# CHIPPY'S CORNER GOVERNANCE, RISK, AND COMPLIANCE REPORT

# AGENDA

EXECUTIVE SUMMARY

GOVERNANCE

RISK MANAGEMENT

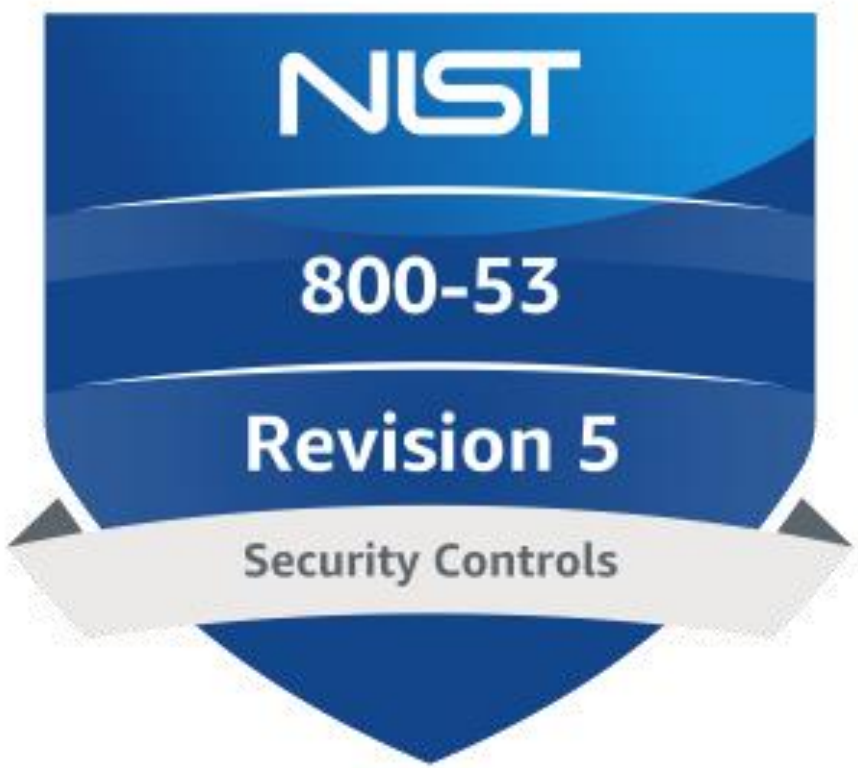
COMPLIANCE

# EXECUTIVE SUMMARY

# PURPOSE

- After the recent incident, Chippy's Corner has placed together a formal governance, risk, and compliance framework.

- This framework introduced new governance policies, assign accountability and roles, review an updated risk assessment, and develop compliance baselines.



