WIDGET Co. CYBERSECURITY PROGRAM PROPOSAL

To address growing security concerns from customers and stakeholders, Widget Co. requires a structured cybersecurity framework that ensures robust risk management and compliance. This report outlines a recommended security framework, governance strategy, and compliance measures tailored to support Widget Co.'s security objectives.

To achieve this, we propose implementing the **NIST Cybersecurity Framework (NIST CSF 2.0)**[1]. This framework provides a comprehensive, scalable, and risk-based approach to cybersecurity, helping Widget Co. manage security threats effectively while meeting compliance requirements. Additionally, the **Centre for Internet Security (CIS) Controls**[2] will be leveraged as a practical guide to implementing the security measures outlined in the framework. By combining NIST CSF 2.0 with CIS Controls, Widget Co. can establish a structured and actionable approach to security that ensures both high-level strategic alignment and operational effectiveness.

NIST CYBERSECURITY FRAMEWORK (CSF 2.0) OVERVIEW

The **NIST CSF 2.0** consists of six core functions: **Govern**, **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. Each function plays a critical role in securing Widget Co.'s infrastructure and customer data by ensuring cybersecurity is aligned with business objectives and operational resilience. To make these functions more actionable, **CIS Controls** provide specific security measures that can be implemented to support the broader framework objectives.

(i) Govern (New in CSF 2.0) – Cybersecurity Strategy & Risk Management

- The **Govern** function establishes security governance by defining leadership roles, cybersecurity policies, and regulatory alignment. Implementing a structured risk management program ensures that Widget Co. can proactively identify and mitigate risks.
- A dedicated **Security Governance Structure**, led by a CISO and a security leadership team, will oversee the cybersecurity strategy and ensure it evolves with emerging threats and compliance requirements.

(ii) Identify – Asset & Risk Management

- The **Identify** function provides visibility into Widget Co.'s technology assets, ensuring proper risk assessment and access control.
- By maintaining an up-to-date inventory of enterprise hardware and software, unauthorized access risks can be mitigated.
- To support this effort, **CIS Control 1 (Enterprise Asset Inventory)** and **CIS Control 2 (Software Asset Inventory)** help in cataloging and managing hardware and software assets, reducing exposure to potential security threats.

---

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[2] https://www.cisecurity.org/controls/cis-controls-list

(iii) Protect – Secure Configuration & Access Controls

- The **Protect** function strengthens Widget Co.'s security posture by implementing secure configurations for systems and applications. Ensuring proper security configurations helps prevent unauthorized changes, misconfigurations, and exploitation by threat actors.
- **CIS Control 4 (Secure Configuration of Enterprise Assets & Software)** provides specific guidance on enforcing configuration baselines across endpoints, servers, and applications to mitigate these risks.

(iv) Detect – Threat & Anomaly Identification

- Proactive detection of potential security threats is essential for Widget Co. to maintain a secure operational environment. Continuous monitoring and logging of network activity ensure that anomalies and unauthorized access attempts are identified in real-time.
- **CIS Control 7 (Continuous Vulnerability Management)**, **Control 8 (Audit Log Management)**, and **Control 13 (Network Monitoring & Defense)** align with this function by enabling structured vulnerability assessments, centralized logging, and network-based threat detection.

(v) Respond – Incident Containment & Mitigation

- An effective **incident response plan** is crucial to mitigating security breaches and minimizing business impact. By implementing structured processes for incident detection, containment, eradication, and recovery, Widget Co. can limit disruptions caused by security incidents.
- **CIS Control 17 (Incident Response Management)** provides guidance on establishing a formal incident response process, ensuring that Widget Co. can rapidly contain and remediate security threats while maintaining operational continuity.

(vi) Recover – Business Continuity & Resilience

Post-incident recovery ensures that Widget Co. can restore operations with minimal disruption. Developing a **Business Continuity Plan (BCP)** and conducting **post-incident reviews** improve resilience against future security threats. This function focuses on restoring affected systems, learning from security incidents, and continuously enhancing security measures to mitigate future risks.

ROADMAP (PHASE-WISE IMPLEMENTATION)

The following phased approach will allow Widget Co. to build a strong security foundation and gradually enhance security operations:

- **Phase 1**: Risk Assessment & Asset Inventory (CIS Controls 1 & 2) – Establish visibility and risk management.
- **Phase 2**: Secure Configurations & Protection Mechanisms (CIS Control 4) – Implement security hardening measures.

- **Phase 3**: Monitoring & Detection (CIS Controls 7, 8, 13) – Set up logging, anomaly detection, and proactive threat hunting.
- **Phase 4**: Incident Response & Recovery Strategy (CIS Control 17) – Ensure structured response and containment capabilities.
- **Phase 5**: Compliance Alignment & Security Certifications – Achieve regulatory compliance and security assurance.

SECURITY OPERATIONS CENTRE

Real time monitoring and threat detection are crucial for Widget Co. Security Operations Centre can be built around a Security Information and Event Management system.

- **SOC Model**: Hybrid SOC which is a combination of both in house and Managed Security Service Provider (MSSP) support 24/7 is best for Widget Co based on the budget and requirements.
- **SIEM**: Splunk Enterprise Security is expensive but it's best for Advanced threat detection integrating feeds from Open-Source Intelligence such as MITRE ATT&CK, Virus Total, ABuseIPDB etc.

SOC ROLES & RESPONSIBILITIES

- **Tier 1 Analysts:** Initial alert triage & investigation.
- **Tier 2 Analysts:** Advanced threat hunting & forensic analysis.
- **Incident Responder:** Immediate containment & mitigation.
- **SOC Manager:** Oversees security operations & compliance.

SOC ROADMAP

- **Phase 1:** SIEM onboarding & rule tuning.
- **Phase 2:** Threat hunting & behavioural analytics.
- **Phase 3:** Automated threat response using SOAR (Security Orchestration, Automation, and Response).
- **Phase 4:** Integration with AI driven analytics and Open-Source Intelligence feed to improve threat detection.

ZERO TRUST SECURITY MODEL

With Software as a Service based application, it is important to implement zero trust architecture to enhance security.

- **Least privilege access:** Implementing Access controls such as Role Based and Rule Based are recommended.
- Enforce Multi Factor Authentication for all users to access their accounts.
- Web Application Firewall to prevent SQL injections, Directory Traversal etc.