UNIVERSITY OF SCIENCE AND TECHNOLOGY
OF SOUTHERN PHILIPPINES

Enterprise Security and Incident Response for Titan Manufacturing Corporation (TMC)

"Manufacturing / Industrial Firm"

Cybersecurity Team

Wendel T. Lapura

Janice P. Tabaco

Klebert S. Acoymo

Mark Roel Zapico

Christian Codilla

Information Assurance and Security

Instructor

Mitzi Clyde Turtor

Table of Contents

Executive Summary

Titan Manufacturing Corporation (TMC) is a mid-sized industrial firm specializing in the production of heavy machinery components and automotive parts for both local and international clients. With the rapid digitalization of manufacturing operations, TMC has integrated advanced automation, industrial control systems (ICS), and Internet of Things (IoT) technologies to enhance production efficiency. However, this digital transformation has also increased the organization's exposure to cybersecurity threats that could severely disrupt operations, compromise sensitive data, and damage corporate reputation.

This document presents a comprehensive cybersecurity strategy and incident response simulation tailored for TMC. It aims to assess the company's digital assets, identify vulnerabilities, and propose security controls aligned with recognized industry standards such as the **NIST Cybersecurity Framework (CSF)** and **ISO/IEC 27001**. The plan includes a detailed Threat and Vulnerability Assessment, Security Controls Plan, Incident Handling Framework, and a Business Impact Analysis (BIA).

The end goal is to establish a resilient and secure manufacturing environment that ensures **business continuity, data integrity, and operational safety** in the face of evolving cyber threats. A technical demonstration, focusing on authentication and encryption mechanisms, will supplement the conceptual strategy to show practical applications of cybersecurity principles in a real-world industrial context.

Company Profile

Company Overview

Company Name: Titan Manufacturing Corporation (TMC)
Industry Sector: Heavy Industrial Equipment & Automotive Component Manufacturing
Headquarters: Calabarzon Industrial Park, Philippines

Number of Employees: Approximately 900

Operational Sites:

- Main Production Facility (Calabarzon)
- Secondary Warehouse (Laguna)
- Corporate Office (Makati City)

Vision

To be a leading and trusted manufacturer of high-quality industrial and automotive components through innovation, technology-driven operations, and sustainable practices.

Mission

To deliver excellence in manufacturing by combining operational efficiency, digital innovation, and robust cybersecurity practices that ensure the protection of assets, workforce, and partners.

Organizational Structure

TMC operates with three main divisions:

1. **Production and Operations Division** – Manages production lines, industrial control systems, and equipment maintenance.
2. **Information Technology Division** – Oversees enterprise systems, cybersecurity, and digital transformation initiatives.

3. **Finance and Administration Division** – Handles financial operations, HR systems, procurement, and compliance.

IT & OT Environment Overview

TMC's infrastructure integrates Information Technology (IT) and Operational Technology (OT) environments to achieve smart manufacturing capabilities.

- **IT Systems:** Enterprise Resource Planning (ERP), email servers, HR systems, and databases.
- **OT Systems:** Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and connected IoT sensors.
- **Network Setup:** Segmented VLANs separating IT and OT, protected by firewalls and access control policies.
- **Cloud Integration:** Certain business data and analytics dashboards are hosted on secure cloud platforms.

Key Cybersecurity Challenges

1. Increasing cyberattacks targeting industrial control systems.
2. Potential insider threats and unauthorized access to production data.
3. Lack of centralized monitoring and incident response.
4. Inadequate awareness of cybersecurity best practices among factory personnel.
5. Dependency on third-party vendors and suppliers for software and machinery maintenance.

Asset Inventory

The following table enumerates TMC's critical assets, categorized and classified based on importance and sensitivity.

Asset Name	Type	Value	Owner/Department	Security Classification
Enterprise Resource Planning (ERP) System	Software / Database	High	IT Division	Confidential
Manufacturing Control System (SCADA + PLCs)	Hardware / Software (OT)	Very High	Production Division	Critical
Employee Workstations	Hardware	Medium	All Departments	Internal Use
Company Email Server	Software / Network Service	High	IT Division	Confidential
Financial Database	Database	Very High	Finance Division	Confidential
HR Information System	Software / Database	High	HR Department	Confidential
IoT Sensors and Smart Machines	Hardware / IoT	High	Production Division	Critical
Internet Gateway & Firewall Appliance	Network Hardware	Very High	IT Division	Critical
Backup and Disaster Recovery Server	Hardware / Storage	High	IT Division	Confidential
Cloud Storage Platform (Business Data)	Cloud Service	High	IT Division	Confidential
Physical Access Control System (RFID Entry)	Hardware / Physical	Medium	Security Office	Internal Use
CCTV Surveillance System	Hardware / Network	Medium	Facilities Management	Internal Use
Source Code Repository (Internal Tools)	Software Repository	High	IT Division	Confidential
Customer and Vendor Database	Database	Very High	Sales & Procurement	Confidential
Corporate Email Accounts (Executives)	Accounts / Identity	High	IT Division	Confidential
Production Line Servers	Hardware	Very High	Production Division	Critical
Network Switches and Routers	Hardware	High	IT Division	Confidential

Employee Training Materials	Document Repository	Medium	HR / IT Security	Internal Use
Business Continuity Plan Documents	Documentation	High	Management	Confidential

Summary of Asset Classification

- **Critical Assets:** Systems whose compromise would directly halt production or endanger safety (e.g., SCADA, IoT, Production Servers).
- **Confidential Assets:** Information whose disclosure could lead to financial loss or reputational damage (e.g., financial database, ERP, email systems).
- **Internal Assets:** Supporting systems necessary for daily operations but with moderate risk impact (e.g., CCTV, RFID access systems).

Infrastructure Overview

TMC operates a **hybrid infrastructure** combining **on-premises** servers and **cloud-hosted** applications. The network is segmented into three primary zones:

1. **Corporate IT Network:** Hosts ERP, HRIS, email, and general office systems.
2. **Production OT Network:** Contains SCADA servers, PLCs, IoT devices, and machine controllers with restricted access.
3. **DMZ (Demilitarized Zone):** Provides controlled access to external vendors and cloud applications.

All networks are protected by **firewalls, intrusion detection systems (IDS)**, and **multi-factor authentication** for privileged accounts.
A **Security Operations Center (SOC)** within the IT Division monitors network activity and performs log analysis.

Threat & Vulnerability Assessment

Overview

As Titan Manufacturing Corporation (TMC) continues to expand its digital footprint through automation and Industrial Internet of Things (IIoT) integration, the attack surface of the organization has significantly widened. The combination of traditional Information Technology (IT) systems and Operational Technology (OT) environments introduces unique cybersecurity risks that, if left unmanaged, could lead to **production downtime**, **data breaches**, and **financial losses**.

