Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Endpoint Protection Software: Deploy robust antivirus and anti-malware solutions for real-time scanning and defense against evolving threats, ensuring adherence to security policies on all devices. **Least Privilege Access:** Enforce the principle of least privilege to limit user access rights, minimizing the risk of unauthorized access and data manipulation. Regularly review and update user permissions. **Regular Patch Management:** Prioritize regular patch management to promptly address software vulnerabilities. Utilize automated tools to ensure systems are up-to-date with the latest security patches, enhancing overall system resilience.

Part 2: Explain your recommendations
Endpoint Protection Software: Implementing robust endpoint protection software is crucial for defending against a wide range of cyber threats. These tools provide real-time scanning and protection against malware, viruses, and other malicious activities. By ensuring that all devices adhere to security policies through endpoint protection, the organization establishes a strong defense mechanism against potential security breaches. Regular updates and continuous monitoring enhance the software's effectiveness in detecting and mitigating evolving threats. **Least Privilege Access:** Enforcing the principle of least privilege is a fundamental security practice that limits user access rights to the minimum necessary for their roles and responsibilities. By minimizing user permissions, organizations reduce the attack surface and potential impact of a security breach. Regularly reviewing

and updating user access privileges helps align permissions with current job requirements, preventing unnecessary access and enhancing overall system security.

Regular Patch Management:
Regular patch management is crucial to addressing vulnerabilities in software and operating systems. Automated patch management tools streamline the process of applying the latest security updates, reducing the window of exposure to known vulnerabilities. By promptly addressing these vulnerabilities, organizations significantly enhance the security of their IT infrastructure, mitigating the risk of exploitation by malicious actors and maintaining a resilient defense against cyber threats.