


RYMARK'S Security Audit Guide

SAFEGUARD YOUR ORGANIZATION FROM CYBER THREATS


PROTECTION

☐ **Security Assessment** 

It's crucial to establish a baseline & address existing vulnerabilities. An assessment scans your environment to identify network, local & cloud application vulnerabilities to mitigate future risks. When was your last assessment?

☐ **Patching & Critical Update Management** 


Critical Patch, update installation and management to protect your IT Assets and network(s) from the latest threats and security vulnerabilities.

☐ **Network Security** 

Enforce & proactively manage Intrusion Prevention, Gateway Antivirus, DNS Protection, Web Blocker, spam blocker, Geofence VPN, Secure WIFI & application control to provide greater security for your internal network.

☐ Firewall/Model: _____


☐ DNS Protection

☐ **Email Security** 

Advanced spam filtering & phishing protection includes: anti-spam, anti-virus, ransomware defense, zero-day virus protection, spear-phishing, CEO fraud protection, & dedicated IP recovery from blacklisting.

☐ Email filtering ☐ Email Encryption


☐ DMARC/DKIM policy

☐ **Password & MFA Management** 


Restricted accounts and privileges. Password policy documentation and policy enforcement.

☐ M365/Google MFA ☐ Local MFA

☐ Password Manager

☐ **IT Asset Management** 

System and software auditing. Inventory and tracking, Asset lifecycle management, cost optimization, increased compliance and security.

☐ **Data Backup** 

Backup management to protect your mission-critical data and minimize downtime in the event of a failure or cyber-attack.


☐ Local backup ☐ Cloud backup

☐ M365/Google Cloud backup

☐ **Privileged Access Management** 

RYMARK's PrivilegeShield helps organizations enhance security and compliance by enforcing the Principle of Least Privilege and providing detailed control over user privileges.


DETECTION

☐ **Managed Endpoint Detection & Response** 

Proactive Threat Detection: Detect and stop exploits and attacks nearly in real-time. Includes 24/7/365 SOC, monitoring, and remediation to prevent threat spread; predicts malicious behavior, quickly eliminates threats, and adapts defenses.

☐ **Dark Web Monitoring** 

Knowing in real time whether passwords & accounts have been posted for sale on the Dark Web allows you to be proactive in preventing a data breach. We scan the Dark Web & take action to protect your organization from stolen credentials.

☐ **Antivirus** 


Next-Gen, real-time protection scans for & blocks viruses, malware & ransomware using advanced technologies like machine learning & anomaly detection. Static signature-based AV solutions are outdated; modern malware needs modern solutions.

☐ **Cloud Platform Security** 

Reporting, enhanced security and alert notification for Microsoft 365 and Google Workplace environments.

☐ **Identity Threat Detection & Response**

Managed ITDR offers 24/7 identity monitoring & threat response. Analyzing user activities, Entra ID & Google Workspace logs to detect unusual activity including session hijacking, privilege escalation, credential theft, location anomalies, & malicious inbox rules.


☐ **SIEM/Log Management** 

A 24/7/365 Security Operations Center (SOC) analyzes security alerts from apps, endpoints, and network hardware to meet compliance needs, reduce complexity, capture essential data, and detect hidden hackers.


RESPONSE

☐ **Help Desk Support** 


Our local IT help desk provides technical support & assistance to users of computer systems, software, hardware, and network devices. Help desk staff troubleshoot, diagnose & resolve various IT issues & train users to use & maintain their IT equipment & applications.

☐ **24/7/365 SOC** 

Our Security Operation Center (SOC) is a facility with security engineers that monitor & respond to cyberattacks 24/7/365. Our SOC uses Artificial Intelligence, tools, processes, & people to identify and mitigate potential threats as quickly as possible.

☐ **Disaster Recovery** 


A valuable investment for any organization that relies on IT systems & data for its daily operations, IT DR is the process of restoring critical IT systems & data after a major disruption, such as a natural disaster, cyberattack or human error.

☐ **Incident Response & Policy Procedures** 

Documented company information security policies and response plans give employees guidelines to not only protect the organization from a cyber-attack, but also provide clear direction in the event of a cybersecurity incident.

☐ **Cloud Platform Monitoring**

Implement baseline security practices: Set up and enforce policies for email, file sharing, and access. Manage conditional access policies, external email forwarding, safe attachments, and audit logs. Conduct security audits, reports & drift monitoring with live support.

☐ **Cyber Insurance** 

Cyber insurance can't protect your organization from cybercrime, but it can keep your organization on stable financial footing should a significant security event occur.