event is initiated or occurs, it is unlikely to have adverse impacts.

  Very Low=> If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

Outcome of this Step:

As a result, we were able to assign Adverse Impact Scores to all 10 threats, with 4 rated as Very High, 3 as High, and 3 as Moderate. These scores provide critical input for the final risk estimation phase, helping AMC prioritize threats not only by their likelihood of initiation, but also by the severity of their impact. This step ensures that risk mitigation efforts focus on both probable and high-consequence events.

4.4 ASSESSMENT SCALE – OVERALL LIKELIHOOD

Objective:

The objective of this step is to determine the Overall Likelihood of each threat event materializing by combining the probability of its initiation and the severity of its potential adverse impact. This combined likelihood serves as a key input for final risk evaluation and prioritization.

What We Did:

For each of the ten threat scenarios, we referenced:

- **Table 9** to obtain the **Likelihood of Threat Initiation or Occurrence** based on adversary motivation and system exploitability.
- **Table 11** to retrieve the **Likelihood of Adverse Impact** resulting from a successful threat event.

Using the qualitative lookup matrix in Table 13, we combined these two scores to generate the Overall Likelihood of Threat Event, assigning one of the following values: Very High, High, Moderate, or Low. This scoring reflects both the technical feasibility and the projected business/clinical consequence of each threat event.

TABLE 12: AMC - Overall Likelihood of a Threat Event

Asset ID	Vulnerability ID	Threat ID	Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts	Overall Likelihood of Threat Event
IT-H	V5	T1	Very High	Very High	Very High
IT-I	V8	T2	Moderate	High	Moderate
IT-I	V7	T3	Very Low	Moderate	Low
IT-A	V11	T4	Very High	Very High	Very High
IT-A	V10	T5	Low	Moderate	Low
IT-A	V9	T6	Moderate	Moderate	Moderate
IT-G	V3	T7	Very High	Very High	Very High
IT-H	V5	T8	High	High	High
IT-J	V6	T9	High	Very High	Very High
IT-J	V12	T10	Very High	High	Very High

NOTE:

- Details of *Asset ID* are provided in *Table 3*.
- Details of *Vulnerability ID* are provided in *Table 4*.
- Details of *Threat ID* are provided in *Table 6*.
- Likelihood of Threat Event Initiation or Occurrence is assessed in *Table 9*.
- Likelihood Threat Events Result in Adverse Impacts is assessed in *Table 11*.
- Overall Likelihood of Threat Event is estimated using the Look-Up *Table 13.*

TABLE 13: AMC - Look-Up table for estimating the Overall Likelihood of a Threat Event

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

NOTE: Explanation of the qualitative measures for the ***Overall Likelihood of Threat*** event happening.

- **Very High** => Threat will happen
- **High** => Threat event will most likely happen
- **Moderate** => Threat is likely to happen
- **Low** => Threat may happen
- **Very Low** => Threat event is unlikely to happen

Outcome of this Step:

All ten threat events were rated using the composite scoring method. The outcome shows that six events are of very high likelihood, two are high, two are moderate, and one is low. This step ensures that AMC's cybersecurity strategy focuses on the most pressing and probable threat scenarios, setting the stage for quantifying risk and proposing mitigation in the next steps.

5. ESTIMATE IMPACT ON IT ASSETS, BUSINESS PROCESSES, AND ORGANIZATION

TABLE 14: AMC - Measurement Scales for Impact After a Threat Event Happens
Assessment Scale for Impact on Confidentiality of the Targeted IT Asset
• High [10]- Confidentiality of the targeted IT asset is fully compromised after the threat event • Medium [5]- Confidentiality is partially compromised after the threat event • Low [1]- Confidentiality is not compromised after the threat event
Assessment Scale for Impact on Integrity of the Targeted IT Asset
• High [10]- Integrity of the targeted IT asset is fully compromised after the threat event • Medium [5]- Integrity of the targeted IT asset is partially compromised after the threat event • Low [1]- Integrity of the targeted IT asset is not compromised after the threat event
Assessment Scale for Impact on Availability of the Targeted IT Asset
• High [10]- Availability of the targeted IT asset is fully compromised after the threat event • Medium [5]- Availability of the targeted IT asset is partially compromised after the threat event • Low [1]- Availability of the targeted IT asset is not compromised after the threat event
Assessment Scale for Impact on Business Process
• **Very High [10]**- Asset failure will result in a total disruption of the business process for at least 2 hours • **High[7]**- Asset failure will result in slowing down of the business process • **Moderate [4]**- Asset failure will have minimal impact on the business process • **Low [2]**- Asset failure will have no impact on the business process • **Very Low [0]**- Almost no impact on the business process
Assessment Scale for Financial Impact on Aggieland Medical Center

