https://doi.org/10.65025/ICAIC25019n

Strategic Cybersecurity Governance: A Risk-Based Policy Framework for IT Protection and Compliance.

Mohammed Nayeem
Trine University, United States
nm2751478@gmail.com

Abstract

As cyber threats evolve, organizations must adopt a proactive, risk-based cybersecurity framework to safeguard digital assets and ensure regulatory compliance. This paper presents a comprehensive IT security policy, integrating incident management, data protection, and access control strategies to mitigate cyber risks. The framework emphasizes information classification, identity governance, and adaptive security enforcement to enhance resilience against emerging threats. Additionally, it outlines best practices for cyber risk assessment, policy enforcement, and compliance with global standards such as GDPR and PCI-DSS. This approach provides a structured methodology for securing IT infrastructure while balancing business continuity and security governance.

1. Introduction

The increasing complexity of the digital ecosystem has elevated the importance of structured cybersecurity policies to counter evolving threats. Enterprises must now embrace adaptive, risk-informed approaches to defend essential assets and align with global compliance mandates. This study outlines a unified security strategy encompassing core pillars such as breach response, data governance, and permission control. Emphasis is placed on categorizing information, managing digital identities, and enforcing dynamic security protocols to strengthen organizational resilience. Additionally, the document reviews regulatory alignment with frameworks like GDPR and PCI-DSS, presenting an equilibrium between defense mechanisms and seamless operational function.

2. **Cybersecurity and its Governance**

A. Strategic Directive

COMPANY adheres to verified methodologies and defined cybersecurity ambitions that reinforce operational reliability and ensure alignment with enterprise targets.

B. Objective

1) This document delineates digital security standards de- signed to uphold the core mission of COMPANY: TEMP MISSION STATEMENT.
2) It contributes to market competitiveness by lowering security-related liabilities, improving revenue assurance, and mitigating reputational and financial exposure.
3) This policy emphasizes stewardship of digital infrastructure, personnel, and information. It establishes foundational guidelines that build credibility, strengthen partnerships, and outline the structured processes necessary for mitigating digital risk while sustaining strategic growth.

C. Coverage

1) This policy is applicable to all employees, contractors, third parties, technologies, systems, communication channels, and datasets associated with or governed by COMPANY.
2) Applicability is subject to prevailing legal stipulations and contractual agreements.

D. Compliance Obligations

Noncompliance with these guidelines may result in corrective measures, including but not limited to employment termination, contract suspension, or other applicable consequences.

E. Responsibility Allocation

1) Personnel are expected to manage access privileges, report system alterations, and highlight vulnerabilities to ensure holistic protection.
2) Executive leadership endorses cybersecurity priorities and aligns them with organizational directives.
3) The chief information security authority oversees threat mitigation, regulatory adherence, and the development of subordinate security policies, sometimes in collaboration with external experts.
4) Legal advisors validate data handling and contingency strategies against legal criteria and contribute during security incidents and stakeholder communication.
5) The internal audit division maintains oversight of high-level policies and ensures uniform implementation across all departments.
6) Technical staff facilitate systems administration, man- age access controls, and execute approved configuration changes across organizational infrastructure.
7) Facility managers supervise on-site security, coordinate incident responses, and communicate with cybersecurity personnel when needed.

8) Privileged users possess elevated permissions and must exercise heightened diligence to preserve system integrity.
9) Authorized third parties are granted access after signing appropriate agreements (e.g., NDAs, SLAs, BAAs) and must adhere to the same data protection standards.
10) For detailed task ownership and communication flow, refer to LINK TO RACI DOCS, which include RACI matrices (Responsible, Accountable, Consulted, In- formed).

F. Terminology

Asset — Refers to intellectual property, technological infrastructure, physical or virtual resources, software, platforms, or any device (including personal ones, if applicable) accessing or interacting with COMPANY's digital ecosystem.

