ASA Cybersecurity Checklist

American Supply Association | Cybersecurity Task Group

Minimal Maturity (Essential Controls)

☐ Multi-Factor Authentication (MFA) enabled for all critical systems

☐ Regular patching for servers, endpoints, and applications

☐ Antivirus/Endpoint Detection & Response (EDR)

☐ Daily backups with periodic test restores

☐ Basic phishing awareness training

☐ Strong password standards

☐ Web filtering enabled

☐ Inventory of devices and applications

☐ Documented incident response plan

☐ At least one tabletop exercise per year

☐ Data Loss Prevention (DLP)

Average Maturity (Structured Program)

☐ Automated patching program

☐ Centralized logging for critical systems

☐ Monthly phishing simulations

☐ Basic network segmentation

☐ Vendor risk assessment process

☐ Privileged access management (PAM)

☐ Documented backup testing schedule

☐ Role-based recovery playbooks

☐ Basic SIEM or log-monitoring capability

Advanced Maturity (High Resilience)

☐ Managed Detection & Response (MDR) or internal SOC

☐ Continuous vulnerability scanning and reporting

☐ Zero Trust architecture components implemented

☐ Dedicated cyber staff

☐ Full incident response playbooks with named roles

☐ Immutable/offline backups

☐ Threat hunting activities

☐ Regular third-party penetration tests

Glossary of Terms

Multi-Factor Authentication (MFA): A security method requiring multiple verification factors.

Patching: Applying updates to fix vulnerabilities and improve security.

EDR: Advanced endpoint protection with threat detection and isolation.

Backups: Restorable copies of critical company data.

Phishing Training: Teaching employees to recognize malicious emails.

Password Standards: Rules ensuring strong, hard-to-guess passwords.

Web Filtering: Blocking known malicious or suspicious sites.

Asset Inventory: List of all hardware/software needing protection.

Incident Response Plan: Documented steps to follow during a cyber incident.

Tabletop Exercise: Simulated cyberattack rehearsal with leadership.

Centralized Logging: Collecting logs into one system for analysis.

Network Segmentation: Dividing networks to limit breach spread.

Vendor Risk Assessment: Evaluating partner cybersecurity hygiene.

PAM: Restricting the use of privileged (admin) accounts.

Backup Testing: Verifying that backup data restores properly.

SIEM: System that aggregates and analyzes logs for threats.

MDR: Managed service that monitors and responds 24/7.

SOC: Team monitoring threats continuously.

Vulnerability Scanning: Automated detection of system weaknesses.

Zero Trust: Never trust; always verify users and devices.

Immutable Backups: Backups that cannot be changed or deleted.

Threat Hunting: Proactively searching for hidden threats.

Penetration Testing: Ethical hacking to find vulnerabilities.