- **High [10]** => Threat event will result in the cost of detection & escalation, incident notification, incident response, and lost business exceeding $1 million
- **Medium [5]** => Threat event will the cost of detection & escalation, incident notification, incident response, and lost business exceeding $0.5 million but less than $1 million
- **Low [1]** => Threat event will the cost of detection & escalation, incident notification, incident response, and lost business exceeding of less than $0.5 million

Assessment Scale for Legal impact on Aggieland Medical Center

- **High [10]** => Asset failure will result in legal action that could lead to imprisonment, fines exceeding $1 million
- **Medium [5]** => Asset failure will result in legal action for correction and fines between $0.5 - $1 million
- **None [0]** => Asset failure will result in no legal action

TABLE 15: AMC - Estimate the Final Impact Value (FIV) due to a Threat Event

Asset ID	Vulnerability ID	Threat ID	Impact											Final Impact Value (FIV) Semi-Qualitative Value	Final Impact Value (FIV) Qualitative Value*
			IT Asset			Business Process						Organization			
			C	I	A	BP1	BP2	BP4	BP8	BP9	BP10	Financial	Legal		
IT-H	V5	T1	10	10	10	10	10	0	0	0	0	10	10	70	Very High
IT-I	V8	T2	10	1	1	0	0	0	0	0	0	5	5	22	Moderate
IT-I	V7	T3	5	1	1	0	0	0	0	0	0	1	0	8	Very Low
IT-A	V11	T4	1	1	10	10	10	0	0	0	0	10	10	52	High

IT-A	V10	T5	1	5	1	4	0	4	0	0	0	1	0	15	Low
IT-A	V9	T6	5	1	1	0	0	0	0	0	0	1	0	8	Very Low
IT-G	V3	T7	10	10	10	7	0	0	7	0	0	10	10	64	Very High
IT-H	V5	T8	10	10	10	10	10	0	0	0	0	10	10	70	Very High
IT-J	V6	T9	10	10	10	10	0	0	0	10	0	10	10	70	Very High
IT-J	V12	T10	10	10	5	7	0	0	0	4	0	5	5	46	High

NOTES:

- **C** => Confidentiality of the IT Asset
- **I** => Integrity of the IT Asset
- **A** => Availability of the IT Asset
- **Business Process (BP)**- Specify here the business process that is impacted. This information will be from *TABLE 1* [in *STEP 1*]. If more than one business process is impacted by a vulnerability-threat pair, then for each business process, add a column to the table. In this table we are assuming two business processes only, i.e., BP1 and BP2.
- **Financial** impact includes the sum of Detection and Escalation, Notification of Cyber-attack to Relevant Stakeholders, Incident Response, and Lost Business costs.
- **Legal** impact could include fines, jail time, and reimbursing individuals and organizations affected by the threat. The relevant state and federal cybersecurity laws should be specified when defining the assessment scale for legal impact.
- **Final Impact Value (FIV)** is a function of the impact on IT assets, operational, financial, and legal impact values. This could be as simple as a sum of the semi-qualitative values for these variables, or some other mathematical function.
- ***** ***FIV Qualitative Score*** Scale:

  Very High=> When 60 < FIV Semi-Qualitative Value ≤ 70

  High=> When 40 < FIV Semi-Qualitative Value ≤ 60

  Moderate=> When 20 < FIV Semi-Qualitative Value ≤ 40

Low=> When 10 < FIV Semi-Qualitative Value ≤ 20

Very Low=> When FIV Semi-Qualitative Value ≤ 10

6. ESTIMATE THE CYBERSECURITY RISK

Objective:

To combine each threat's overall likelihood (from STEP 4, Table 12) with its Final Impact Value (FIV) (from STEP 5, Table 15) into a single, qualitative Risk Level. This provides a clear, at-a-glance view of which threat/vulnerability pairs pose the greatest danger to AMC's operations, assets, and reputation, in line with NIST SP 800-39's tiered risk-management framework.