This assessment identifies the **most probable threats**, associated **vulnerabilities**, and their potential **likelihood** and **impact**. Each risk factor is analyzed to support the formulation of an effective **Security Controls Plan** in the next phase.

The methodology aligns with best practices outlined in the **NIST SP 800-30 (Guide for Conducting Risk Assessments)** and **ISO/IEC 27005 (Information Security Risk Management)** standards.

Key Threat Categories in Manufacturing

1. **Ransomware and Malware Attacks** – Targeting production systems and data backups to disrupt operations or extort payment.
2. **Insider Threats** – Negligent or malicious employees causing unauthorized access, data leakage, or sabotage.
3. **Phishing and Social Engineering** – Deceptive emails or messages designed to steal credentials or distribute malware.
4. **Industrial Espionage** – Competitors or nation-state actors seeking to steal intellectual property, designs, or production data.
5. **Supply Chain Attacks** – Compromises introduced through third-party vendors or software updates.
6. **Network Intrusions** – Exploitation of unpatched systems, weak credentials, or misconfigured firewalls.

7. **IoT and ICS Vulnerabilities** – Exploitation of insecure protocols or outdated firmware in IoT sensors and SCADA devices.
8. **Denial-of-Service (DoS) Attacks** – Flooding network resources or production servers, causing downtime.
9. **Physical Security Breaches** – Unauthorized physical access to servers, control rooms, or sensitive areas.
10. **Natural Disasters or Power Outages** – External factors leading to data loss or operational disruption if disaster recovery is insufficient.

Identified Vulnerabilities

A vulnerability assessment was performed on TMC's IT and OT assets to identify weak points exploitable by threat actors.

Vulnerability Area	Description
Outdated SCADA firmware	Legacy devices do not receive frequent security patches.
Shared administrative accounts	Multiple staff use common credentials for PLC maintenance.
Weak email filtering system	Limited phishing detection and spam protection.
Inadequate user access controls	Employees retain access after transfer or resignation.
Lack of regular penetration testing	Absence of proactive vulnerability identification.
Insufficient endpoint protection	Some workstations lack updated antivirus or EDR solutions.
Shadow IT usage	Unapproved cloud apps are used by employees for file sharing.
Poor physical access control	Shared ID badges and unsecured control room doors.
Absence of centralized log monitoring	Logs from production and IT systems are not fully aggregated.
Weak encryption of sensitive data	Some internal databases still use outdated cryptographic algorithms.

Threat and Vulnerability Matrix

Threat	Vulnerability Exploited	Likelihood	Impact	Countermeasure / Mitigation Strategy

Ransomware Attack	Unpatched systems, weak email filtering, no offline backups	High	Very High	Implement email sandboxing, network segmentation, and offline encrypted backups. Conduct regular phishing awareness training.
Insider Threat (Malicious or Negligent)	Shared credentials, excessive access privileges	Medium	High	Enforce Role-Based Access Control (RBAC), apply least privilege principles, and implement behavior monitoring with alerts.
Phishing / Social Engineering	Weak employee awareness, lack of MFA	High	Medium	Conduct continuous cybersecurity awareness programs and enforce MFA for all external logins.
Industrial Espionage / Data Theft	Weak encryption, unsecured intellectual property files	Medium	High	Apply AES-256 for encryption on sensitive files, network DLP solutions, and access logging for IP-related assets.
Supply Chain Attack	Vendor software updates not verified	Medium	High	Enforce vendor security assessments and digital signature verification for all third-party updates.
IoT Device Exploitation	Outdated firmware, unsecured communication protocols	High	High	Regular patching schedule for IoT devices, network isolation for OT systems, and implementation of an IoT security gateway.
DoS Attack (Network Flooding)	Unfiltered network traffic, lack of redundancy	Medium	High	Deploy network firewalls with rate limiting, DDoS mitigation tools, and redundant connectivity.
Physical Intrusion / Theft	Inadequate access control or CCTV coverage	Low	Medium	Strengthen physical security through biometric access, CCTV coverage review, and regular audits.
Data Breach (Database Compromise)	Weak encryption, outdated database software	Medium	Very High	Apply database hardening, encryption at rest, regular vulnerability scanning, and data masking.
Natural Disaster / Power Outage	Lack of backup power and disaster recovery plan	Low	Very High	Establish DR site, conduct regular backup tests, and deploy UPS/Generator systems.

Risk Analysis Summary

Risk Level	Criteria	Examples from TMC	Action Priority
Critical (High Likelihood + High Impact)	Threats that can halt production or cause severe data loss.	Ransomware, IoT exploitation, and insider misuse.	Immediate implementation of technical and administrative controls.
Moderate (Medium Likelihood + High Impact)	Could disrupt operations or leak sensitive data.	Supply chain attacks, data breaches, and DoS attacks.	Mitigate within short-term cybersecurity roadmap.
Low (Low Likelihood + Medium Impact)	Limited operational damage or quick recovery possible.	Physical intrusion, natural disasters.	Included in contingency and disaster recovery planning.

Observations

1. The **highest risks** for TMC are related to **ransomware, IoT device exploitation, and insider misuse**, which can cause both production and financial disruptions.
2. Lack of **centralized log monitoring** and **limited incident response capability** increases the potential dwell time of attackers.
3. The **human factor** remains the weakest link, emphasizing the need for continuous awareness training and access control enforcement.
4. Supply chain dependencies represent a **rising cybersecurity concern**, as compromised vendor software or hardware can introduce backdoors into the network.

Conclusion

The Threat and Vulnerability Assessment establish a clear risk landscape for Titan Manufacturing Corporation. It identifies **critical operational and information security weaknesses** that must be addressed through a well-defined **Security Controls Plan**, which will be developed in the next phase.

Mitigation efforts should prioritize:

- Enhanced **endpoint protection and patch management**,
- Strengthened **access control and authentication**,
- Implementation of **IoT and OT network segmentation**, and
- Continuous **monitoring and employee training**.

By proactively addressing these vulnerabilities, TMC can build a **resilient and secure manufacturing ecosystem** capable of defending against modern cyber threats.

Security Controls Plan

Overview

In response to the threats and vulnerabilities identified in the previous phase, Titan Manufacturing Corporation (TMC) must adopt a **multi-layered defense approach** that integrates **physical**, **technical**, and **administrative** security controls.

This plan follows the guiding principles of the **NIST Cybersecurity Framework (CSF)** — *Identify, Protect, Detect, Respond, Recover* — and the **ISO/IEC 27001:2022** Information Security Management System (ISMS) standard. Together, these frameworks ensure that TMC establishes not only preventive measures but also **detective** and **corrective** mechanisms to maintain business continuity and operational safety.