G. Framework Directives

1) The cybersecurity directive is governed by the Internal Audit authority and forms the basis for subsidiary protocols enumerated in the attached appendices.
2) The policy is designed to not only satisfy compliance requirements (e.g., GDPR, PCI-DSS) but also to ensure sustainable service delivery and proactive risk oversight.
3) Security mechanisms include but are not limited to:
   a) Defining baseline controls
   b) Identifying and categorizing threats
   c) Conducting employee awareness initiatives
   d) Managing credentials and access rights
   e) Enforcing change governance protocols
   f) Applying least-access principles in a zero-trust model
   g) Prioritizing cloud-native application protection
   h) Evaluating third-party exposure
   i) Encrypting communication channels and digital assets
   j) Implementing backup communication systems
   k) Handling data lifecycle: classification, storage, and elimination
   l) Performing periodic audits and penetration evaluations
   m) Maintaining assets, vulnerability, and patch logs
   n) Executing predefined threat mitigation workflows
   o) Monitoring event logs and retaining forensic records
   p) The overarching strategy is: "Diminish vulnerability exposure, obstruct unauthorized entry, and swiftly identify and contain breaches."

H. Policy Exceptions

1) Any divergences from established protocols must be formally submitted for review and logged by the designated cybersecurity authority and IT department.
2) An official log of sanctioned deviations, along with their associated risk levels, is maintained at: LINK TO EXCEPTIONS REGISTRY
3) Note: Access permissions for the exception archive are role-specific and require justified necessity. The link may be inaccessible without these prerequisites.

I. Governance and Retention

1) Managed Documents

   a) This IT and cybersecurity framework, including all embedded or referenced guidelines and organizational protocols, is versioned to track amendments. Digital copies are preserved for 24 months post their last enforcement date unless regulated otherwise.
   b) After the designated period, obsolete files in physical or electronic form will be eliminated using secure destruction techniques unless exempted by a legal or regulatory requirement.
   c) This directive excludes system log files, which fall under a distinct archival policy.

2) **Archival Records**

   a) Records produced in adherence to the cybersecurity framework or linked policies shall be stored for a minimum of two years. Responsible units must conduct annual audits. All data will be encrypted during storage and transmission.
   b) For compliance purposes, documents subject to extended retention due to legal, financial, or statutory obligations (e.g., litigation materials, insurance claims, or fiscal records) will be preserved accordingly.

3) Circulation and Updates

   a) The cybersecurity policy remains internal and restricted. It is selectively shared with authorized personnel or external entities, as applicable. All modifications will be disseminated to eligible recipients.
   b) A digital archive of present and archival governance documents is available at: LINK TO DOCS AND POLICY

J. **Supplementary Protocols (Appendices)**

A. Data Categorization, Handling, and Preservation Guide- lines
B. Incident Response and Escalation Procedure
C. Asset Oversight Framework
D. Usage Compliance Regulations
E. Change Authorization and Implementation Strategy
F. Telecommuting Standards — Refer to Employee Manual
G. Security Training Framework
H. Continuity Operations Strategy
I. Technical Protection Protocol
J. Brand Risk Oversight
K. Infrastructure Lifecycle Oversight

2. Information Classification, Handling, And Retention Policy

A. **Overview and Purpose**

1) COMPANY follows structured, validated methodologies to assign suitable classifications to information based on sensitivity and potential impact. This policy clarifies how data may be accessed, where it may be used, and the boundaries governing its distribution to safeguard against unauthorized disclosure.
2) By maintaining structured information governance, COMPANY ensures that business continuity objectives remain uninterrupted, and stakeholder interests are diligently protected.
3) Information is a fundamental corporate asset for COM- PANY. The nature and confidentiality requirements of information assets vary and are treated with corresponding protocols.

B. **Scope**

This directive pertains to the entities specified in the foundational Cybersecurity and IT Policy and concerns the classification and stewardship of organizational information assets.

C. Enforcement

Refer to the enforcement provisions detailed within the base Cybersecurity and IT Policy.

D. Roles and Responsibilities

Maintenance of this directive is assigned to the designated security executive (e.g., CISO), in cooperation with legal and departmental heads. Implementation across departments rests with the respective unit leaders.

E. Acronyms

There are no acronyms defined under this section.

F. Policy

Privacy alignment is inherited from the parent cybersecurity policy. Certain segments of this directive may be held under a stricter classification and stored separately according to relevant access control standards.

