Risk Treatment Plan for SSAS Inc.

Introduction: SSAS Inc. is a company with a high cybersecurity risk appetite, meaning they are willing to accept more risks compared to typical organizations in exchange for business gains or innovation. This plan outlines how SSAS Inc. can address potential cyber threats while balancing risks against their business strategy.

Identifying Threats

Based on their operations, SSAS Inc. faces several cybersecurity threats:

- Data breaches due to unauthorized access or vulnerabilities in the platform.
- Phishing or social engineering attacks targeting employees.
- Cloud infrastructure vulnerabilities, which could expose customer or internal data.
- Insider threats, where employees misuse their access to sensitive information.
- Malware or ransomware attacks that could disrupt operations and affect business continuity.

Threats and Preventions

Since SSAS Inc. has a very high risk appetite, they may choose to accept certain risks, especially those that would otherwise stifle innovation. However, they still need to mitigate critical risks that could cause major harm to the business.

Threat	Risk Level	Details
Data Breaches (Unauthorized Access)	High	Use advanced encryption (AES, RSA), multi-factor authentication (MFA), and regular security updates to reduce the risk of unauthorized access.
Phishing Attacks	Moderate	Given their high-risk appetite, SSAS may accept some risk but should continue regular cybersecurity training to reduce the chances of phishing success.
Cloud Vulnerabilities	High	Ensure strong access controls, regular security

		patches, and constant monitoring of cloud systems to minimize vulnerabilities.
Insider Threats (Employee Misuse)	Moderate	Accept some level of risk while implementing monitoring tools to track user activities. Regular audits can reduce the risk of misuse.
Malware/Ransomware	High	Use robust endpoint security, regular backups, and software updates. Implement intrusion detection systems to detect and respond quickly.

Prioritizing Security Measures

For SSAS Inc., high-risk threats like data breaches, cloud vulnerabilities, and malware attacks should be the top priority for mitigation. These could have significant negative impacts on the business and customer trust if not properly addressed. For moderate-risk threats like phishing and insider misuse, the company can accept some level of risk due to their high-risk tolerance, but measures should still be in place to reduce these risks where possible.

Conclusion

SSAS Inc. prioritizes addressing high-risk issues such as data breaches and cloud vulnerabilities through security measures like encryption and strong access controls. At the same time, they are comfortable accepting some risk, particularly in areas like phishing or insider threats, to remain agile and innovative in their SaaS offerings. This risk treatment plan aligns with their high-risk appetite while ensuring that critical security concerns are still managed.