Objectives of the Security Controls Plan

1. Protect the confidentiality, integrity, and availability of TMC's information and operational systems.
2. Reduce the likelihood and impact of cybersecurity incidents targeting IT and OT infrastructures.
3. Establish standardized procedures and roles for cybersecurity governance.
4. Ensure compliance with relevant laws, regulations, and industry standards.
5. Promote a security-aware culture across all departments and levels of the organization.

Classification of Security Controls

The following subsections detail the **Physical**, **Technical**, and **Administrative** controls designed for Titan Manufacturing Corporation's specific environment.

A. Physical Security Controls

Physical controls protect facilities, assets, and personnel from unauthorized access or environmental hazards. In a manufacturing setting, these measures are critical for ensuring both safety and security.

Control Measure	Description	Purpose / Expected Outcome
Perimeter Security and Access Control	Implement RFID or biometric-based entry systems at main gates, server rooms, and control centers.	Prevent unauthorized physical access to sensitive areas.
24/7 CCTV Monitoring System	Maintain surveillance coverage across production lines, data centers, and administrative offices. Store recordings for at least 90 days.	Deter insider threats and provide post-incident evidence.
Security Personnel and Patrols	Station trained guards in critical locations and conduct periodic rounds.	Immediate response to unauthorized or suspicious physical activity.
Environmental Controls (Fire, Power, HVAC)	Equip server rooms with fire suppression systems, UPS, and temperature/humidity monitoring.	Prevent physical damage and data loss due to environmental factors.
Visitor Management System	Require pre-approved visitor access, identity verification, and escorts in restricted zones.	Protect against industrial espionage or unauthorized entry.
Asset Tagging and Inventory Checks	Assign asset IDs and conduct quarterly physical audits.	Detect missing or tampered hardware devices.

B. Technical Security Controls

Technical controls address vulnerabilities in digital systems, networks, and applications. These are essential for defending against cyberattacks and ensuring continuous protection of both IT and OT environments.

Control Measure	Description	Purpose / Expected Outcome
Network Segmentation (IT vs. OT)	Separate business systems from industrial networks using VLANs and firewalls.	Prevent lateral movement from compromised IT systems to production systems.
Intrusion Detection and	Deploy network- and host-based monitoring solutions for anomaly detection and intrusion blocking.	Enable early detection and mitigation of cyberattacks.

Prevention System (IDPS)		
Multi-Factor Authentication (MFA)	Enforce MFA for VPN, remote access, and privileged accounts.	Reduce risk of unauthorized access even if credentials are compromised.
Regular Patch Management	Establish monthly patch cycles for operating systems, firmware, and applications.	Mitigate exploitation of known vulnerabilities.
Endpoint Protection and EDR	Install advanced antivirus and endpoint detection and response (EDR) agents on all devices.	Detect, contain, and remediate malware threats.
Data Encryption (At Rest and In Transit)	Use AES-256 for database and file encryption; enforce HTTPS/TLS 1.3 for communications.	Protect data confidentiality and integrity.
Security Information and Event Management (SIEM)	Aggregate and analyze logs from all critical systems for real-time threat monitoring.	Centralized visibility and faster incident detection.
Backup and Disaster Recovery System	Maintain daily incremental and weekly full backups stored offline or in secure cloud.	Ensure rapid restoration in case of ransomware or system failure.
Email Security Gateway	Implement anti-phishing, spam filtering, and attachment sandboxing.	Defend against social engineering and email-based attacks.
IoT and SCADA Hardening	Restrict remote access to control systems, use encrypted communication protocols (e.g., MQTT over TLS), and disable default accounts.	Secure operational devices and prevent ICS exploitation.

C. Administrative Security Controls

Administrative controls govern human behavior, policy enforcement, and organizational processes. They ensure that security is systematically managed across departments.

Control Measure	Description	Purpose / Expected Outcome
Information Security Policy (ISP)	Develop and enforce an organization-wide cybersecurity policy aligned with ISO 27001.	Establish formal governance and accountability.
Access Control and Account	Apply Role-Based Access Control (RBAC) and periodic review of privileges.	Ensure least-privilege access and timely revocation for ex-employees.

Management Policy		
Security Awareness and Training Program	Conduct mandatory quarterly cybersecurity training for all employees.	Improve human firewall against phishing and social engineering.
Incident Response Plan (IRP)	Define detection, reporting, escalation, and response procedures for security events.	Enable rapid, coordinated, and effective response.
Vendor and Supply Chain Security Policy	Require third-party vendors to comply with TMC's cybersecurity standards and undergo audits.	Reduce supply chain risks and third-party vulnerabilities.
Data Privacy and Classification Policy	Classify data based on sensitivity (Critical, Confidential, Internal).	Ensure proper data handling and legal compliance (RA 10173).
Periodic Security Audits and Penetration Testing	Engage certified professionals to test system resilience annually.	Identify and remediate vulnerabilities before exploitation.
Business Continuity and Disaster Recovery Plan	Maintain documented recovery steps, communication lines, and responsibilities.	Minimize downtime and maintain essential operations.
Change Management Process	Approve and log all system and network configuration changes.	Prevent accidental or unauthorized system alterations.
Compliance and Legal Oversight	Appoint a compliance officer to monitor adherence to local and international cybersecurity regulations.	Maintain regulatory compliance and avoid penalties.

Control Mapping to Frameworks

Framework Domain	Key Controls Implemented
NIST CSF – Identify	Asset Inventory, Risk Assessment, Access Control Policy
NIST CSF – Protect	MFA, Encryption, Security Awareness Training, Firewalls
NIST CSF – Detect	SIEM, IDS/IPS, Log Monitoring
NIST CSF – Respond	Incident Response Plan, Escalation Procedures
NIST CSF – Recover	Disaster Recovery, Backup Management, BCP
ISO 27001 Controls	A.5 (Policies), A.9 (Access Control), A.10 (Cryptography), A.12 (Operations Security), A.16 (Incident Management)

Implementation Roadmap

Phase	Timeline	Key Activities
Phase 1 – Immediate (0–3 months)	Short-term mitigation	Patch critical systems, deploy MFA, implement network segmentation, and initiate security training.
Phase 2 – Medium Term (3–6 months)	Reinforcement & optimization	Deploy SIEM, standardize backup routines, and enforce vendor security policies.
Phase 3 – Long Term (6–12 months)	Continuous improvement	Conduct annual penetration tests, review ISMS, and upgrade endpoint protection infrastructure.