G. Classification Categories

1) COMPANY organizes data into three tiers: Public, In- ternal, and Confidential.
   a. Public: Data suitable for general release that does not jeopardize the firm’s position or operations if disclosed.
      i. Includes assets without confidentiality constraints, such as public reports, marketing publications, or corporate websites.
   b. Internal: Data not meant for public circulation but not severely harmful if inadvertently released.
      i. Examples include internal notices, administrative circulars, resource scheduling, or vendor invoices.
   c. Confidential: Data vital to projects, departments, or corporate processes whose exposure may inflict operational, financial, or reputational harm.
      i. Includes business strategies, sensitive agreements, proprietary technology, personal identifiable data, and anything with legal or regulatory safeguarding.
      ii. Must be shared strictly on a need-to-know basis. If stored, data must be backed up and encrypted or password-protected; if transmitted, encryption is mandatory.

   d. Confidential: Special (e.g., XYZ-specific): A specialized subclass requiring exceptional protection due to legal, regulatory, or client constraints. De- tails are maintained in separately secured documentation.

H. Secure Handling of Information Assets

1) Each asset must be labeled with its classification in headers, footers, and filenames; physical media must bear visible external tags.
2) Some data levels mandate pre-approval from senior leadership or legal entities before transmission.
3) Confidential materials must only be dispatched via authenticated, trusted courier services.
4) Printed confidential data must be physically secured in locked environments and shredded when obsolete.

5) Restrict exposure of classified materials to essential personnel through access controls and custodial chains.
6) Prior to printing, validate the requester's identity and encrypt print spools where feasible.
7) Limit dissemination exclusively to authorized individuals.
8) Periodic audits of user access must occur monthly or at major project milestones.
9) Declassification decisions reside with department heads in consultation with policy custodians and legal counsel.
10) Supplementary reference materials and control procedures: LINK TO INFO INVENTORY

I. Classification by Aggregation

1) Merging or transforming datasets into higher-value in- formation may necessitate reclassification due to elevated sensitivity or derived strategic insights.
2) Aggregated datasets are classified according to the most sensitive element involved.
3) Combinations of identically classified assets may require elevation to the next sensitivity tier.

4. Incident Management Policy and Process

A. Overview and Purpose

The aim of this directive is to enhance information security posture by systematically detecting, assessing, and resolving security incidents, thereby maintaining a competitive operational advantage.

B. Scope

Applicable to all divisions and personnel identified within the Cybersecurity and IT Policy base documentation.

C. Enforcement

Enforcement protocols align with the overarching Cybersecurity and IT Policy.

D. Roles and Responsibilities

1) Security Executive or Designee:
    a) Oversees execution and adherence to the Incident Response Framework.
    b) Coordinates incident containment, acts as primary communication liaison, prepares internal and external briefings, and leads incident drills.
2) Facilities Coordinator: Ensures physical access control prevents disruption during incident management.
3) IT Lead: Maintains real-time updates to the security executive on potential breaches.

E. Acronyms

1) IRT - Incident Handling Unit
2) PACE Strategy - A methodology encompassing Primary, Alternate, Contingency, and Emergency means for completing mission-critical tasks. It ensures communication pathways are predefined for immediate response actions during critical scenarios.
3) MTTR - Mean Time to Remediation
4) CAL OES - California Governor's Office of Emergency Services, which provided the foundational structure for this documentation.
5) SUNY Broome - Referenced as a publicly available source for incident management frameworks.

F. Response Protocol

1) **IRT Composition**
    a) Each organizational division will assign a continuously reachable contact point to support security- related occurrences.
    b) Relevant units may include:
        i. Infrastructure and Security Oversight
        ii. Finance
        iii. Legal Affairs
        iv. Operations
        v. Digital Systems
        vi. Cybersecurity Lead
        vii. Public Engagement and Media
        viii. Internal Review
        ix. Regulatory and Risk Functions
        x. Others, as necessitated
    c) In the absence of the designated representative, the department lead assumes responsibility until the contact role is reassigned.
    d) Comprehensive stakeholder contact data is located at: LINK TO IRT STAKEHOLDERS

