Understanding the NIST Cybersecurity Framework (CSF)

Using the CSF to support a small organization that operates an online business that utilizes computers, network, servers, and cloud services to store and process customer data.

Part 1: Identify – Asset Inventory

Asset Name	Asset Type	Description	Owner	Criticality
Employee Laptops	Hardware	This is used for operations and customer service	IT Manager	Medium
Web Application Server	Cloud VM	Primary server hosting the organization's public website and API endpoints. Handles all inbound customer traffic and integrates with the payment gateway.	DevOps Engineer	High
Customer Database	SQL Database(Cloud)	Stores customer accounts, order history, and authentication data.	Database Administrator	High
Payment Gateway Integration	Saas Payment Processor	Processes credit card and digital wallet payments through a third-party provider.	Lead Developer	High
DNS Hosting Service	Cloud	Manages domain records for website, email and API endpoints	DevOps Engineer	High
Firewall	Network Security Device	Protects the web application by filtering	Security Engineer	High

		traffic and enforcing access policies.		

Part 2: Govern - Organizational Roles

#	Role	Risk Decision	Security Controls	Policy Compliance
1	Chief Technology Officer (CTO)	The CTO makes final decisions on cybersecurity risks—what risks the business accepts, mitigates, or transfers. They balance security needs with business goals.	Approves major security controls such as encryption standards, firewall configurations, and cloud security architecture.	Ensures the organization follows internal security policies and external regulatory requirements (e.g., data protection laws).
2	Chief Executive Officer (CEO)	The CEO has ultimate authority over business-level risk acceptance. They decide which cybersecurity risks the organization is willing to tolerate based on financial impact, customer trust, and strategic priorities	The CEO does not configure controls but approves funding and resources for major security initiatives (e.g., new firewalls, cloud security tools, compliance programs).	The CEO ensures the entire organization follows security policies by setting expectations, supporting enforcement, and holding leadership accountable.
3	Security Engineer / Cybersecurity Analyst	Identifies risks through monitoring, scanning, and assessments, and recommends actions to leadership.	Configures and monitors security tools (SIEM, WAF, vulnerability scanners) and supports secure cloud configurations.	Conducts audits, reviews logs, and reports compliance gaps to leadership.

Part 3: Identify – Data Types and Applicable Laws

#	Data Type	Description	Applicable Law/Standards

1	Payment Card Data	Credit/debit card information	PCI DSS
2	Personally Identifiable Information (PII)	Customer names, emails, addresses	GDPR / CCPA
3	Protected Health Information	Any identifiable health, treatment, or payment information like health history, DOB, SSN, Medical record number, Treatment plans	HIPAA

Part 4: Protect – Protection Control

Asset: Payment Gateway Integration

Control: Enforcing TLS 1.2+ Encryption for All Payment Transactions

Reasons:

- Payment data (e.g., card numbers, billing details) is highly sensitive and must be protected from interception.
- TLS prevents attackers from reading or modifying payment information during transmission.
- Many payment processors and compliance frameworks (including PCI DSS) require strong encryption for all payment-related traffic.
- Without TLS, the organization risks data breaches, fraud, and regulatory penalties.

NIST Function: Protect (PR.DS – Data Security) which aligns with -

- PR.DS-2 — Data-in-transit is protected
- PR.PT-4 — Communications and control networks are protected

Part 5: Detect – Detection Control

Method: SIEM log monitoring

Detects: Multiple failed login attempts from the same IP/ Sudden spikes in authentication failures

NIST CSF Mapping — Detect Function specifically:

- DE.AE-1 — Anomalous activity is detected
- DE.CM-7 — Monitoring for unauthorized personnel, connections, devices, and software is performed
- DE.CM-1 — The network is monitored to detect potential cybersecurity events

Part 6: Respond – Incident Response Process

1. Notification
   - ❖ The person who discovers the issue (employee, IT admin, monitoring alert, or automated system) immediately notifies the IT Administrator or Security Analyst.
   - ❖ If the incident appears serious (e.g., customer data exposure, system compromise), the CTO and CEO are notified as part of the escalation process.
   - ❖ Notification should be done through the organization's designated channel (ticketing system, incident hotline, or direct message to IT).

2. Immediate Action

- ❖ Contain the incident to prevent further damage. Examples include:
- ❖ Disabling a compromised user account
- ❖ Isolating an infected workstation from the network
- ❖ Blocking suspicious IP addresses or API keys
- ❖ Stopping unauthorized processes or shutting down affected services

3. Documentation: The responder records all relevant details, including:

- ❖ What was detected
- ❖ When it was detected
- ❖ Who reported it
- ❖ Systems or data affected
- ❖ Actions taken and by whom
- ❖ Any evidence collected (logs, screenshots, timestamps)

Documentation is to be stored in the organization's incident tracking system for review and future improvement.

Part 7: Recover – Business Continuity

Scenario: If the primary web server or database becomes unavailable due to an incident or system failure, the organization activates its redundant backup server (or cloud failover instance) to restore service availability to ensure customers can continue accessing the online platform with minimal downtime.

The recovery plan would be that:

- ❖ The IT Administrator confirms the primary system is offline or compromised.
- ❖ The backup server—kept updated and synchronized—is brought online.
- ❖ DNS or load balancer settings are updated to route traffic to the backup environment.
- ❖ The team verifies that the backup system is functioning correctly and serving customer requests.
- ❖ Once the primary system is repaired and validated, operations are transitioned back.