Expected Outcomes

By implementing this layered security controls plan, Titan Manufacturing Corporation will achieve the following outcomes:

- Strengthened **resilience against cyberattacks** targeting IT and OT systems.
- Enhanced **visibility** into security events and potential intrusions.
- Improved **data protection** through encryption and access control.
- Sustained **compliance** with national and international regulations.
- A **culture of cybersecurity awareness** across all levels of the organization.

Conclusion

The Security Controls Plan provides the structural foundation for protecting Titan Manufacturing Corporation's critical assets. It ensures that every layer — from the factory floor to executive offices — is equipped with the necessary safeguards to prevent, detect, and respond to cyber threats.

The next phase, **Cryptography & Authentication Demo**, will translate some of these technical controls into a **practical web-based simulation** demonstrating secure login, encryption, and data protection mechanisms relevant to TMC's operations.

Cryptography & Authentication Demo

Overview

This phase demonstrates the practical implementation of Titan Manufacturing Corporation's (TMC) cybersecurity controls through a web-based prototype entitled **TMC Secure OT–IT Data Transfer and Encryption System**.
The system simulates how TMC protects operational (OT) data when transferring it into information technology (IT) systems by enforcing secure authentication, robust encryption, and continuous auditing.

The demo directly translates the company's cybersecurity plan into a working model that applies **AES-GCM 256 encryption**, **role-based authentication and authorization**, and **comprehensive event logging**—all aligned with the organization's data protection and compliance requirements under the **Data Privacy Act of 2012 (RA 10173)** and **ISO/IEC 27001** security controls.

System Architecture and Flow

High-Level Data Flow

1. **OT Operator Upload** – The operator logs in and uploads a validated Excel file representing machine or production data.
2. **Validation** – The file headers are canonicalized and checked for required columns and at least one data row.
3. **Encryption** – Data is encrypted using **AES/GCM/NoPadding (AES-256)**. An `EncryptedFile` entity is persisted containing ciphertext, IV, authentication tag, and metadata.
4. **File Assignment** – The **Admin** assigns the encrypted file to an **IT Analyst**, granting implicit *DECRYPT* permission.
5. **Decryption** – The analyst accesses assigned files, decrypts and downloads them after GCM tag and integrity verification.
6. **Compliance Oversight** – The **Compliance Officer** exports audit logs for reporting; the **CISO** reviews global key performance indicators (KPIs).

7. **Audit & Incident Logging** – Every action triggers an `AuditLog` or `IncidentLog` entry, ensuring traceability and accountability.

This flow mirrors TMC's operational data lifecycle from **factory floor (OT)** to **enterprise IT**, implementing confidentiality, integrity, and accountability controls at each stage.

Encryption and Integrity Model

Components

`EncryptionService`, `DecryptionService`, `CryptoConfig`, `HashUtil`, and the `EncryptedFile` entity collectively manage the cryptographic lifecycle.

Algorithmic Details

Parameter	Implementation
Cipher	AES/GCM/NoPadding (AES-256)
Initialization Vector (IV)	12 bytes random per encryption
Authentication Tag	Automatically generated and validated by GCM
Integrity Hash	SHA-256 hash of ciphertext stored as fileHash
Key Reference	aesKeyRef links encrypted files to active AES key
Metadata Stored	filename, contentType, size, ciphertext, IV, fileHash, aesKeyRef, algorithm, uploader, timestamps

During decryption, the GCM authentication tag is validated to ensure message integrity. The additional SHA-256 hash provides secondary verification against tampering, thus enforcing a dual-layer integrity assurance mechanism.

Authentication and Session Security

Components

`SecurityConfig`, `CustomUserDetailsService`, `RoleBasedAuthSuccessHandler`, and `AuthEventListener`.

Features

- **Credential Verification:** Username/email + password authenticated via **BCrypt** hash comparison.
- **Event Auditing:** Login successes and failures recorded as `AuditLog` entries.
- **Account Lockout:** After consecutive failures, accounts are temporarily disabled, and a corresponding `IncidentLog` entry is created.
- **Session Security:** Idle sessions auto-expire; CSRF protection is enabled on all form submissions.

These mechanisms ensure secure access while reducing exposure to brute-force attacks and session hijacking.

Authorization and Role-Based Access

Access to every endpoint is governed by **Role-Based Access Control (RBAC)** enforced through `SecurityConfig` and `DashboardResolver`.

Role	Authorized Endpoints	Key Privileges
OT Operator	/api/ot/**	Upload and view own encrypted files
IT Analyst	/api/analyst/**	Decrypt and analyze assigned datasets
Administrator	/api/admin/**	Manage users, file assignments, and monitor logs
Compliance Officer	/api/compliance/**	Read-only access to audit and incident logs
CISO	/api/ciso/**	View global metrics and KPIs

Each user accesses an individualized dashboard filtered by account ID, ensuring complete isolation of datasets. Unauthorized attempts trigger the `LoggingAccessDeniedHandler`, which logs the incident with contextual metadata (actor, IP address, timestamp).

Logging and Audit Trail

Two complementary entities, `AuditLog` and `IncidentLog`, record all operational and security-relevant activities.

AuditLog Events

LOGIN_SUCCESS, LOGOUT, FILE_UPLOAD_STORED, VALIDATION_FAILED, DECRYPTION_SUCCESS, ADMIN_ACTION, and LOGS_EXPORTED.

IncidentLog Events

Unauthorized access attempts, account lockouts, integrity validation failures, and any anomalous behavior.

Log Enrichment

`LogHelper` appends contextual data such as actor identity, IP address, and session ID for forensic accuracy.

The **Compliance Officer** can export logs for reporting, while the **CISO** reviews aggregated KPIs such as number of incidents, response times, and compliance rate.

File Assignment and Permission Model

`AssignmentService` manages controlled file distribution:

- **Assignment** – Admin links an `EncryptedFile` to one or more analysts.
- **Permissions** – Default permission: *DECRYPT* only.

- **Revocation** – Assignments can be revoked (`status → REVOKED`) or set to expire automatically.
- **Auditability** – Each change generates an `ADMIN_ACTION` log entry.

This model demonstrates segregation of duties: uploaders cannot decrypt, analysts cannot upload, and administrators cannot view data contents.

Data Validation and Pre-Processing

Before encryption, uploaded Excel files undergo schema validation by the `ExcelValidator` component.

- **Header Canonicalization:** Converts headers to lowercase and removes non-alphanumeric characters.
- **Schema Enforcement:** Verifies that all required headers are present.
- **Data Integrity Check:** Ensures that at least one valid data row exists.
- **Validation Result:** Returned as structured feedback, logged for auditing.

This prevents malicious or malformed data injection from the OT layer into the IT environment.

