MEMORANDUM

TO: CISO of COMPANY X

FROM: Utsav Patel

SUBJECT: Security Services Directory Plan

DATE: November 3rd, 2025

Hello CISO of COMPANY X,

After reviewing the company's current structures and conducting my own research on cybersecurity frameworks, I have concluded that the NIST framework is the best fit for the company given its current vulnerabilities. NIST security framework is essentially based on simple steps of Identity, Protect, Detect, Respond, and Recover. It also has a foundation called Govern, which is basically the core around which the other five revolve for security. The company is very dependent on its executive team, while also lacking in some simple, outdated methods, based on the overview provided to me of the company's operations and strategies.

I look over countless other security frameworks. One was the ISO 27001 Framework, whose focus is on ensuring the proper security of sensitive information. The framework is similar to the NIST framework, but the security needed was not only sensitive but also ensured that overall security is improved. Another framework I researched was CIS Controls, which is more towards making sure to have a strong system to defend against cyber-attacks. Since there are more around controls instead of an overall understanding of risk, the framework would only create more gaps in the company's operations. Finally, I also looked over the COBIT framework, which felt like a more complex infrastructure of the NIST framework. The framework is structured in a more complex and efficient way. The framework would be a better option, but the framework needed a more elevated foundation in place; hence, despite choosing the NIST framework, this framework can be implemented in the future once the company is accustomed to the NIST framework.

Please let me know if you have any questions or concerns. I am happy to discuss more in-depth about my framework chosen in a meeting, either one-on-one or with other personnel. I look forward to implementing the NIST framework for the security plan.

Sincerely,

Utsav Patel

Cybersecurity Consultant

utsav.patel@aegissecuritypartners.com

Security Services Directory Development Plan

Purpose

The purpose of this plan is to create a clear and comprehensive security service plan for COMPANY X The service directory will serve as both a handbook and a record of the security services established for the firm's business operations, risk management efforts, and regulatory compliance obligations. Each service item will provide key information about the service, such as a description of the service, which department or stakeholder will receive the service, service frequency, justification of why the service is required, and the associated costs of the service. With the creation of this service plan, COMPANY X aims to standardize its cybersecurity operations, ensure accountability, and establish its security practices with the NIST Cybersecurity Framework.

Plan

The Security Service Directory Development Plan will be established through a structured and collaborative process, ensuring the creation is done with accuracy, consistency, and aligned with both business and security objectives. The initial stage will involve the identification of COMPANY X's primary risk areas and operational requirements, which will be acquired through reviewing all critical documents and conducting interviews with crucial members holding important roles in the company. These documents highlight areas where cybersecurity controls are critical, including access management, incident response, data protection, and compliance monitoring.

After identifying the risks in the firm, those risk areas will then be mapped to the five core functions of the NIST framework, which are Identity, Protect, Detect, Respond, and Recover. Mapping these risks will ensure the directory plan establishes a balanced approach to cybersecurity management, addressing both initiative-taking and reactive measures. Each relevant service will be outlined based on the function the service is connected to in relation to the core function. This alignment guarantees that all aspects of cybersecurity are represented and that no critical service area is overlooked.

Once the framework alignment is complete, the next phase focuses on defining each service in standardized terms to maintain clarity and consistency. Each entry will follow a common structure that includes the service name, description, receiver of service, frequency, justification, and cost or cost recovery method. Information for each service will be gathered through collaboration with key departments, including IT Operations, HR, Compliance, Finance, and Legal, to ensure that services are accurately represented and that ownership is correctly assigned. Additionally, industry standards and vendor best practices will be reviewed to benchmark service frequencies and cost estimates, providing realistic and defendable values.

After the initial draft is assembled, the directory will undergo internal review for completeness and alignment with business needs. This review will ensure that each service contributes directly to COMPANY X's operational efficiency, security posture, and regulatory compliance goals. The directory will then be formatted into a professional, easy-to-reference structure that can be used by both executives and operational teams. The final plan will serve not only as a working reference for day-to-day cybersecurity activities but also as a strategic planning tool for budgeting and resource allocation in future fiscal cycles.

Plan Validation

Once the directory is drafted, it will be validated through collaboration with business unit partners and executive leadership. Department heads will first review their respective service listings to confirm ownership, frequency, and cost accuracy. The draft will then be evaluated by the CISO, CIO, and GRC Office to ensure that all services align with COMPANY X's strategic security objectives and compliance obligations. After revisions are made, the final version will be approved by executive management. The SSD will be maintained as a living document and reviewed annually or after major changes to keep it current and aligned with COMPANY X's evolving cybersecurity landscape.

