- Query successful

Here's an analysis of the provided documents to address the risk management requirements:

1. Identification of Risks from Vulnerability Scan Results

The "vulnerability assessment.pdf" document contains the results of a vulnerability scan. It shows various vulnerabilities detected on a system. To identify risks, we need to consider the Common Vulnerability Scoring System (CVSS) scores provided, which indicate the severity of each vulnerability.

Critical Risk 1

- **Vulnerability:** CVE-2017-14493, CVE-2017-14492, CVE-2017-14491

- **CVSS Score:** 9.8

- **Explanation:** These vulnerabilities have a critical CVSS score, indicating a high likelihood of exploitation and significant impact. An attacker could exploit these vulnerabilities to gain full control of the affected system, potentially leading to data breaches, system downtime, and other severe consequences.

- **Treatment Recommendation: Mitigate.** These vulnerabilities should be addressed immediately due to their severity.
- **Basic Mitigation Steps:**
    1. **Patching:** Apply the necessary security patches provided by the vendor to eliminate the vulnerabilities.
    2. **System Isolation:** Isolate the affected system from the network until it can be patched to prevent lateral movement by attackers.
    3. **Intrusion Detection:** Implement or enhance intrusion detection systems (IDS) to monitor for and block any exploitation attempts.

Critical Risk 2

- **Vulnerability:** Multiple "EXPLOIT" entries with high CVSS scores (e.g., 9.8)

- **Explanation:** The presence of known exploits with high CVSS scores means that attackers have readily available tools to take advantage of these weaknesses. This significantly increases the risk of successful attacks.

- **Treatment Recommendation: Mitigate.** Similar to the first critical risk, immediate action is required.
- **Basic Mitigation Steps:**
  1. **Exploit Prevention:** Implement exploit prevention techniques, such as memory protection and intrusion prevention systems (IPS), to block exploit attempts.
  2. **Vulnerability Scanning:** Conduct regular vulnerability scans to identify and address new vulnerabilities promptly.
  3. **Security Awareness Training:** Educate users about the risks of phishing and social engineering attacks, which can be used to deliver exploits.

2. Risk Monitoring Procedure

Here's a basic risk monitoring procedure to track the identified risks:

- **Risk ID:** Assign a unique identifier to each risk (e.g., CR-001 for Critical Risk 1, CR-002 for Critical Risk 2).
- **Vulnerability:** Record the specific vulnerability (e.g., CVE-2017-14493).
- **CVSS Score:** Note the CVSS score to quantify the risk's severity.
- **Status:** Track the current status of the risk (e.g., Open, In Progress, Mitigated, Accepted).
- **Mitigation Plan:** Document the planned or implemented mitigation steps.
- **Owner:** Assign responsibility for monitoring and mitigating the risk to a specific individual or team.
- **Monitoring Frequency:** Define how often the risk will be reviewed (e.g., daily, weekly, monthly).
- **Next Review Date:** Schedule the next date for risk review.
- **Notes:** Record any relevant information, such as changes in status, new developments, or challenges encountered.

Example Risk Monitoring Table

Risk	**Vulnerability(ies)**	**CVSS**	**Status**	**Mitigation Plan**	**Owner**	**Monitoring Frequ**	**Next Rev**	**Notes**
CR-0	CVE-2017-14493, CVE-2017-1449	9.8	In Progres	1. Patch systems. 2. Isolate affected systems. 3. Enhance	Security Team	Daily	2024-04-2	Vendor patches are being tested; temporary
CR-0	Multiple EXPLOIT entries	High	In Progres	1. Implement exploit prevention. 2. Regular vulnerability scans. 3.	Infrastructure	Weekly	2024-04-3	IPS deployed; vulnerability scan scheduled for next

Export to Sheets

Justification for Decisions

- **Risk Prioritization:** Critical risks are prioritized for immediate attention due to their potential for severe impact on the organization.
- **Mitigation Focus:** The treatment recommendation for critical risks is "Mitigate" to reduce the likelihood and impact of these risks to an acceptable level.
- **Monitoring Frequency:** Critical risks are monitored more frequently (daily or weekly) to ensure that mitigation efforts are effective and that the risk status is up-to-date.
- **Risk Monitoring Table:** The risk monitoring table provides a structured way to track risks, assign responsibilities, and ensure that mitigation efforts are progressing as planned. This promotes accountability and facilitates effective risk management.