Dashboards and Monitoring Interfaces

Each role operates within a dedicated dashboard:

- **OT Operator:** Upload history and encryption status.
- **IT Analyst:** Assigned datasets with decrypt/download controls.
- **Administrator:** Incident and audit logs with pagination controls (`incPage`, `audPage`).
- **Compliance Officer:** Read-only log viewer with export option.
- **CISO:** KPI overview—incident trends, compliance metrics, user statistics.

Severity levels are visually coded (Critical = red, High = orange, Medium = gray, Low = light), enhancing situational awareness.

Security Controls Implemented

Control Category	Implementation	Corresponding Standard
Password Hashing	BCrypt algorithm	ISO 27001 A.9.4.3
CSRF Protection	Enabled on all POST forms	OWASP Top 10 A05
RBAC Enforcement	Role-based URL mapping and controller guards	NIST AC-2
Account Lockout	Failure count → temporary lock	NIST IA-5
Encryption at Rest	AES-256 GCM with per-file IV	ISO 27001 A.10
Integrity Verification	GCM auth tag + SHA-256 hash	NIST SC-13
Audit Trail	Structured AuditLog + IncidentLog with context	ISO 27001 A.12
Data Segregation	Per-user dashboards and file ownership enforcement	Principle of Least Privilege

Summary and Significance

The implemented demo successfully demonstrates TMC's applied cybersecurity mechanisms for protecting industrial data:

- **Confidentiality:** Achieved through AES-256 GCM encryption with unique IVs per file.
- **Integrity:** Maintained through GCM authentication tags and SHA-256 hashing.
- **Authentication & Authorization:** Managed by BCrypt password hashing and role-based routing.
- **Accountability:** Realized via structured audit and incident logs.
- **Traceability:** Enabled through contextual metadata in every recorded event.

This phase validates the organization's technical capability to protect sensitive operational data while maintaining strict separation of duties across its personnel. It exemplifies how **information assurance principles**—confidentiality, integrity, availability, and accountability—are effectively integrated into TMC's digital manufacturing ecosystem.

Legal & Ethical Compliance Measures

Overview

Titan Manufacturing Corporation (TMC) recognizes that cybersecurity is not solely a technical concern but also a **legal, regulatory, and ethical responsibility**.
As a manufacturing enterprise operating within the Philippines and serving international partners, TMC is bound by national cybersecurity laws, data protection statutes, and globally recognized security frameworks.

This section outlines the company's compliance with **legal mandates**, adherence to **industry standards**, and promotion of **ethical conduct** among employees, vendors, and partners. The objective is to ensure that TMC's cybersecurity posture not only defends against attacks but also upholds the **principles of accountability, transparency, and data stewardship.**

Applicable Laws and Regulations

A. Republic Act No. 10173 — Data Privacy Act of 2012 (Philippines)

The Data Privacy Act (DPA) governs the collection, processing, and protection of personal information.
TMC commits to compliance by:

- Appointing a **Data Protection Officer (DPO)** responsible for ensuring adherence to DPA principles.
- Implementing **data subject rights**: access, correction, deletion, and objection.
- Conducting **Privacy Impact Assessments (PIA)** on systems handling employee, customer, and vendor data.
- Using **data minimization** and **purpose limitation** to collect only necessary personal information.
- Ensuring **secure disposal and anonymization** of obsolete records.

Legal Reference: National Privacy Commission (NPC) – Implementing Rules and Regulations of RA 10173.

B. Republic Act No. 10175 — Cybercrime Prevention Act of 2012

This law criminalizes offenses such as unauthorized access, data interference, and system sabotage.
TMC enforces the following compliance measures:

- Enabling **access control systems** to prevent unauthorized logins or data breaches.
- Preserving **digital evidence** during incident investigations following NPC and NBI guidelines.
- Enforcing **employee code of conduct** prohibiting cyber offenses (e.g., misuse of credentials, sharing of classified data).
- Reporting incidents involving cybercrimes to appropriate authorities (e.g., NBI Cybercrime Division).

C. Republic Act No. 8792 — E-Commerce Act of 2000

Ensures the legality of electronic transactions and protection of online data integrity.
TMC supports compliance through:

- Use of **digital signatures and certificates** for internal approvals.
- Maintaining **audit logs** for all digital business transactions.
- Ensuring **data integrity** and non-repudiation of electronic communications.

D. Republic Act No. 10844 — Department of Information and Communications Technology (DICT) Act of 2015

This act empowers the DICT to oversee ICT policy and infrastructure security.
TMC aligns by:

- Adopting **DICT Cybersecurity Management System (CMS)** guidelines for enterprise-level protection.
- Participating in **information sharing** with DICT's National Computer Emergency Response Team (NCERT) for threat intelligence.

E. International Standards and Frameworks

Standard / Framework	Description	Compliance Application in TMC
ISO/IEC 27001:2022	Information Security Management System (ISMS) standard defining controls for confidentiality, integrity, and availability.	TMC implements ISMS controls such as policy creation, access management, and continuous monitoring.
NIST Cybersecurity Framework (CSF)	U.S.-based voluntary framework focusing on Identify–Protect–Detect–Respond–Recover.	Serves as structural reference for TMC's overall cybersecurity strategy.
General Data Protection Regulation (GDPR)	European Union regulation for data protection and privacy.	Adopted as a best practice for handling data from international partners.
ISO/IEC 22301:2019	Business Continuity Management System (BCMS) standard.	Ensures TMC maintains resilience and recovery capability during incidents.

Corporate Cybersecurity Governance

TMC integrates compliance through a structured **Cybersecurity Governance Framework**, ensuring that accountability and responsibility are clearly defined.

Governance Structure

Role / Function	Responsibilities
Board of Directors / Executive Management	Approve cybersecurity budgets, policies, and risk appetite. Oversee ISMS implementation.
Chief Information Security Officer (CISO)	Lead the cybersecurity program, enforce compliance with laws and standards, and report directly to executives.

Data Protection Officer (DPO)	Ensure compliance with the Data Privacy Act, conduct PIAs, and handle data subject concerns.
IT Security Team / SOC Analysts	Monitor threats, analyze incidents, and maintain logs for audit and forensic purposes.
Department Managers	Ensure employee adherence to cybersecurity and privacy policies.
All Employees	Practice security awareness, report suspicious activities, and protect company data.

Ethical Principles in Cybersecurity

Ethics are central to TMC's cybersecurity operations. All personnel are required to follow standards of **integrity, confidentiality, accountability, and professional conduct** in handling information and systems.

Ethical Principle	Implementation at TMC
Integrity	Employees must act honestly and avoid manipulation or falsification of data.
Confidentiality	Sensitive information (financial, operational, or personal) must never be disclosed to unauthorized parties.
Accountability	Every system access and data modification is traceable to an authorized user.
Non-maleficence	IT staff are prohibited from conducting unauthorized testing, data extraction, or disruption of systems.
Transparency	Any data collection or monitoring process must be disclosed to affected parties as required by law.
Professional Competence	Personnel involved in cybersecurity must continuously enhance their knowledge through training and certification.

