Chippy Chip’s GRC Team

Governance, Risk, and Compliance Report

Prepared by:

Mamadu Bah

Date:

August 16, 2025

Table of Contents

Executive Summary

1.1 Purpose of Report

The purpose of this Governance, Risk, and Compliance (GRC) report is to formally establish a security governance framework in response to the recent cyber incident. Prior to this event, Chippy's Corner had no formal governance policies or procedures in place, leaving critical systems vulnerable and security responsibilities undefined. This report sets the foundation for developing and adopting governance policies that assign accountability, set minimum security requirements, and ensure the organization's operations remain resilient against future threats.

1.2 Scope and Objectives

This report focuses on building a governance structure that both addresses the gaps revealed by the incident and ensures long-term compliance with industry standards. The objectives are to:

- Introduce three new governance policies and standards where none previously existed: a Password Policy, Access Control Policy, and a System Hardening Standard.

- Establish accountability by defining clear roles and responsibilities for security oversight, incident management, and compliance monitoring.

- Conduct a new risk assessment following the system hardening efforts completed during the recovery phase of the incident response. This assessment will re-evaluate the organization's exposure to threats in its newly secured state and ensure that residual risks are identified and prioritized.

- Develop compliance baselines aligned with widely recognized frameworks such as NIST SP 800-53 and ISO 27001 to guide future audits and reviews.

These policies and processes will serve as the foundation for consistent risk reduction, compliance assurance, and stronger security maturity across the organization.

Governance

2.1 Security Policies in Place

Before this assessment, the organization did not have formalized, documented security policies. Security practices existed informally but lacked consistency and standard enforcement. This report establishes a foundation for governance by introducing new policies that address critical areas of password security, access control, and system hardening.

2.2 Updates and New Policies Implemented

Password Policy

All user accounts must be protected by strong, complex passwords that reduce the risk of unauthorized access. Multi-factor authentication (MFA) will be required where available. The following standards must apply to all passwords:

- Minimum password length: 12 characters.
- Must include uppercase, lowercase, numbers, and special characters.
- Passwords expire every 90 days and cannot be reused for the previous 5 cycles.
- MFA is required for all administrator and remote access accounts.
- IT Security is responsible for enforcing and monitoring compliance.

Access Control Policy

Access to systems, applications, and data will follow the principle of least privilege. Users will be granted only the permissions necessary to perform their job duties. The following standards apply for access control:

- All administrative privileges must be formally approved and reviewed quarterly.
- Shared accounts are prohibited; every user must have a unique login.

- Remote access (e.g., SSH, RDP) is disabled by default unless justified and approved.
- Access rights must be removed within 24 hours of employee separation.
- IT Security will maintain centralized logs of all access attempts for auditing.

System Hardening Standards

All servers, endpoints, and applications must be configured to minimize vulnerabilities by removing unnecessary services and applying secure configurations. The following system hardening standards have been put in place:

- Only essential software and services are installed; unnecessary tools (e.g., Python, Sysinternals) are removed unless explicitly approved.
- Firewall configurations allow only required ports (e.g., HTTP/HTTPS) and block unauthorized outbound connections.
- Logging is enabled to capture process execution, file transfers, and network connections for monitoring and incident response.
- Security patches and updates must be applied within 14 days of release for critical vulnerabilities.

2.3 Roles and Responsibilities for Security Oversight

Security oversight within the organization is shared across several functions to ensure accountability and clear lines of authority. The IT Security Lead is responsible for implementing and enforcing the new security policies, including password controls, access restrictions, and system hardening standards. This role also oversees logging, monitoring, and incident response readiness.

Department managers are accountable for ensuring that their staff adhere to the established security policies. They are expected to review access rights on a quarterly basis and promptly notify IT Security when personnel changes require modification or revocation of system access.

Executive leadership provides strategic oversight by approving major policy changes and ensuring that adequate resources are allocated for security initiatives. Their role is to ensure that security objectives remain aligned with broader organizational goals.

To maintain coordination, quarterly security governance meetings will be held between IT Security, department managers, and executive leadership. These meetings will review compliance with established policies, discuss emerging risks, and identify areas for continuous improvement.

Risk Management

3.1 Identified Risks and Threats

All relevant risks and threats have been documented in the organization's risk register. These include risks related to weak authentication practices, insecure remote access, unmonitored system activity, and improper system hardening.

3.2 Risk Assessment and Rating (Likelihood vs. Impact)

Each identified risk was assessed and rated within the risk register using a likelihood-versus-impact methodology. Risks were prioritized accordingly, and treatment plans were applied based on severity. The detailed register serves as the authoritative reference for the assessment results.

3.3 Residual Risk Post-Mitigation

Following remediation efforts, nearly all risks have been fully addressed and mitigated. The only remaining residual risk is related to centralized log management. While Splunk was identified as the preferred solution for robust, enterprise-grade log correlation, it has not been implemented due to cost constraints. As a temporary measure, Windows Event Viewer and Sysmon are being used to capture and monitor security logs. This provides visibility but lacks the correlation and long-term retention capabilities of Splunk.