2) **IRT Alerting Mechanism**

a) The cybersecurity division will collaborate across departments to create a PACE-based notification model for all IRT affiliates, encompassing internal and third-party entities (e.g., external SOC, IR units, MSSPs).
b) All involved personnel must be familiar with the alert structure and ready to implement any listed communication methods.
c) Each contributing division must configure an alias, mailing list, or system that aligns with the communication hierarchy outlined in the PACE structure.
d) The notification strategy can be accessed at: LINK TO PACE PLAN

3) **IRT Communication Strategy**
    a) According to the PACE design, a centralized command space will be activated to enable collaborative discussions.

b) Physical command centers should accommodate group collaboration, contain multimedia tools, and host a workstation with high-bandwidth connectivity for remote inclusion.

c) Virtual alternatives should support shared media, discussions, and segmented virtual rooms for sub- group coordination.

d) Reference document: LINK TO PACE PLAN

4) External Liaison Records

a) The cybersecurity office will keep contact records for the following:

- Managed Service Providers (MSPs)
- Security-as-a-Service vendors (MSSPs)
- ISP contacts
- Federal Bureau of Investigation (local division)
- Digital Crimes Task Force (local jurisdiction)
- Regional Cyber Response Teams
- Hosting Providers
- Additional relevant external actors

5) Event and Incident Differentiation

a) Definitions are adapted from NIST SP 800-61 Revision 2:

b) Event – A system/network activity such as web- page requests or firewall filtering.

c) Negative Event – An activity with adverse effects like privilege misuse or crashes.

d) Security Breach – Any breach or likely breach of digital policy, standards, or guidelines (e.g., DoS attacks or misuse of organizational assets).

6) Prioritization and Escalation

a) Reported activities undergo preliminary assessment by the first authorized evaluator, who determines whether escalation is warranted. All judgments must be logged in the designated tracking system.

7) Logging and Assessment

a) All incidents must be logged with classification and tracked per internal protocol using guidance from NIST SP 800-61 Rev. 2 and US-CERT.

b) Key documentation includes:

- Incident label and identifier
- Functional and data exposure impacts
- Time of detection and estimated occurrence
- Scope: systems, users, records affected
- Physical/network location data
- Contact references for further inquiry
- Origin mechanism or root exploitation vector
- Related detection or forensic indicators
- Containment/mitigation steps and client guidance

c) Documentation supports retrospective analysis, adversary profiling, and enhancement of organizational resilience.

8) Incident Taxonomy

Table 1: Incident types and response time objectives

—p1.2cm—p2.5cm—X—p1.8cm—
Code Label Definition Target Resolution
CAT A Emulated Events manufactured for testing purposes without operational impact Not Assigned
CAT B Breach or Unauthorized Control Gained physical/logical unauthorized access or deliberate compromise of data/systems. Includes active malware control. Within 1–3 hours
CAT C Disruption of Service attacks that hinder system/service availability 3 Hours
CAT D Malware Introduction System infection from worms, trojans, or malicious payloads (excluding live control cases) 12 Hours
CAT E Illegal System Activity Criminal or unauthorized actions, including digital fraud or threats to safety, possibly involving law enforcement 24 Hours
CAT F Policy Breach Use violations contrary to established computing or network standards 24 Hours
CAT G Probing or Reconnaissance Scanning or enumeration attempts with no direct security impact 72 Hours
CAT H Unverified Behavior Unclassified anomalies under current examination 72 Hours

G. Impact Levels

Outlined below are the levels used to assess impact severity across operational capability.

Table 2: Business Functionality Impact Classification

p2.5cm X
Level Explanation
None No disruption to competitive operational continuity. Low Slight operational disadvantage, with ongoing access to markets. Moderate Market performance becomes uncertain or questionable. Severe Complete inability to maintain competitive market presence.