Ethical Compliance in Third-Party and Vendor Relationships

Given TMC's reliance on third-party suppliers, vendors, and maintenance partners, the company enforces ethical and legal obligations across its supply chain:

- Vendors must **sign Non-Disclosure Agreements (NDAs)** and comply with TMC's internal data protection policies.
- Third-party software and equipment providers are required to **undergo security vetting** and provide **vulnerability management reports**.

- Contracts include **data protection clauses** ensuring shared accountability in the event of a data breach.
- TMC discourages unethical business practices such as intellectual property theft, counterfeit equipment, or unauthorized system modifications.

Data Handling and Privacy Practices

TMC enforces data privacy and protection throughout the data lifecycle:

Data Lifecycle Stage	Compliance Measures
Collection	Collect only necessary personal and operational data, with informed consent.
Storage	Encrypt sensitive data using AES-256 and store only on approved servers.
Access	Implement least-privilege principles and multi-factor authentication.
Processing	Ensure lawful and transparent data use, aligned with declared purpose.
Sharing	Share data only with authorized internal users or approved partners under NDAs.
Retention & Disposal	Retain data only as long as legally necessary; securely delete or anonymize obsolete records.

Compliance Auditing and Continuous Improvement

To maintain long-term compliance, TMC establishes a **Cybersecurity and Privacy Compliance Audit Program**:

1. **Annual Internal Audits** – Evaluate adherence to ISMS policies and laws.
2. **Third-Party Security Audits** – Conducted by independent certified auditors.
3. **Compliance Metrics** – Use KPIs such as number of incidents, audit findings, and training completion rates.
4. **Corrective and Preventive Actions (CAPA)** – Address identified gaps through documented remediation steps.
5. **Continuous Training** – Regular workshops on legal updates and ethical decision-making.

Reporting and Accountability

- Any data breach or security incident must be reported to the **Data Protection Officer** and escalated to the **National Privacy Commission (NPC)** within **72 hours**, as required by law.
- Employees must report any unethical conduct or security violation through a **confidential whistleblowing mechanism**.
- Violations of cybersecurity or ethical policies are subject to disciplinary actions under company policy and applicable laws.

Conclusion

Legal and ethical compliance is a foundational pillar of TMC's cybersecurity strategy. By adhering to the **Data Privacy Act**, **Cybercrime Prevention Act**, and **international standards**, TMC not only protects its assets but also builds **trust** among employees, customers, and partners.

The company's commitment to ethical behavior ensures that cybersecurity efforts are conducted responsibly, transparently, and in alignment with the principles of **corporate governance and professional integrity.**

Incident Handling & Reporting Plan

Overview

In a manufacturing environment where downtime directly affects production and revenue, **rapid and coordinated incident response** is critical.
Titan Manufacturing Corporation (TMC) recognizes that no organization can be completely immune to cyber threats, but through a robust **Incident Handling & Reporting Plan**, it can minimize the impact, ensure business continuity, and protect its critical assets.

This plan establishes the **standard procedures, roles, and communication channels** to be followed during any cybersecurity incident affecting the company's IT or OT systems. It also integrates **legal compliance**, **forensic readiness**, and **continuous improvement** based on lessons learned.

Objectives

1. Provide a **systematic and repeatable process** for managing cybersecurity incidents.
2. Reduce the **operational and financial impact** of security breaches.
3. Ensure **timely communication and escalation** to responsible personnel and authorities.
4. Preserve **digital evidence** for investigation and compliance with regulatory requirements.
5. Improve organizational readiness and resilience through regular testing and reviews.

Scope

This plan applies to:

- All **IT systems**, including servers, databases, email, ERP, and HRIS.

- All **OT systems**, such as SCADA, PLCs, and IoT devices.
- **Employees, contractors, and third-party vendors** with system access.
- Any cybersecurity-related event that threatens the **confidentiality, integrity, or availability** of TMC data and operations.

Incident Response Framework

TMC's incident handling process follows the **six-phase model** derived from **NIST SP 800-61**:

Phase	Description
1. Preparation	Establish and maintain incident response policies, tools, and training.
2. Detection & Analysis	Identify and confirm potential incidents through monitoring systems and user reports.
3. Containment	Isolate affected systems to prevent further damage or data leakage.
4. Eradication	Remove malicious components and patch exploited vulnerabilities.
5. Recovery	Restore systems to normal operations and verify system integrity.
6. Lessons Learned	Document the incident, analyze root causes, and update procedures to prevent recurrence.

Roles and Responsibilities

Role / Team	Primary Responsibilities
Incident Response Manager (CISO or IT Head)	Oversees entire response process, authorizes containment actions, and reports to executive management.
Security Operations Center (SOC) Team	Monitors alerts, performs initial triage, and conducts digital forensics and log analysis.
System / Network Administrators	Implement containment, patching, and system restoration activities.
Data Protection Officer (DPO)	Assesses privacy implications and notifies the National Privacy Commission (NPC) when required.
Department Heads / Managers	Coordinate with IT to ensure minimal disruption in their respective units.

Communications Officer / HR	Handles internal and external communication, ensuring consistent and accurate public messaging.
Third-Party Vendors / Contractors	Support investigation and resolution if their systems or services are involved.

Incident Classification Levels

To ensure an appropriate and proportional response, incidents are classified by **severity** and **scope**.

Level	Classification	Description	Response Priority
Level 1 – Minor	Localized issue	Minimal operational impact; quickly contained (e.g., isolated malware on one PC).	Handled by SOC within the same day.
Level 2 – Moderate	Department-level issue	Affects multiple systems or users; may cause service disruption.	Escalate to CISO; containment within 4 hours.
Level 3 – Major	Organization-wide incident	Widespread system compromise, ransomware, or critical data breach.	Activate full Incident Response Team; notify NPC and DICT within 72 hours.

Incident Detection and Analysis

Detection Sources

- **Security Information and Event Management (SIEM)** alerts.
- **Intrusion Detection Systems (IDS)** and **firewalls**.
- **User or employee reports** (phishing, suspicious activity, etc.).
- **Vendor notifications** or threat intelligence feeds.
- **System behavior anomalies**, such as sudden CPU spikes or data exfiltration alerts.

Incident Verification Process

1. SOC validates alert authenticity and severity.
2. Logs and evidence are preserved in a secure, read-only format.

3. Incident Response Manager is notified for classification and action authorization.

Containment, Eradication, and Recovery

Containment Strategies

- **Short-Term Containment:** Isolate affected devices or networks (e.g., disable network port, disconnect endpoint).
- **Long-Term Containment:** Apply temporary firewall rules or network segmentation to prevent re-infection.
- Disable compromised accounts and revoke access tokens.