3.4 Risk Acceptance and Treatment Strategy

Executive leadership has formally accepted the residual risk related to the absence of Splunk, given the financial trade-offs. To reduce exposure, compensating controls such as Sysmon installation, improved firewall configurations, and custom file activity logging scripts have been deployed. A long-term strategy includes revisiting centralized logging solutions when budgetary conditions allow.

Compliance and Controls

4.1 Applicable Regulatory Requirements

The organization is committed to maintaining compliance with relevant information security regulations and best practices. The key framework used in the report is NIST SP 800-53 Rev. 5.

These standards serve as the foundation for implementing technical, administrative, and monitoring controls to ensure resilience against cybersecurity threats.

4.2 Mapping to NIST SP 800-53 and Implemented Controls

Following the recent security review, existing gaps were addressed by implementing targeted controls. These align with specific NIST SP 800-53 control families.

NIST Control Family	Example Control Implemented	Organizational Action Take
Access Control (AC)	AC-2, AC-6 (Least Privilege, Access Enforcement)	Implemented strict password policies (minimum complexity, rotation, and lockout rules). SSH services were disabled on non-essential endpoints. Accounts now follow least-privilege principles.
System and Information Integrity (SI)	SI-3 (Malicious Code Protection), SI-4 (System Monitoring)	Malicious scripts removed. Sysmon is deployed on endpoints to log process, file, and network events. A custom script logs sensitive file transfers for visibility.
Configuration Management (CM)	CM-6 (Configuration Settings), CM-7 (Least Functionality)	Web server rebuilt on a hardened baseline with only required services. Unnecessary software (Python, Sysinternals tools) was removed to reduce the attack surface.
System and Communications Protection (SC)	SC-7 (Boundary Protection), SC-18 (Mobile Code)	Firewalls reconfigured to restrict all but essential inbound ports (HTTP/HTTPS). Outbound restrictions were added to prevent reverse shell traffic. Input sanitization applied to PHP code.

Identification and Authentication (IA)	IA-2 (User Identification and Authentication)	Weak credentials replaced with stronger authentication requirements. Multi-factor authentication is planned for administrative access.
Audit and Accountability (AU)	AU-2, AU-6 (Audit Events, Review, and Analysis)	Windows Event Logs are centralized and enhanced with Sysmon to provide higher fidelity monitoring. Audit trails for file modifications and transfers enabled.

4.3 Gaps Identified and Corrective Actions

The following compliance gaps were identified during the review process, along with the actions taken to address them:

- Weak authentication controls: Passwords were not consistently aligned with best practices. A new password policy has been implemented, requiring longer, complex credentials and regular updates.
- Unrestricted remote access: SSH services were enabled unnecessarily on multiple systems. SSH has now been fully disabled where not required.
- Insufficient web application input validation: The PHP web application lacked sufficient sanitization, allowing malicious input. The script has been updated to properly sanitize and validate all inputs.
- Limited centralized logging: Due to cost constraints, Splunk was not deployed. As a corrective action, enhanced logging has been configured with Windows Event Viewer and Sysmon to ensure monitoring continues.

4.4 Ongoing Compliance Monitoring

To maintain compliance and ensure continuous improvement, the following measures are in place:

- Regular audits: Quarterly reviews of system configurations, firewall rules, and account permissions will be conducted.

- Log review and alerting: Sysmon and Windows Event Viewer are actively monitored to detect anomalous behavior.

- Policy compliance checks: New password and access control policies are enforced and reviewed regularly for adherence.

- Risk reassessment: Following significant changes or updates, a risk review will be performed to ensure that mitigations remain effective.

Conclusion

5.1 Summary of Findings

The organization's recent review demonstrates that critical security gaps identified in prior assessments and operational practices have been effectively addressed. Systems have been hardened, unnecessary services removed, and enhanced monitoring and logging mechanisms implemented. Policies for password management, access control, and system hardening have been established, creating a foundation for sustainable governance. While a residual risk remains in centralized SIEM capabilities, compensating controls via Sysmon and Windows Event Viewer provide ongoing visibility and risk mitigation.

5.2 Path Forward for Security Governance

Looking ahead, the organization will continue to strengthen governance, risk, and compliance maturity through:

- Ongoing monitoring of security controls and log data to detect and respond to emerging threats.

- Periodic risk assessments to maintain awareness of evolving organizational and technical risks.

- Continuous review and enhancement of security policies and procedures to align with best practices and regulatory requirements.

- Structured compliance readiness activities to ensure sustained adherence to NIST SP 800-53 and other applicable standards.

These steps establish a clear path toward resilient security operations and demonstrate a proactive approach to protecting organizational assets and data.