H. Evidence Retention and Chain of Custody

1) All collected evidence must be tracked with a quantity and detailed description.
2) Custodians of evidence must:
    - Secure the evidence appropriately,
    - Limit access to authorized personnel only,
    - Report the evidence in their control along with transfer history,
    - Maintain thorough documentation.
3) If the evidence is a physical device, document:
    - Manufacturer
    - Model
    - Serial Number
4) If the evidence is a digital file, include:
    - Filename
    - File hash
    - File creation, modification, and access timestamps
    - File size
    - Any physical media used (e.g., USB) must be protected with write blockers
5) For testimonial or recorded statements, include:
    - Interviewee and interviewer names
    - Location and medium used (audio/video/text)
    - Collection date and time
    - Signatures of both parties
6) Testimonial records should only be collected upon legal guidance or requirement.
7) When evidence is transferred between parties, the chain of custody must be strictly maintained. Each transfer record should include:
    - Date and time of transfer
    - Name and department of both parties
    - Purpose of the custody change
    - Signatures of transferring and receiving parties

V. Asset management guidelines

A. Purpose and Overview

1) This policy outlines the procedures for managing IT and information security assets, aiming to support organizational success in competitive markets by establishing clear asset management protocols.
2) It defines the guiding principles for managing various types of assets, including hardware, software, information, and other essential resources.

B. Scope of Application

This policy is applicable to all assets listed in the Cybersecurity and IT Policy. It covers all information and technology re- sources that are owned, leased, or utilized by the organization, or those containing organizational data. This includes IT assets like hardware (e.g., endpoints, office devices, access points), software, IaaS, SaaS solutions (e.g., Google Workspace, AWS, GitHub), and other related platforms.

C. Policy Enforcement

Enforcement mechanisms are detailed in the Cybersecurity and IT Policy.

D. Roles and Responsibilities

1) The CISO or designated representative is tasked with overseeing the execution of this policy and ensuring the program's successful implementation.
2) The IT department is responsible for maintaining precise asset inventories and management tools, including asset deployment and ongoing operational support.
3) Departmental managers are accountable for maintaining accurate asset records and notifying the IT team and CISO of any updates or modifications.

E. Terminology and Definitions

Asset management: The structured process of identifying, tracking, maintaining, and decommissioning both physical and virtual assets within the organization.

F. Guidelines

1) Asset Inventory Management:
    a) The IT department, in collaboration with the information security team, will maintain an up-to-date inventory of all organizational assets. This record will include, but not be limited to:
        i. Device identifiers (name, serial number, IP ad dress, MAC address)
        ii. Operating system and firmware details
        iii. Acquisition and end-of-life dates
        iv. Support and warranty expiration dates
        v. Service contract expiration dates
        vi. Device classification, location, and department ownership
        vii. Primary point of contact and device role description.
2) The asset inventory record is accessible at: LINK_TO_NETWORK_INVENTORY

3) The network topology diagram is available at: LINK_TO_NETWORK_DIAGRAM

G. Software and Service Inventory

1) The IT team will catalog all software and services, detailing information such as:
   a) Vendor name and contacts
   b) Software type and version
   c) Subscription details (account number, quantity, cost, renewal date)
   d) End of support and service expiration dates

2) This inventory will encompass all software (including open-source and proprietary), services, domain registrations, and third-party hosted solutions.

3) Development teams are responsible for tracking software dependencies and packages in production and development environments. These inventories will support risk management through a software bill of materials (SBOM).

4) Software and service records can be found at: LINK_TO_ASSET_INVENTORY

H. Critical Account Management

1) Privileged accounts, which are essential for access to sensitive systems or administrative functions, will be closely monitored and categorized as critical assets.
2) Critical accounts include root/system credentials, third-party access keys, and executive-level personal accounts.
3) Critical account inventories will include:
   a) Account name and access details
   b) Privilege levels and assigned personnel
   c) Date of provisioning and audit reviews

4) Critical account information is stored at: LINK_TO_ASSET_INVENTORY

I. Provisioning and Standardization (Gold Image)

1) Standardized "gold images" will be defined for all key assets.
2) Each server, container, and user workstation will be configured using approved gold images, ensuring vulnerability mitigation and configuration consistency. These images will be reviewed annually.
3) New assets will be provisioned using the organization's gold images and verified prior to deployment in production or testing environments.
4) Gold image details are accessible here: LINK TO GOLD IMAGE LIST

J. Configuration and Patch Management

1) Configuration management is fundamental to patch management.
2) Maintaining up-to-date gold images and their subsequent deployments is essential for lifecycle management and vulnerability mitigation.
3) Patches will be deployed via configuration management systems, ensuring that updates are distributed efficiently across all assets, rather than performing individual system patches.