What We Did:

In this step, we take each threat's overall likelihood (from Step 4, Table 12) and its Final Impact Value (FIV) (from Step 5, Table 15) and cross-reference them against the Risk Matrix in Table 16 to derive a single, qualitative Risk Level for each threat/vulnerability pairing. For every identified threat event, we extract its assessed likelihood category and its FIV category, then look up the corresponding risk rating, ranging from Very Low to Very High, in the matrix. These results are recorded in Table 17 alongside the asset, vulnerability, and threat identifiers, yielding a concise, prioritized dossier of cybersecurity risks. This consolidated risk register highlights those threat events that pose immediate, severe dangers ("High" and "Very High" risks), guiding AMC's leadership to focus remediation efforts where they will have the greatest impact, while also informing medium- and long-term mitigation planning for lower-rated risks.

TABLE 16: AMC - RISK MATRIX for Looking up the Level of Risk

Likelihood that Threat Event Occurs and Results in Adverse Impact	FINAL IMPACT VALUE (FIV)				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Moderate	High	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High

Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

NOTE: Explanation of the **qualitative measures for levels of risk**.

- **Very High** => Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- **High** => High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- **Moderate** => Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- **Low** => Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- **Very Low** => Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

TABLE 17: AMC - Cybersecurity Risk to IT Assets

Asset ID	Vulnerability ID	Threat ID	Threat Event Likelihood	Final Impact Value (FIV)	Risk Level
IT-H	V5	T1	Very High	Very High	Very High
IT-I	V8	T2	Moderate	Moderate	Moderate
IT-I	V7	T3	Low	Very Low	Very Low
IT-A	V11	T4	Very High	High	High

IT-A	V10	T5	Low	Low	Low
IT-A	V9	T6	Moderate	Very Low	Very Low
IT-G	V3	T7	Very High	Very High	Very High
IT-H	V5	T8	High	Very High	Very High
IT-J	V6	T9	Very High	Very High	Very High
IT-J	V12	T10	Very High	High	Very High

Outcome of this Step:

The outcome of Step 6 is a consolidated **Cybersecurity Risk Register** (Table 17) that maps each threat event to its overall likelihood, its Final Impact Value (FIV), and the resulting qualitative **Risk Level**, using the AMC Risk Matrix (Table 16). In practice, this produces at-a-glance visibility into which vulnerability–threat pairs pose the greatest danger and should be remediated first.

Concretely, for Aggieland Medical Center:

- **Very High Risk** (4 events):
  - T1 (Unauthorized network intrusion)
  - T7 (Ransomware via email)
  - T8 (Malware propagation via firewall)
  - T9 (Supply-chain compromise)
- **High Risk** (2 events):
  - T4 (Extended DoS of PDIS)
  - T10 (Exploitation of unremediated CVEs)
- **Moderate Risk** (1 event):
  - T2 (Insider disclosure of patient records)

- **Low Risk** (1 event):
    - T5 (Accidental data corruption)

- **Very Low Risk** (2 events):
    - T3 (Unauthorized workstation access)
    - T6 (Social-engineering for PHI)

Linking the assets, vulnerabilities, threats, likelihood, impact, and risk levels enable AMC's leadership to focus immediate mitigation on the "Very High" risks, plan "High" and "Moderate" controls next, and monitor the lower-rated threats over time.

FINAL NOTE

Aggieland Medical Center's risk assessment identified four "Very High" risk scenarios that demand immediate, multi-layered mitigation:

1. Network Intrusion (T1) and Malware Propagation (T8):

In its current configuration, the Cisco ASA firewall permits broad "any to any" traffic rules, allowing unrestricted communication between all systems, regardless of source, destination, or protocol. While often used as a temporary default, these rules significantly weaken network security by eliminating segmentation boundaries. In effect, if a single device is compromised, an attacker can move laterally across the network without encountering policy-based restrictions. This undermines the principle of least privilege and exposes high-value systems such as PDIS and ECDS to unnecessary risk. To reduce the attack surface, AMC must replace these open rules with tightly scoped access controls that permit only essential communication between known, trusted systems.