Eradication Steps

- Identify root cause and remove all traces of malware or malicious code.
- Patch vulnerable systems and update security configurations.
- Scan systems to ensure no residual compromise exists.

Recovery Actions

- Restore systems from verified clean backups.
- Gradually reconnect restored systems to the production network.
- Closely monitor for any recurring suspicious activity for at least 72 hours post-recovery.

Communication and Reporting Procedures

Internal Communication Flow

1. Employee or system detects an anomaly → reports to SOC.
2. SOC verifies and logs the incident → escalates to Incident Response Manager.
3. If personal data is affected → DPO evaluates breach notification requirements.
4. Management is informed of the potential business impact.

External Reporting Obligations

- **National Privacy Commission (NPC):** Notify within 72 hours if the incident involves personal data breach.
- **DICT or Law Enforcement:** Notify critical or large-scale attacks (e.g., ransomware, cyber extortion).
- **Clients and Partners:** Informed when contractual or operational dependencies are affected.

Incident Handling Report Form

Field	Description
Incident ID:	Unique tracking code for reference.
Incident Type:	e.g., Malware, Phishing, Unauthorized Access, Data Breach.
Date & Time Detected:	Timestamp of initial detection.
Detected By:	Name and position of reporter.
Systems Affected:	Servers, networks, or devices impacted.
Description of Incident:	Summary of what occurred.
Actions Taken:	Containment, eradication, recovery steps executed.
Status:	Ongoing, Resolved, Under Investigation.
Reported To:	Responsible authority or personnel.
Lessons Learned:	Improvements identified post-incident.

Forensic Readiness and Evidence Handling

To ensure legal defensibility and support post-incident investigation:

- All digital evidence (logs, memory dumps, emails) must be collected **forensically** and stored securely.
- Chain-of-custody documentation is required for every evidence transfer.
- Only authorized personnel are permitted to handle or analyze digital evidence.
- Integrity of evidence must be maintained using cryptographic hash verification (e.g., SHA-256).

Post-Incident Review (Lessons Learned)

After each major incident:

1. The Incident Response Team conducts a **post-mortem meeting** to review actions and outcomes.
2. Identify **root causes**, including process, technology, or human errors.
3. Recommend improvements for **policy updates, security controls, or training programs**.
4. Update **Incident Response documentation** and **business continuity procedures** accordingly.
5. Share relevant findings (without sensitive data) with DICT or industry information sharing partners.

Integration with Business Continuity

Incident handling is tightly linked with TMC's **Business Continuity Plan (BCP)** and **Disaster Recovery (DR)** strategy:

- Critical systems identified in the **BIA (Phase 7)** have predefined **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)**.
- Incident Response actions trigger automatic escalation to **BCP activation** if production downtime exceeds thresholds.
- Communication with **key stakeholders** and **external vendors** is governed by continuity protocols.

Testing and Continuous Improvement

TMC ensures readiness by conducting:

- **Tabletop exercises** (quarterly) simulating phishing, ransomware, or insider threat scenarios.
- **Full-scale incident simulations** (annually) involving all departments.

- **After-action reports (AARs)** to evaluate performance metrics and response times.
- Continuous update of tools, policies, and playbooks based on evolving threat intelligence.

Conclusion

The **Incident Handling & Reporting Plan** equips Titan Manufacturing Corporation with the structured capability to **detect, contain, and recover** from cybersecurity incidents efficiently.
By aligning with international standards and enforcing legal reporting requirements, TMC ensures that its **response is swift, coordinated, and compliant**.

This systematic approach minimizes downtime, protects sensitive information, and reinforces the organization's commitment to **operational resilience and regulatory integrity**.

Business Impact Analysis (BIA)

Overview

A **Business Impact Analysis (BIA)** is a crucial component of Titan Manufacturing Corporation's (TMC) overall **Information Assurance and Business Continuity strategy.** It provides a structured assessment of how cybersecurity incidents, natural disasters, or operational failures could affect critical business functions, financial stability, and customer confidence.

This BIA evaluates potential **threat scenarios**, measures **financial and operational impacts**, and establishes **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)** to guide effective disaster recovery and continuity planning.

The analysis is aligned with **ISO/IEC 22301:2019** (Business Continuity Management Systems) and complements the **Incident Handling & Reporting Plan** detailed in the previous phase.

Objectives

1. Identify and prioritize critical assets and business processes essential to TMC's operations.
2. Assess potential financial and operational impacts resulting from system disruptions or breaches.
3. Define acceptable recovery timeframes and data loss tolerances (RTO/RPO).
4. Recommend recovery strategies that ensure operational continuity and regulatory compliance.
5. Strengthen the organization's resilience against disruptive cyber or physical incidents.

Methodology

The BIA follows a structured three-step approach:

1. **Data Collection** – Review of TMC's business processes, IT/OT assets, and dependencies.
2. **Impact Assessment** – Evaluation of the potential effects of disruption based on financial loss, downtime, and reputational damage.
3. **Recovery Planning** – Determination of recovery priorities, resource needs, and response timelines.

Inputs were gathered from department heads, IT system administrators, and financial management to ensure that both technical and business perspectives were captured.

Critical Business Functions

Business Function	Description	Department / Owner	Dependency
Manufacturing Operations (SCADA / PLC)	Controls the automated production lines for automotive parts and heavy equipment components.	Production Division	SCADA Servers, PLCs, IoT Sensors
Enterprise Resource Planning (ERP)	Manages inventory, orders, procurement, and accounting.	IT & Finance Division	ERP Servers, Database Systems
Human Resource Information System (HRIS)	Maintains employee records, payroll, and attendance.	HR Department	HRIS Application, Database
Email and Communication Systems	Enables internal and external communication.	IT Division	Email Server, Network Infrastructure
Customer and Vendor Management System	Manages client orders, supplier contracts, and logistics.	Sales & Procurement	Web Portal, Vendor Database
Backup and Disaster Recovery System	Ensures data protection and restoration capability.	IT Division	Backup Servers, Cloud Storage
Physical Access Control and CCTV	Controls facility access and monitors site security.	Security Office	RFID System, Surveillance Servers