K. Asset Control Tools

1) The IT team, with support from information security and relevant external partners, will deploy monitoring tools for asset health and status.
2) These tools will track:
   a) Asset status and location (at least on a logical network level)
   b) Running state of assets and associated services
   c) Associated accounts, services, and software
   d) Endpoint protection and log collection for incident response
3) Documentation for asset management tools can be found at: LINK_TO_ENDPOINT_TOOLS_DOCS

VI. Acceptable Use Policy

A. Overview and Intent

1) The objective of this policy is to outline the appropriate and inappropriate usage of data, information, network resources, and electronic devices within COMPANY, fostering a culture rooted in ethical practices, legality, transparency, trust, and integrity. This enables COMPANY to remain competitive in a fast-paced market.
2) COMPANY supplies computing devices, networks, and access to information systems to achieve organizational goals and serve its stakeholders. Management of these resources is crucial for safeguarding the confidentiality integrity, and availability of company assets. Authorized users are responsible for upholding the company's assets and adhering to established policies.

B. Scope

This policy pertains to all entities and assets specified in the foundational Cybersecurity and IT Policy document.

C. Enforcement

Refer to the enforcement clause in the Cybersecurity and IT Policy.

D. Roles and Responsibilities

Roles and responsibilities outlined in the Cybersecurity and IT Policy are inherited by this document.

E. Definitions and Acronyms

1) Honeypot, Honeynet – Technical systems designed for early detection and monitoring of potential security breaches.
2) Spam – Unsolicited electronic communication, including junk emails or newsgroup postings.

F. Policy

1) General Obligations

a) Proprietary information belonging to COMPANY remains its exclusive property, regardless of whether the devices storing this information are owned by the company, leased, or belong to third parties. Employees may access or share proprietary data only within the limits of their assigned duties.

b) Users must exercise sound judgment in utilizing COMPANY resources, aligning with company policies, standards, and guidelines. Company resources should not be used for any unlawful or prohibited activities.

c) Users are prohibited from taking any action that could undermine COMPANY's market position, confidentiality, data integrity, or asset availability without explicit authorization from the relevant authority within the company.

d) For security and maintenance, COMPANY may monitor all infrastructure, user accounts, and systems, including network and endpoint scans. Users must not interfere with authorized auditing processes.

2) Account Security and Access

a) Users are responsible for safeguarding all accounts, data, and systems they manage.

b) All accounts must be protected by a secure username, password, and multi-factor authentication where applicable.

c) Strong password guidelines must be followed:

i. Passwords must be at least 20 characters long.

ii. Passwords should include at least one uppercase letter, one numeral, and one special character.

d) Passwords must not be stored unencrypted. They should be saved in COMPANY's approved password manager.

e) Multi-factor authentication is required, with users being allowed to use tools like Google Authenticator, Authy, or Azure Authenticator for added security.

f) SMS-based authentication is not permitted.

g) Users must never share their credentials with anyone, including the IT team or external parties.

h) Default passwords must be changed immediately after account setup.

i) If an account or password is compromised, it must be changed immediately unless authorized otherwise by the security team.

3) Device Security

a) Users are responsible for securing COMPANY devices, including utilizing cable locks and other security mechanisms. Devices left overnight at COMPANY must be secured by locking doors or cable locks.

b) Any theft or loss of devices must be reported immediately to the Facilities Manager and the IT team.

c) Devices must be locked automatically after 10 minutes of inactivity.

4) Use of COMPANY Assets

a) COMPANY network resources must not be used for unauthorized activities, such as disclosing proprietary information, unauthorized access attempts, or causing disruptions in service.

b) The introduction of unauthorized technology, data, or equipment to COMPANY networks is prohibited.

5) Access Termination

a) Access to COMPANY assets will be revoked immediately upon termination of employment, contract, or agreement, except where legal, investigative, or contractual requirements apply.