Security Services Table

Service	Description	Receiver of Service	Frequency	Justification	Expenditure / Cost Recovery
Access Management	Manage account creation, modification, and termination; enforce MFA and RBAC policies.	HR Department / IT Operations	As needed	Ensures proper access control during onboarding, promotions, or separations. Reduces insider threat risk.	Cost per employee for identity management billed to HR.
Security Awareness Training	Conduct phishing simulations and cybersecurity awareness programs.	All Employees	Quarterly	Reduces human error vulnerabilities and social engineering incidents.	Training license fee billed to HR/Training budget.
Vulnerability Management	Perform automated scanning and patch verification for servers, endpoints, and network devices.	IT Security Department	Monthly	Identifies and remediates system weaknesses before exploitation.	Included in InfoSec budget; tool licensing billed to IT.
Endpoint Detection & Response (EDR)	Deploy and manage real-time endpoint protection and behavioral monitoring.	IT Security Department	Continuous	Provides initiative-taking detection and isolation of threats at the device level.	Managed service cost billed to IT Operations.
SIEM / Log Monitoring	Aggregate and analyze logs for anomalies across infrastructure using a Security Information and Event Management system.	Security Operations Center (SOC)	24/7 Continuous	Enables early detection of cyber incidents and compliance with audit standards.	Managed SOC service billed monthly to IT.
Incident Response & Forensics	Coordinate investigation, containment, and recovery from cybersecurity events.	CISO / Incident Response Team	As needed	Minimizes damage from security incidents and supports legal/regulatory reporting.	Per-incident consulting fee billed to the Security Department.

Service	Description	Receiver of Service	Frequency	Justification	Expenditure / Cost Recovery
Disaster Recovery & Business Continuity	Maintain redundant data backups and assess recovery procedures to ensure operational resilience.	IT Operations / Business Units	Semi-annually	Ensures critical systems can recover after data loss, outage, or attack.	Cloud storage and testing costs are billed to Operations.
Network Security Management	Configure and monitor firewalls, VPNs, and IDS/IPS systems to protect data in transit.	Network Operations	Continuous	Reduces risk of unauthorized access and data interception.	Hardware/software maintenance billed to IT.
Data Loss Prevention (DLP)	Implement policies to detect and block unauthorized data transfers or leaks.	Compliance & Legal	Continuous	Prevents data exfiltration and protects intellectual property.	Annual license cost billed to Compliance.
Cloud Security Management	Monitor cloud-based environments (Azure, SaaS apps) for compliance and access integrity.	IT Cloud Team	Continuous	Protects critical assets as COMPANY X expands cloud services and remote operations.	Service subscription billed to Cloud Division.
Third-Party Vendor Risk Assessment	Assess external vendors and partners for compliance, data protection, and contract risk.	Procurement / Legal	Annual	Ensures vendors adhere to security standards and reduces supply chain exposure.	Consulting cost billed to Procurement.
Penetration Testing & Red Teaming	Conduct ethical hacking exercises to evaluate system resilience and response capabilities.	Information Security	Semi-annually	Validates system defenses and identifies exploitable vulnerabilities.	External testing cost billed to InfoSec.

Service	Description	Receiver of Service	Frequency	Justification	Expenditure / Cost Recovery
Policy & Compliance Auditing	Review and update organizational security policies for NIST, ISO 27001, and HIPAA alignment.	GRC / CISO Office	Annual	Maintains regulatory compliance and supports investor assurance.	Compliance audit fee billed to the GRC Department.

Summary of Approach

The approach to developing the Security Services Directory for Diamond Hands Holdings Inc. followed a structured, methodical process rooted in the NIST Cybersecurity Framework. The first step involved identifying COMPANY X's core cybersecurity needs and risk areas by reviewing the organization's critical documents, policies, and existing governance structure. This allowed for a clear understanding of the company's operations, data dependencies, and areas requiring stronger security oversight. These findings were then mapped to the five NIST CSF functions, Identify, Protect, Detect, Respond, and Recover, to ensure that all aspects of cybersecurity were represented within the directory.

Once the foundational framework was established, specific services were defined under each functional area. Each service was described in consistent terms, including the purpose of the service, its frequency, cost model, and business justification. Input from key departments such as IT, HR, Compliance, and Operations was incorporated to ensure that each service reflected realistic operational practices and ownership responsibilities. This cross-departmental collaboration helped create a directory that not only supports cybersecurity goals but also aligns with business priorities and financial planning.

In a real-world organizational setting, this process would be far more dynamic and iterative. Departments would provide continuous feedback, and services would be adjusted based on new technologies, emerging threats, and changes in regulatory requirements. The directory would also integrate with the company's Governance, Risk, and Compliance tools to automate tracking and reporting. Additionally, service performance metrics would be gathered over time to evaluate effectiveness and inform decision-making.

Validation of the directory would occur through collaboration with business unit partners and executive leadership. Department heads would review entries for operational accuracy, and the CISO would ensure strategic alignment with the company's risk management objectives. The final directory would be approved by senior leadership and reviewed on an annual basis to maintain its accuracy and relevance. This structured approach ensures that the Security Services Directory remains a living document that is continuously improving and aligning with COMPANY X's evolving environment and providing lasting value to both security operations and the broader organization.