Threat Scenarios and Impact Assessment

Asset / Process	Threat Scenario	Financial Impact	Operational Impact	Recovery Strategy
Manufacturing Control System (SCADA/PLC)	Ransomware attack halts production for 48 hours.	₱3.5 million in lost production output and penalties.	Severe – full production downtime.	Isolate affected network, restore from clean backups, switch to manual fallback process.
ERP System	SQL injection leading to data corruption.	₱1.2 million in reprocessing and data recovery costs.	High – delay in financial and procurement operations.	Apply secure backup restoration, implement web application firewall (WAF).
Email Server	Phishing campaign causes credential compromise.	₱500,000 potential loss due to fraudulent transactions.	Medium – temporary communication disruption.	Reset credentials, enhance MFA, deploy advanced email filtering.
IoT Devices and Sensors	Malware causes incorrect readings on production line.	₱800,000 in defective materials and recall costs.	High – product quality and safety risk.	Patch firmware, deploy IoT security gateway, enforce segmentation.
Customer & Vendor Database	Data breach exposing sensitive client information.	₱2 million in regulatory fines and reputational loss.	High – loss of customer trust and operational delay.	Notify NPC, enforce data breach response, apply AES-256 re-encryption and access audits.
Backup Server	Corruption or deletion of backup files.	₱600,000 due to data re-entry and extended downtime.	High – inability to recover systems promptly.	Maintain offsite backups, regular verification tests, and encryption.
Physical Access Control System	Unauthorized entry due to RFID cloning.	₱200,000 in equipment theft and security breach costs.	Low – localized incident.	Upgrade to encrypted RFID or biometric authentication; strengthen CCTV coverage.

Financial and Operational Impact Analysis

Financial Impact

- **Direct Losses:** Production stoppage, data restoration costs, and contract penalties.
- **Indirect Losses:** Reputational damage, client compensation, and regulatory fines.
- **Estimated Maximum Tolerable Downtime (MTD):** 72 hours for production operations before severe financial consequences occur.

Operational Impact

- **Critical:** Disruption in SCADA/PLC operations (immediate loss of production).
- **Significant:** ERP, IoT, and backup system compromise.
- **Moderate:** Email and access control system outages.
- **Minor:** HRIS downtime for less than one business day.

Recovery Time and Point Objectives (RTO / RPO)

System / Process	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)	Priority Level
Manufacturing Control System (SCADA/PLC)	8 hours	1 hour	**Critical**
ERP System	12 hours	4 hours	**High**
IoT Monitoring System	12 hours	2 hours	**High**
Customer & Vendor Database	24 hours	6 hours	**High**
Email and Communication Systems	24 hours	8 hours	**Medium**
Backup and Recovery Infrastructure	4 hours	0 hour (real-time replication)	**Critical**
HRIS	48 hours	12 hours	**Medium**
Access Control / CCTV Systems	72 hours	24 hours	**Low**

Prioritization of Recovery Activities

1. **Phase 1 (0–8 hours):**
    a. Restore SCADA, PLC, and backup systems to ensure production continuity.
    b. Activate manual process fallback if automation remains compromised.
2. **Phase 2 (8–24 hours):**
    a. Recover ERP and IoT systems for material tracking, logistics, and reporting.
    b. Verify integrity of production data and re-synchronize with ERP.
3. **Phase 3 (24–48 hours):**
    a. Reestablish email, HRIS, and communication systems for business coordination.
    b. Resume standard IT operations once confirmed that they are stable.
4. **Phase 4 (48–72 hours):**
    a. Conduct full validation, patching, and post-incident documentation.
    b. Notify external stakeholders of operational restoration.

Business Continuity and Recovery Strategies

Category	Strategy	Description
Data Protection	Regular offline and cloud backups	Maintain secure redundant backups in separate physical locations.
System Redundancy	Deploy high-availability (HA) servers	Minimize downtime for ERP and SCADA systems.
Alternate Site Operations	Maintain secondary recovery site	Allow partial manufacturing continuation in case of facility outage.
Manual Fallback Procedures	Documented production fallback plans	Enable minimal operations if automation systems fail.
Vendor Coordination	Activate vendor emergency response	Coordinate with SCADA and ERP vendors for support during incident recovery.
Communication Plan	Establish pre-approved communication templates	Ensure timely and accurate stakeholder updates.
Insurance Coverage	Cyber liability and business interruption insurance	Offset potential financial losses due to cyberattacks or downtime.

Key Observations

1. The **Manufacturing Control System (SCADA/PLC)** and **Backup Infrastructure** are the **most critical assets**, demanding the shortest RTO and RPO values.
2. The **ERP system** serves as the backbone for financial and logistics operations — a prolonged outage can cascade into other processes.
3. **IoT vulnerabilities** can cause operational disruption and product defects, requiring strict patch management and monitoring.
4. Non-technical disruptions, such as **communication breakdowns** or **employee unawareness**, can worsen incident recovery times.
5. A **clear chain of command** and regular continuity drills are vital to meet recovery objectives.

Conclusion

The Business Impact Analysis (BIA) confirms that **Titan Manufacturing Corporation's operational continuity** heavily depends on secure and reliable IT/OT integration.
The company's resilience lies in its ability to **recover critical systems quickly**, **limit financial exposure**, and **maintain customer trust** even in the event of severe cyber disruptions.

By adopting the identified **recovery strategies**, enforcing **redundancy and backup policies**, and integrating these findings into the **Incident Handling Plan**, TMC ensures that it can **withstand and recover** from both cyber and physical incidents with minimal impact to operations and revenue.

References

1. National Privacy Commission (NPC), Republic of the Philippines — Implementing Rules and Regulations of Republic Act No. 10173 (Data Privacy Act of 2012).
2. Republic Act No. 10175 — Cybercrime Prevention Act of 2012 (Philippines).
3. Republic Act No. 8792 — E-Commerce Act of 2000 (Philippines).
4. Republic Act No. 10844 — Department of Information and Communications Technology (DICT) Act of 2015 (Philippines).
5. NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology.
6. NIST Special Publication 800-61 Rev. 2, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology.
7. NIST Cybersecurity Framework (CSF) — *Identify, Protect, Detect, Respond, Recover*.
8. ISO/IEC 27001:2022, *Information Security Management Systems — Requirements*.
9. ISO/IEC 27002:2022, *Code of practice for information security controls*.
10. ISO/IEC 22301:2019, *Business Continuity Management Systems — Requirements*.
11. ISO/IEC 27701, *Privacy Information Management — Extension to ISO/IEC 27001 and ISO/IEC 27002*.
12. ENISA / ICS-CERT guidance and advisories on Industrial Control System (ICS) security (representative industry guidance).
13. SANS Institute — Best practices and whitepapers on incident response, log management, and endpoint detection.
14. OWASP — *Top 10 Web Application Security Risks* and *Testing Guide* (for web portal/ERP security).
15. Vendor documentation and best-practice guides for common SCADA/PLC platforms and IoT gateways (e.g., Siemens, Rockwell Automation) — used as recommended configuration references.
16. Industry articles and vendor technical whitepapers on ransomware mitigation and OT/IT convergence (representative literature).