## Risk Assessment and Mitigation Plan

We have carried out a comprehensive assessment of cybersecurity risks in accordance with the recommendations in NIST Special Publication 800-30 Revision 1. We started by outlining the assets at risk, defining the risk assessment process, and determining the boundaries of the system. In the assessment phase, we looked at vulnerabilities including unpatched software and misconfigurations and detected possible dangers like insider threats and cyberattacks. To ascertain the total risk levels, we next examined the likelihood and impact of various threats and vulnerabilities.

To further strengthen our approach, we applied the Threat-Vulnerability-Asset (TVA) model to systematically manage risks. We identified assets, potential threats, vulnerabilities within our systems, and focused on protecting assets such as hardware, software, and data. For example, we addressed the threat of malware attacks by patching vulnerabilities in critical systems and safeguarding assets like our GenAI application that processes customer data.

By understanding the relationships between threats, vulnerabilities, and assets, we have prioritized our security efforts, addressed the most critical vulnerabilities and protected our valuable assets from potential threats. This systematic approach has enabled us to develop robust risk management and mitigation strategies.