6) Electronic Communication

a) The misuse of company assets for illegal or unethical activities, including fraudulent communications or harassment, is strictly prohibited.

7) Training and Awareness

a) All staff must complete annual security training and participate in any simulated exercises conducted by the IT or security teams.

8) Exceptions

a) Any deviation from this policy must be approved by the CISO and documented by the IT Team.

VII. Change Management and Control Policy

A. Policy Overview

This policy ensures effective planning, documentation, response, and learning from modifications to organizational operations.

B. Objective

The objective of this policy is to enhance information security, thereby supporting the organization's competitiveness and market success.

C. Terminology

Change Management denotes the structured approach for modifying IT systems. Its primary aim is to improve organizational awareness and understanding of proposed changes, ensuring minimal negative impact on services and clients.

D. Coverage

1) This policy applies to all entities described in the Cybersecurity and IT Policy documentation.
2) Any alterations to IT services must follow a formalized procedure to ensure adequate planning and execution.

E. Procedure

1) **Planning:** Develop the change plan, including the design, schedule, communication strategy, testing protocol, and contingency plan.
2) **Evaluation:** Assess the change, determine its nature, identify impacted assets, evaluate outage risks, and select the appropriate change classification and process.
3) **Review:** Discuss the change plan with relevant stakeholders or the Change Advisory Board, depending on the change type.
4) **Approval:** Obtain necessary approval from management or designated authorities, depending on the change type. Communication about the change must be shared with the appropriate parties, particularly if it impacts users.
5) **Testing:** Test changes in a controlled environment, prepare fallback procedures, and document lessons learned. Runbooks should be created for user-impacting changes, aiding the help desk during implementation.
6) **Execution:** Execute the change, prepared for potential reversion if needed. For significant or user-impacting changes, a phased approach should be applied, testing with smaller user groups first.
7) **Documentation:** Record the change, including approval and review details. Documentation should include feedback from:
   a) Departments or individuals affected by the change
   b) Teams responsible for implementation
   c) Key stakeholders
   d) Emergency response teams involved

   Post-change reflection is critical for enhancing future changes, enabling faster and more efficient organizational transitions. This phase fosters an understanding of the system and prepares for improved future change planning.

F. Responsibility

Department heads manage the change process within their areas, coordinating with other departments. For changes requiring additional resources, consultation with Finance is necessary during the Approval stage.

G. Documentation Protocol

1) **Log Maintenance:** All changes, whether Normal or Emergency, and their evaluations, will be systematically documented to provide clarity regarding the modifications made, their rationale, and the procedure followed.
2) **Change Log:**
   a) All changes (Standard, Normal, Emergency) will be recorded in the Change Log, including:
      i. The individual or team executing the change
      ii. Description of the change
      iii. Justification for the change
      iv. Date and time of the change
3) **Process Log:**
   a) Changes with Medium or High impact, along with Emergency changes, will be documented in the Process Log, including:
      i. Test plan and results
      ii. Risk assessments
      iii. Communication strategies
      iv. Deployment plans with fallback contingencies

VIII. Security Awareness Policy and Program

A. Policy Statement

This policy aims to foster vigilance among stakeholders to identify and report potential or confirmed incidents.

B. Purpose

The organization's success is tied to safeguarding assets and information. Collective efforts to protect these resources are paramount.

C. Scope

1) This policy extends to all entities as described in the Cybersecurity and IT Policy framework.
2) All users of COMPANY and external partners with access to the organization's information or systems are required to undergo training.

D. Policy

1) The objective is to raise awareness about information risks and guide users in taking suitable actions based on their access privileges. The program encompasses:
   a) Annual mandatory training sessions.
   b) Periodic awareness surveys.
   c) Unannounced evaluations to ensure compliance.
   d) Feedback mechanisms to refine the training program.
   e) Phishing and social engineering exercises.
   f) Simulated penetration testing and physical security checks.
   g) Specialized training for high-privilege users, including incident response and forensic analysis.

2) Training completion records and performance results will be stored in the individual's Human Resources file.

E. Responsibility

The Chief Information Security Officer (CISO) oversees the program, with contributions from Legal, HR, and the IT Committee.