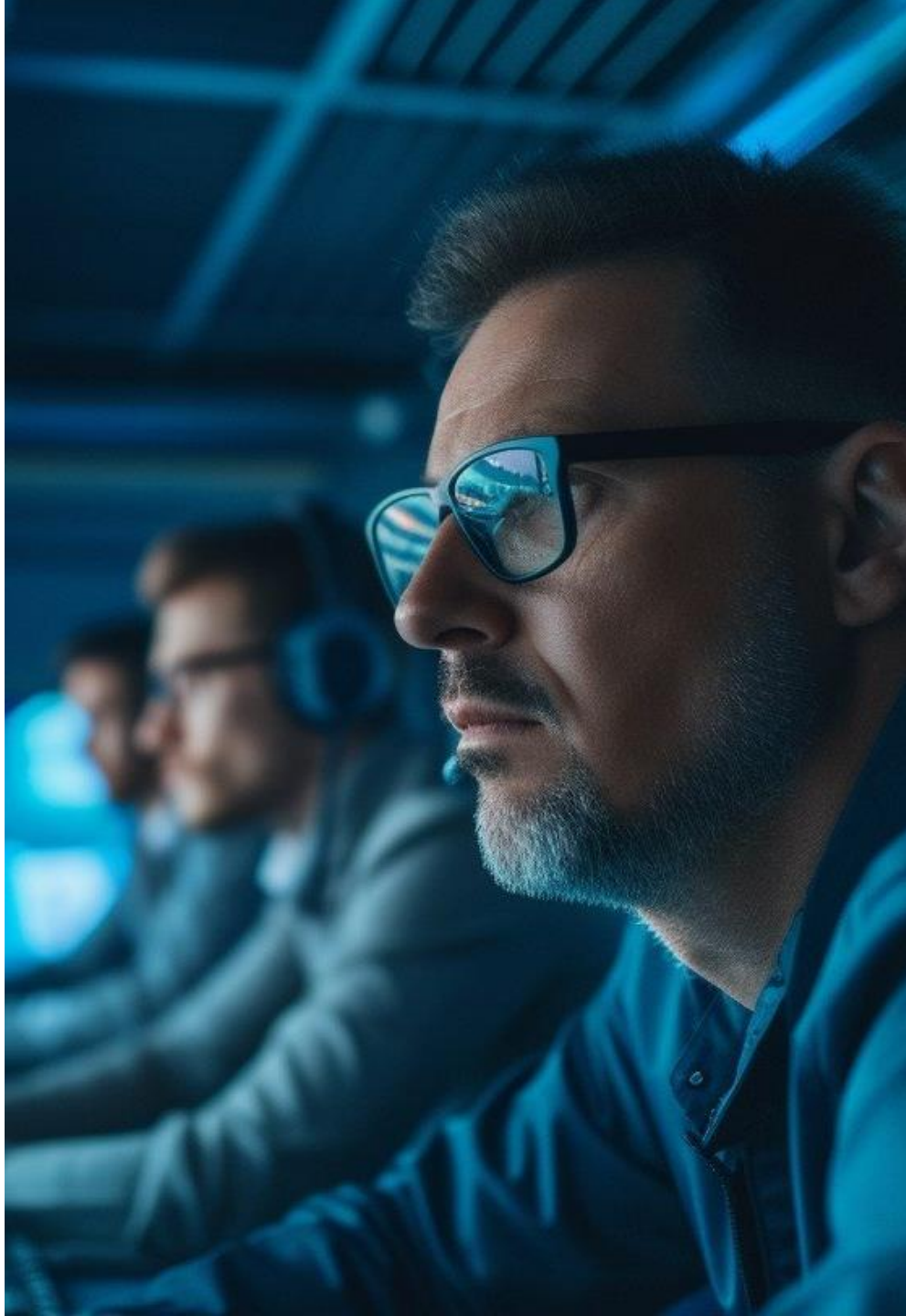
# OBJECTIVES

- Introduce three new governance policies for the organization
- Establish accountability and roles for the organization’s security posture
- Review the updated risk assessment post-hardening.
- Review compliance alignment with NIST SP 800-53

# GOVERNANCE

# SECURITY POLICIES

- Before the incident, Chippy's Corner staff subnet did not have any type of security policies standards in place.
- After the incident, three new policies and standards have been introduced: A password policy, an access control policy, and a set of hardening standards.
- Roles and responsibilities for enforcing these new policies and standards have also been established.



# PASSWORD POLICY

- Minimum 12 characters with upper/lowercase, numbers, and special characters.
- Expiration every 90 days along with no reuse of last 5 passwords.
- Multifactor authentication required for all admin and remote access accounts
- Passwords securely stored using hashing and salting techniques.
- Accounts automatically lock after 3 failed login attempts.

# ACCESS CONTROL POLICY

- Least privilege enforced.
- Remote access (e.g., SSH, RDP) is disabled by default unless justified and approved.
- IT Security will maintain centralized logs of all access attempts for auditing.
- All administrative privileges must be formally approved and reviewed quarterly.
- Access rights must be revoked within 24 hours of employee separation or role change.

# SYSTEM HARDENING STANDARDS

Any software or service that is not necessary for the operation of a system must be removed

Firewall rules must be set on the endpoints and router to block unwarranted traffic

Thorough logging is enabled for processes, data moving throughout the network, and network communications

All system must remain up to date with recent security patches and updates.

# ROLES AND RESPONSIBILITIES

**IT Security:** enforce policies, monitoring.

**Department Managers:** ensure compliance, review access.

**Executives:** strategic oversight and resource allocation.

# RISK MANAGEMENT

# RESIDUAL RISK POST-MITIGATION

All the risks identified in the risk register has been addressed and mitigated properly except for one.

Due to financial constraints, Splunk is unable to be used to view and aggregate the logs collected by Sysmon. The organization is unable to upgrade to a managed switch.

Compensating controls such as endpoint logging with Sysmon and Windows Event viewer have been implemented.

# COMPLIANCE

# COMPLIANCE MAPPING TO NIST SP-800 53

| NIST Control Family | Example Control Implemented | Organizational Action Take |
|---|---|---|
| Access Control (AC) | AC-2, AC-6 (Least Privilege, Access Enforcement) | Strong password rules, MFA for admins, least-privilege enforced, SSH disabled where not needed. |
| System and Information Integrity (SI) | SI-3 (Malicious Code Protection), SI-4 (System Monitoring) | Malicious scripts removed, Sysmon logging for processes/files/network, file transfer monitoring. |
| Configuration Management (CM) | CM-6 (Configuration Settings), CM-7 (Least Functionality) | Servers rebuilt on hardened baseline, only required services/software kept. |
| System and Communications Protection (SC) | SC-7 (Boundary Protection), SC-18 (Mobile Code) | Firewalls restricted to HTTP/HTTPS, outbound blocks added, PHP input sanitization applied. |
| Identification and Authentication (IA) | IA-2 (User Identification and Authentication) | Weak credentials replaced with strong ones, MFA planned for admin accounts. |
| Audit and Accountability (AU) | AU-2, AU-6 (Audit Events, Review, and Analysis) | Centralized event logging with Sysmon, audit trails for file changes and transfers. |