2. Email-borne Ransomware (T7):

The legacy Sendmail 8.9.3 service on Red Hat Enterprise Linux 6 (V3) remains a known attack vector for ransomware that targets protected health information. AMC should expedite migration to a supported operating system such as RHEL 8 or Windows Server 2019 and replace Sendmail with a modern, fully patched mail transfer agent. All inbound email should be filtered through an advanced security gateway with sandboxing for links and attachments, along with enforcement of DMARC, DKIM, and SPF policies. Endpoint protection with rollback capabilities must be deployed on both mail servers and clinical workstations. Daily monitoring of mail queues by the security team will help detect abnormal patterns early. Regular phishing simulations, followed by targeted training, will further strengthen staff awareness.

3. Supply-Chain Compromise (T9):

Unrestricted vendor access through the ABC Systems remote management console (V6) poses a critical risk to all core systems. To reduce exposure, AMC should place vendor consoles on a dedicated management VLAN that does not route into clinical or financial networks. All vendor access must require hardware token multi-factor authentication and certificate-based VPN connections. Service Level Agreements should be updated to include quarterly security assessments, penetration testing, and immediate breach notification. Access privileges should be limited strictly to the systems the vendor is responsible for, with all activity logged, sent to a centralized monitoring system, and reviewed weekly by AMC IT leadership.

Two “High”-risk scenarios require robust process and resilience improvements:

4. Extended DoS of PDIS (T4):

Without a business continuity and disaster recovery plan (V11), a successful attack could halt patient admissions, diagnostics, and prescribing for an extended period. AMC should implement an active-passive PDIS cluster across two geographically separate data centers, with clear recovery time and recovery point objectives. A cloud-based service should be used to filter distributed denial of service traffic targeting external systems. The continuity plan must be formally documented, tested through staff-led tabletop and failover exercises at least twice a year, and updated based on lessons learned from each drill.

5. Exploitation of Unremediated CVEs (T10):

The lack of a structured vulnerability remediation process (V12) leaves all systems exposed to known threats. AMC should adopt a centralized vulnerability management platform that integrates with automated patching tools such as SCCM or Ansible. High-severity vulnerabilities with CVSS scores of 7 or above must be patched within 72 hours, while those rated between 4 and 6 should be addressed within 30 days. A remediation board that includes IT, security, and clinical stakeholders should meet monthly to review open issues, assign actions, and confirm resolution.

A “Moderate” risk insider threat and two “Low” or “Very Low” risk issues can be addressed through targeted access and training enhancements:

6. Insider Disclosure of PHI (T2):

Shared passwords and missing session time-outs (V8) facilitate unauthorized record access. Implementing enterprise SSO (Azure AD/Okta) will eliminate shared credentials; group-policy must enforce auto-lock after five minutes of inactivity. Role-based access controls in PDIS should ensure that users can only view the patient data necessary for their job. A DLP solution, configured to monitor PHI egress, will generate alerts for unusual data transfers.

7. Accidental Data Corruption (T5):

Over-privileged administrators (V10) have already mishandled patient records. PDIS provisioning must move to a stricter RBAC model, with dual-approval required for schema changes and permission grants. All changes should be logged and subject to daily supervisory review. Immutable backups with rapid restore procedures will minimize downtime if corruption occurs.

8. Unauthorized Workstation Access (T3 and T6):

Weak session management (V7) and limited security training (V9) present low operational risk but should still be addressed. Group policies should enforce a two-minute screen lock on all clinical workstations. Introducing smart card or biometric login will further discourage users from leaving sessions unattended. Annual, scenario-based security training that includes social engineering simulations should reinforce the importance of verifying all requests before releasing protected health information.

Governance, Monitoring & Continuous Improvement:

All controls should be overseen by a quarterly cybersecurity steering committee that monitors key performance indicators such as patch completion rates, detection and response times, and phishing susceptibility, adjusting budget priorities as needed. A formal vendor risk management program, including annual audits and joint tabletop exercises, will strengthen third-party resilience. AMC must also invest in around-the-clock security operations center monitoring, supported by a capable SIEM, to ensure that deviations from secure configurations trigger immediate and coordinated action.

By combining stronger network defenses, endpoint protection, access governance, operational discipline, and executive oversight, AMC can reduce its most critical threats to manageable levels and lay the groundwork for long-term cybersecurity maturity.