IX. Technical Security Policy

A. Policy Statement

This policy is designed to establish a framework for technical security, guiding the strategy to reduce vulnerabilities and enhance defenses.

B. Purpose

The policy ensures that technical security efforts support the organization's competitive edge in the market.

C. Scope

The policy is applicable to entities defined in the Cybersecurity and IT Policy framework.

D. Roles

1) Roles follow the guidelines outlined in the Cybersecurity and IT Policy document, with exceptions made when necessary.
2) Data Loss Prevention Officer (DLPO): This role may either be added as an additional responsibility or independently assigned. The DLPO leads risk mitigation efforts to support the CISO and minimize risks within the partner network. Responsibilities include data identification, classification, and safeguarding.
3) IT Committee: Works with the CISO and DLPO to ensure technical security policies are relevant. The committee serves as the Change Control Review Board, with a voice in decision-making, particularly regarding user spend.

E. Policy Overview

1) Continuous efforts will be made to minimize the attack surface and enhance security by implementing the NIST framework: Identify, Protect, Detect, Respond, and Recover.
2) Regular reviews will be conducted to comply with security requirements from partners or legislation, adopting prudent measures where formal requirements are absent.
3) Assuming compromise is an integral part of the security strategy, with efforts focused on answering critical incident-related questions, including containment, notification, and recovery.
4) **Identify:**
   a) Continuous integration of security measures with IT and operations to understand and manage the attack surface. A regular inventory of assets and proactive identification of "Shadow IT" are key.
   b) Security sensors will be deployed to monitor changes to the attack surface, with regular external scans to detect unapproved additions.

5) **Protect:**
   a) While some systems may follow a shared responsibility model, prudent controls will be applied, especially for cloud-based services, with multifactor authentication and vendor risk assessments.
   b) Endpoint security will involve preconfigured images, device registration, and multifactor authentication, along with behavioral analytics to identify suspicious activities.

6) **Detect:**
   a) Focused efforts on identity, endpoint, and network monitoring will ensure early detection of anomalies.
   b) A zero-trust identity model will be implemented, with extended integration across critical SAAS platforms to monitor access points and identify unauthorized activities.
   c) Device health checks and intrusion detection systems will be deployed to detect threats at the endpoint level.
   d) Network monitoring solutions will be applied to track data flows within internal networks and during remote access.
   e) Log Aggregation Policy:
      i. Logs will be retained for 13 months to ensure visibility, with precomputation to reduce unnecessary data transmission.

ii. Aggregated logs will be used for correlation, forensic analysis, and incident response.

7) **Respond:** Refer to the Incident Management Policy for detailed response actions.
8) **Recover:** Refer to the Business Continuity Policy for recovery strategies.

X. Conclusion

This study highlights the necessity of adopting a forward-thinking, risk-driven cybersecurity strategy to safeguard organizational assets and meet compliance requirements. By consolidating incident management, data security, and access control mechanisms, the proposed cybersecurity framework offers a resilient defense against emerging threats. Emphasizing data categorization, identity management, and flexible security practices enhances the system's ability to withstand evolving risks. Moreover, compliance with international standards such as GDPR and PCI-DSS strikes a balance between maintaining robust security and supporting operational continuity. This framework provides a systematic and scalable solution for fortifying IT infrastructure in a constantly changing security environment.

References

[1] NIST, Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, Version 1.1, Apr. 2018. [Online]. Available: https://www.nist.gov/cyberframework

[2] International Organization for Standardization, ISO/IEC 27001:2013 - Information technology – Security techniques – Information security management systems – Requirements, ISO, 2013.

[3] Voigt, P., and von dem Bussche, A., The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017.

[4] PCI Security Standards Council, PCI DSS v4.0: Payment Card Industry Data Security Standard, March 2022. [Online]. Available: https://www.pcisecuritystandards.org

[5] Bertino, E., and Takahashi, K., "Identity management: Concepts, technologies, and systems," Computers & Security, vol. 31, no. 4, pp. 451–459, 2012.

[6] Shedden, P., Smith, W., and Ahmad, A., "Information security risk assessment: Towards a business practice perspective," Journal of Information Security and Applications, vol. 34, pp. 33–43, 2017.