APPENDICES

APPENDIX A:

Capability, Intent, and Targeting Scales for Aggieland Medical Center (AMC)

1. Capability Scale

Qualitative Value	Interpretation
Very High	Nation-state actors or highly organized cybercriminal groups with expertise in healthcare systems and EMR/EHR platforms. Often exploit zero-days and advanced persistent threats.
High	Skilled external attackers (e.g., ransomware groups) or well-trained insiders with admin-level access and knowledge of medical IT infrastructure.
Moderate	IT-aware insiders or external attackers using known vulnerabilities and openly available tools (e.g., script kiddies using Metasploit or phishing kits).
Low	General staff or users with limited tech skills who might misuse access accidentally or out of curiosity.
Very Low	Individuals with minimal/no technical expertise (e.g., physical intruders, untrained staff, or patients/visitors).

2. Intent Scale

Qualitative Value	Interpretation
Very High	Threat actor's objective is full-scale disruption (e.g., ransomware that shuts down operations or leaks patient records for blackmail or damage).
High	Objective is to maintain access to sensitive data (e.g., credentials, billing records) for ongoing fraud or surveillance.

Moderate	Actor wants to access or modify specific patient data or billing records, possibly for personal gain or revenge.
Low	Access motivated by curiosity or minor benefits, like checking unauthorized patient info or misusing HR data.
Very Low	Accidental or incidental access without harmful intent (e.g., unaware clinical staff, patients stumbling onto unlocked screens).

3. Targeting Scale

Qualitative Value	Interpretation
Very High	Actor persistently targets AMC specifically for strategic value (e.g., it holds unique demographic/medical data or is part of a broader attack on regional hospitals).
High	Actors specifically seek out healthcare institutions like AMC for ransomware, PII, or financial fraud.
Moderate	Actor targets the healthcare sector broadly, but AMC is not a specific target. Any exposure is incidental.
Low	Opportunistic targeting of open or poorly secured systems; no preference for healthcare or AMC.
Very Low	No deliberate targeting; any impact is purely random or due to physical proximity.

APPENDIX B:

EXAMPLES OF ADVERSE IMPACTS [Source: NIST Special Publication 800-30 Revision 1]

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions. - In a sufficiently timely manner. - With sufficient confidence and/or correctness. - Within planned resource constraints. - Inability, or limited ability, to perform missions/business functions in the future. - Inability to restore missions/business functions. - In a sufficiently timely manner. - With sufficient confidence and/or correctness. - Within planned resource constraints. - Harms (e.g., financial costs, sanctions) due to noncompliance. - With applicable laws or regulations. - With contractual requirements or other requirements in other binding agreements (e.g., liability). - Direct financial costs. - Relational harms. - Damage to trust relationships. - Damage to image or reputation (and hence future or potential trust relationships).
HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft.

	- Loss of Personally Identifiable Information. - Damage to image or reputation.
HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance. - With applicable laws or regulations. - With contractual requirements or other requirements in other binding agreements. - Direct financial costs. - Relational harms. - Damage to trust relationships. - Damage to reputation (and hence future or potential trust relationships).

REFERENCES

1. S. Alder, "$185,000 Settlement Proposed to Resolve Grays Harbor Community Hospital Ransomware Lawsuit," *HIPAA Journal*, Jul. 2, 2020. [Online]. Available: https://www.hipaajournal.com/185000-settlement-proposed-to-resolve-grays-harbor-community-hospital-ransomware-lawsuit/. [Accessed: Apr. 13, 2025].
2. U.S. Department of Health and Human Services, "Distributed Attacks and the Healthcare Industry," [Online]. Available: https://www.hhs.gov/sites/default/files/hph-distributed-attack-vectors-tlp-white.pdf. [Accessed: Apr. 15, 2025].
3. R. Lakshmanan, "CISA Warning: Akira Ransomware Exploiting Cisco ASA/FTD Vulnerability," *The Hacker News*, Feb. 16, 2024. [Online]. Available: https://thehackernews.com/2024/02/cisa-warning-akira-ransomware.html. [Accessed: Apr. 17, 2025].
4. National Institute of Standards and Technology, "CVSS v3 Calculator," [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator. [Accessed: Apr. 11, 2025].
5. National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Revision 1, Sep. 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. [Accessed: Apr. 20, 2025].